Report of the Office of the High Commissioner for Human Rights on the right to privacy in the digial age

Contribution by the Federal Republic of Germany

1. Recent developments in national or regional legislation, case law, and practice concerning the right to privacy in the digital age

Reform of the EU data protection framework

On 6 April 2016, the EU agreed on a major reform of its data protection framework, by adopting the data protection reform package, comprising the General Data Protection Regulation (Regulation (EU) 2016/679 - GDPR)[1] and the Police Directive (Directive (EU) 2016/680)[2]. The GDPR applies from 25 May 2018 and will become directly applicable to all matters concerning the protection of fundamental rights and freedoms vis-à-vis the processing of personal data within the EU's competency which are not subject to specific obligation. The GDPR was designed to harmonize data privacy laws across Europe, to strengthen the protection of the individual's right to personal data protection and will guarantee the free flow of personal data between EU Member States. Thus, a harmonized legal framework is leading to a uniform application of rules for citizens and businesses. However, the GDPR permits Member States to modify several provisions under certain conditions via local legislation (opening clauses). In order to keep the quality of German data protection standards and in using several opening clauses Germany adopted the Act to Adapt Data Protection Law to Regulation (EU) 2016/679 and to Implement Directive (EU) 2016/680 which includes the Federal Data Protection Act[3]. These amendments will also come into force in May 2018.

ePrivacy Regulation

Further discussion is ongoing at EU level on the proposal for a Regulation concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EG (ePrivacy Regulation)[4], containing rules for processing electronic communication data and the use of processing and storage capabilities of terminal equipment and the collection of information form end-user's terminal equipment. The latter is relevant for using Cookies.

Interoperability of EU information systems (justice and home affairs)

[1] http://eur-lex.europa.eu/eli/reg/2016/679/oj

[2] http://eur-lex.europa.eu/eli/dir/2016/680/oj

[3] https://www.bmi.bund.de/SharedDocs/downloads/EN/gesetztestexte/datenschutzanpassungsumsetzungsgesetz.html

[4] http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2017:0010:FIN

Also on EU level, special attention should be drawn to the COM proposal on the interoperability of EU information systems in the area of justice and home affairs (procedure 2017/0352/COD). This proposal aims at strengthening in a comprehensive manner the EU's information tools for border management, migration and security in full respect of the right to the protection of personal data by

(1) ensuring that end-users, particularly border guards, law enforcement officers, immigration officials and judicial authorities have fast, seamless, systematic and controlled access to the information that they need to perform their tasks;

(2) providing a solution to detect multiple identities linked to the same set of biometric data, with the dual purpose of ensuring the correct identification of bona fide persons and combating identity fraud;

(3) facilitating identity checks of third-country nationals, on the territory of a Member State, by police authorities; and

(4) facilitating and streamlining access by law enforcement authorities to non-law enforcement information systems at EU level, where necessary for the prevention, investigation, detection or prosecution of serious crime and terrorism.

Decision of the Federal Constitutional Court of 20 April 2016 (BVerfGE 141, 220 ff.)

On federal level, in addition to the implementation of Directive (EU) 2016/680, a far-reaching decision of the Federal Constitutional Court (Bundesverfassungsgericht) of 20 April 2016 had to be implemented into the law governing the work of the tasks of the Federal Criminal Police Office (Bundeskriminalamt, BKA). In this decision the Court further framed its approach to the requirements that have to be met in order to process personal data for purposes other than those that the data originally had been collected for. These requirements have been met in the new 2017 law on the Federal Criminal Police Office (Bundeskriminalamtgesetz) and were implemented by a reorganization of the way the BKA – being the focal point (Zentralstelle) of the information sharing in the German law enforcement sector – processes personal data in both a data protection friendly way and using state-of-the-art technology. The implementing process (project "Polizei 2020") is ongoing and requires efforts both on the federal level and the level of the German states (Länder).

2. Surveillance and communications interception:

a. Government surveillance, including, for example, communications interception and bulk data collection and processing, targeted intrusions in ICT systems and issues relating to cross-border surveillance and access to personal data.

German police and law enforcement authorities as well as federal intelligence services are authorized to intercept and record telecommunications. These activities are inter alia

governed by the Act to restrict the Privacy of Correspondence, Posts and Telecommunications (also known as the Act adopted by virtue of Article 10 of the Basic Law, Artikel 10-Gesetz) which provides for various safeguards for the collection and processing of personal data. Under this act, collecting information on the core area of private life is prohibited, and relevant records must be deleted without undue delay. The authority collecting data will verify immediately and at subsequent intervals of no more than six months whether a further storage of the data is necessary and it will delete data that are no longer needed. Moreover, sharing data with other authorities is permitted only for specific purposes defined by law.

The German government considers it legitimate for a government to use telecommunication surveillance also by intelligence services, including the collection of meta data, as long as the measures are in line with international human rights obligations and in accordance with national law. Therefore, legal surveillance requires an authorization by a duly enacted law having a legitimate purpose and being proportionate.

This interpretation is in line with a judgement of the European Court of Human Rights in the case of Klass and others v. Germany (5029/71), which explains: “Democratic societies nowadays find themselves threatened by highly sophisticated forms of espionage and by terrorism, with the result that the State must be able, in order effectively to counter such threats, to undertake the secret surveillance of subversive elements operating within its jurisdiction. The Court has therefore to accept that the existence of some legislation granting powers of secret surveillance over the mail, post and telecommunications is, under exceptional conditions, necessary in a democratic society in the interests of national security and/or for the prevention of disorder or crime.“

German legislation is in line with this judgement. The protection of human rights obligations is guaranteed through precise legal requirements regarding surveillance measures, as well as through the constitutional guarantees, in particular proportionality.

The OHCHR workshop on the right to privacy (19-20 February 2018) in Geneva discussed the extraterritoriality of government actions outside its borders. The German government considers the extraterritorial application of constitutional and human rights a complex issue. Decisions by domestic and international courts provide necessary guidance, whereas several questions in that regard remain to be decided.

b. Role of business enterprises in contributing to, or facilitating government surveillance activities, including:

i. Sale of surveillance technology by business enterprises and ensuing responsibilities

ii. Business enterprises' internal safeguards and remedial mechanisms.

Through its National Action Plan on Business and Human Rights, the German government is committed to address the human rights responsibility of business enterprises, in line with the Guiding Principles on Business and Human Rights which were adopted by consensus by the UN Human Rights Council in June 2011. Where the business operations of an enterprise have an international dimension, procedures for identifying any actual or potential adverse impact on the human rights of people affected by its business activity should be developed and implemented.

On Privacy, locally operating municipal utilities play a particular role. They are increasingly developing new information and communication technology for networks and innovative storage technologies such as smart grids and smart meters. Municipal utilities also have an obvious advantage over global corporations: they have local roots and enjoy a higher degree of public trust than the latter. The municipal economy can use the public's trust to establish new, intelligent services that also meet the high standards for data protection.

3. Encryption and anonymity as enablers for the enjoyment of human rights, including the right to freedom of expression and of opinion; challenges raised by encryption and anonymity and ways to address these challenges.

The use of encryption can mitigate the risks of unlawful processing of personal data. Federal legislation takes into account the role of encryption in ensuring the protection of personal data: The De-Mail Act which entered into force on 3 May 2011 is the national legal basis for confidential e-mail communication. Service providers accredited under this act are obliged to offer a mailbox and e-mail delivery service that guarantees the confidentiality, integrity and authenticity of e-mails. To this end, e-mails are encrypted in transit; when transmitted between service providers, also the content of e-mails is encrypted. In addition, users may encrypt their e-mails end-to-end themselves.

Upon request, the service provider may assign users pseudonymous De-Mail addresses. On EU level, the "Eleventh progress report towards an effective and genuine Security Union"[5] by the European Commission provides for a comprehensive description of challenges faced by

[5] https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-we-do/policies/european-agenda-security/20171018_eleventh_progress_report_towards_an_effective_and_genuine_security_union_en.pdf, p. 8 ff.

law enforcement and judicial authorities and proposes a set of measures to support these authorities when encountering the use of encryption by criminals in criminal investigations.

4. National legislative and regulatory frameworks concerning the collection, processing, retention or use of personal data by Governments and other actors, in particular business enterprises, related human rights protection gaps and ways to bridge those gaps.

In Germany the law provides for the mandatory retention of traffic data by telecommunications providers for a period of ten weeks and of location data for a period of four weeks. E-Mail related data is excluded from mandatory retention as is all content-related data. Access to the data is strictly limited and requires authorization by a court. The court may order retained data to be transferred to law enforcement authorities if facts give rise to the suspicion that a person has committed one of several listed particularly serious criminal offences, and the offence is particularly serious in the individual case as well, and other means of establishing the facts or determining the accused's whereabouts would be much more difficult or offer no prospect of success and finally access to the data is proportionate. After the retention period(s) the data have to be deleted; access is no longer possible. During the time of detention, the access is strictly limited to cases of serious criminal offences listed in the Code of Criminal Procedures.

This regulation has been challenged in court by an Internet Access Provider. A Higher Administrative Court ruled in July 2017 that the provider is not obliged to store data until the main proceedings are concluded. It based its decision on the notion that in light of the Tele2 judgment the German legislation on data retention would clearly be incompatible with EU law.

Following the decision of the Higher Administrative Court, the Federal Network Agency announced that it will abstain from enforcement measures regarding the storage obligations and that it won’t impose fines for non-compliance with the storage obligations until main proceedings are concluded. Therefore currently no data is being mandatorily retained by telecommunications providers.

Furthermore the law provides access to traffic data (not: location data) retained by providers for commercial or technical reasons. The access requires authorization by a court or - if urgent - by a public prosecutor. The court may order data retained for commercial reasons to be transferred by the provider if the case is dealing with a serious criminal offence (or in cases where the offence was committed by means of telecommunication) and if access to the data is necessary and proportionate.

See also answer to question 1.

5. Growing reliance on data-driven technology and biometric data*:*

a. **How can new technologies help promote and protect the right to privacy?**
b. **What are the main challenges regarding the impact on the right to privacy and other human rights?**
c. **What are the avenues for adequate protection of the right to privacy against threats created by those technologies? How can the international community, including the UN, address human rights challenges arising in the context of new and emerging digital technology?**

In our networked world, technology or technical and organizational measures are key elements to put data protection rules into practice. The principle of data protection by design and by default can help to create incentives for innovative solutions to address data protection issues from the start. The application of pseudonymisation to personal data can reduce the risks to the data subjects concerned and help controllers to meet their data-protection obligations. Particularly in the context of big data where personal data are often used for a purpose other than that for which the personal data have been collected, pseudonymisation can be an efficient tool to balance the legitimate interests of the controller and the rights and freedoms of the data subjects.

More and more algorithms (particularly machine learning based) will be used for complex application scenarios and personalized recommendations. Regulatory approaches in the GDPR are the following, which could be an example for legislation: Art. 21 GDPR gives the data subject the right to object to processing of personal data in certain situations, including profiling and according to Art. 22 GDPR the data subject will – with certain exemptions – have the right not to be subject to a decision based solely on automated processing or profiling, if this decision produces legal effects concerning him or her or similarly significantly affects him or her.

As enterprises depend more and more on big data analysis, and as these decisions have the potential to significantly impact on people's lives, transparency and accountability become increasingly necessary to make sure that the algorithm picks up the right reasons and human bias and errors did not influence the algorithm. However, transparency rules should not adversely affect the trade secrets or intellectual property and in particular the copyright protecting the software. Furthermore, data-ethic committees could supply answers in more detail to the accompanying questions in this field raised by governments, business enterprises and citizens.

Both in the area of law enforcement and immigration, the use of biometrics in full respect of the right to the protection of personal data is an important tool not only to detect the use of multiple identities and identity fraud but also in order to enable the competent authorities to focus their resources on individuals correctly identified.

6. **Undue interferences with the right to privacy in the digital age that may have particular effects for women, as well as children and persons in vulnerable situations or marginalized groups, and approaches to protect those individuals.**

People in vulnerable situations and their needs and situation are given special consideration in the implementation of human rights.

The precept of equality for men and women is constitutionally enshrined as a fundamental right in Article 3(2) of the Basic Law. Participation by men and women on an equal footing at all levels is a top priority of the Federal Government. Persons with disabilities enjoy special protection and support based on Article 3(3) of the Basic Law. Moreover, the Federal Government will clarify and therefore enhance the fundamental rights of children in the Basic Law within the next years.

The GDPR contains various rules in order to provide a high level of data protection to children. According to Recital 38 of the GDPR children "merit specific protection with regard to their personal data, as they may be less aware of the risks, consequences and safeguards concerned and their rights in relation to the processing of personal data. Such specific protection should, in particular, apply to the use of personal data of children for the purposes of marketing or creating personality or user profiles and the collection of personal data with regard to children when using services offered directly to a child." When assessing whether or not there is a "legitimate interest" in processing personal data the controller has to specifically take into account the fact that the data subject is a child (Article 6 § 1 (f) of the GDPR). Moreover, according to Article 8 of the GDPR there is a minimum age for children to give valid consent in the processing of their personal data. Controllers are also obliged to provide information in "a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child" (Article 12 § 1 of the GDPR). Under Article 57 § 1 (b) of the GDPR data protection supervisory authorities have the task to "promote public awareness and understanding of the risks, rules, safeguards and rights in relation to processing. Activities addressed specifically to children shall receive specific attention".

7. **Procedural and institutional safeguards, oversight mechanisms and remedies available to individuals exposed to domestic or extraterritorial surveillance, the interception of digital**

communications or other forms of processing of personal data by governments, business enterprises or private organizations.

Both internal data protection officers being embedded in public authorities and private entities and supervisory data protection authorities, which act in complete independence and are provided with the human, technical and financial resources, premises and infrastructure necessary for an effective performance, are crucial. Social networks – especially those with high market power – collect and produce a vast amount of information, much of which is of interest to businesses for commercial intention. We experience that in certain cases users of social networks do not receive clear, transparent and easily accessible information on the purpose of processing. International common standards on data protection requirements on social networks together with intensified cooperation between data protection authorities could be a way to globally improve this situation.