11 June 2021 T-PD(2021)6

CONSULTATIVE COMMITTEE OF THE CONVENTION FOR THE PROTECTION OF INDIVIDUALS WITH REGARD TO AUTOMATIC PROCESSING OF PERSONAL DATA

Report on the need for a Guidance note on Article 11 of the modernised Convention 108

prepared by

Dr. Thorsten Wetzling and Charlotte Dietrich

Directorate General of Human Rights and Rule of Law

Contents

Preface[1]

State Parties to the modernised Convention 108 have legitimate needs to collect and to process personal data. They also share core values, notably the respect for the rule of law, as well as human rights and fundamental freedoms.

Therefore, State Parties to the modernised Convention 108 recognise, both internally and in their cooperation with other State Parties, that the collection and processing of personal data might interfere with fundamental rights and freedoms and must, therefore, be justified and conducted in compliance with a wide range of safeguards throughout the entire lifecycle of data processing measures.

It is especially with regard to the conditions that the modernised Convention 108 places on the processing of personal data that it offers an important contribution to the ongoing quest for clearer and more comprehensive and binding articulation of what, exactly, such safeguards must entail, both in the books and on the ground. It's contribution is all the more important because, *prima facie*, the Convention does not rule out safeguards when the data processing takes place for security and defense purposes.

This being said, the modernised Convention 108 offers several exceptions in Article 11 that allow State Parties to derogate from specific provisions of the Convention.[2] Having studied these exceptions more carefully, we caution that the very scope and the compatibility of some of them with the European Convention on Human Rights ought to receive far more critical attention. Some exceptions, as will be illustrated further in Section 3, are remarkably broad. In our view, they ought to be trimmed significantly and we offer some guidance in this note as to possible things to consider or steps to reflect in this regard.

Yet, in order to illustrate this further at the outset, consider the "requirement that processing activities for national security and defense purposes are subject to independent and effective review and supervision under the domestic legislation of the respective Party" (Article 11 paragraph 3). To us, there is a considerable need for further clarity, especially in light of recent jurisprudence of key European courts on matters of bulk collection, cross-border data transfers and data retention, how this requirement can be aligned with the third exception mentioned in Article 11, paragraph 3, where State Parties might be allowed to do away with the safeguard in Article 15, paragraph 2, littera a, namely that "supervisory authorities responsible for ensuring compliance with the provisions of this Convention shall have powers of investigation and intervention" (the same applies to the important other features of effective review and supervision under Article 15, paragraph, 2 literrae b, c and d).

The question arises what to do if the important requirement of the last sentence in Article 11 paragraph 3 is not being met? In other words that if neither domestic legislation nor domestic review and supervision practice on data processing for national security and defense purposes sufficiently incorporate what the European Court of Human Rights has recently called "the

[1] The authors would like to thank Mr. Corbinian Ruckerbauer for his valuable research assistance.

[2] Unless otherwise mentioned, when this Guidance note refers to Articles, it refers to the provisions in the modernised Convention 108.

cornerstone of any Article 8 compliant bulk interception regime" (Centrum för Rättvisa v. Sweden, 25 May 2021, paragraph 264), namely

> "end-to-end safeguards", "meaning that at the domestic level, an assessment should be made at each stage of the process of the necessity and proportionality of the measures being taken; that bulk interception should be subject to independent authorisation at the outset, when the object and the scope of the bulk operation are being defined; and that the operation should be subject to supervision and independent ex post facto review"?

Should the third exception in Article 11 paragraph 3 be available to State Parties even when the "review and supervision under the domestic legislation of the respective Party" does not incorporate "end-to-end safeguards"? To us, such mechanisms should no longer be considered "independent and effective".

Before turning to this and other exceptions of Article 11 of the modernised Convention 108, let us briefly recall the important joint statement by Alessandra Pierucci, Chair of the Committee of Convention 108 and Jean-Philippe Walter, Data Protection Commissioner of the Council of Europe on "better protecting individuals in the context of international data flows: the need for democratic and effective oversight of intelligence services":

> "Personal data is generated by each of our keyboard strikes, every movement made under the gaze of cameras and smartphones, any message sent, or picture taken. As our lives become increasingly digital, and online services internationally intertwined, our personal data flow across frontiers, regardless of national or regional borders, and our effective protection becomes difficult to secure.
>
> [...] Privacy and data protection are fundamental rights. They are essential to the effective functioning of democratic societies and have become even more essential in our digital era. [...] Those rights cannot be compromised: they can only be lawfully limited, under specific and strict conditions, as may for instance be the case when threats to national security exist, or as was the case more recently, to our health. Such restrictions on our fundamental rights to privacy and data protection are narrowly circumscribed and a number of safeguards have to be observed for such interferences to be permissible and the essence of the fundamental rights and freedoms to be respected." (Pierucci and Walter 2020)

As indicated, whether or not restrictions and exceptions are indeed "narrowly circumscribed" or whether they remain too broad and grant States "unduly wide leeway"[3] will be discussed with regard to each of the exceptions listed in Article 11. We note at the outset, however, Pierucci and Walter's observation:

[3] Explanatory Report to the Council of Europe's Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data of 1981 and its Additional Protocol (CETS No. 108, paragraph 56)

> "While Convention 108+ provides a robust international legal framework for the protection of personal data, it does not fully and explicitly address some of the challenges posed in our digital era by unprecedented surveillance capacities. For years, calls for a comprehensive international human rights law instrument framing the operations of intelligence services have intensified, and the need for strong safeguards at international level, complementing and specifying those of Convention 108+, can no longer be ignored." (Pierucci and Walter 2020)

The fact that challenges arising from unprecedented surveillance capacities are not fully and explicitly addressed by the modernised Convention 108 manifests itself, we argue, in the many broad exceptions that the Convention allows to State Parties in Article 11. The challenge, therefore, remains how to ensure that data processing, including in the realm of national security, which doubtlessly can be necessary, adheres as much as possible to the core principles of the modernised Convention 108. For this, the exceptions and restrictions ought to be sufficiently curtailed so as to reduce the potential for abuse and to allow for independent and effective accountability mechanisms, both in the books and on the ground.

This, we believe, is a key requirement for public trust in government. That trust is not a given but needs to be earned. It ties the delicate fabric of our open societies together and is our key asset vis-à-vis authoritarian regimes.

I. A note on the aim and the structure of this guidance note

Much of the modernised Convention's real-world effectiveness depends on its precision and clarity. This presupposes a common understanding among State Parties with regard to the key terms invoked in the provisions of this Convention, including a joint understanding as regards the scope and limitations of the exceptions and restrictions listed in Article 11. Our means to promote such a common understanding are, of course, limited but we hope that delegations will find parts of the material presented here helpful.

We undertook the following efforts in the preparation of this note: As you can see in the Annex, we distilled from previous explanatory notes and additional material such as the jurisprudence of key courts as much information as we deemed helpful to hone in on the essence of the meaning of the key terms invoked in Article 11. By itself, this turned out to be a significant challenge and we are conscious that our work is incomplete and that more work needs to be done in this regard. Also, we know that the "knowledge base" we refer to is constantly evolving and subject to change. Still, our discussion of the terms has helped us to prepare this guidance note on the exceptions in Article 11 and we invite you to consider the material and point us to material that can help us address some of the open questions we identified.

Next, and this became section 3.3, we went through the first regime of exceptions in Article 11, paragraph 1, followed by a discussion of the second regime of exceptions in Article 11, paragraph 3 (see section 3.4). In both sections, we begin by describing in plain language the essence of each individual exception, followed by a *general* problem statement which includes

our elaboration, where suitable, of what the exception could entail in actual practice. Then, we try to go deeper and focus on the individual litterae and discuss what the criteria

- respect the essence of fundamental rights and freedoms
- constitute a necessary and proportionate measure in a democratic society
- provided by law
- (and in section 3.4.) the requirement "subject to independent and effective review and supervision under the domestic legislation of the respective Party"

would require for such exceptions to be lawful. Finally, we summarise our findings for each exception followed by guidance as to possible actions or steps that might help to "*to avoid that, with regard to the general application of the convention, States would have an unduly wide leeway.*"[4]

The aim of this guidance note is to help generate a common understanding among the Parties to the modernised Convention 108 on the key terms and notions used in Article 11 and to allow for discussions as to whether the exceptions are still suitable in light of recent jurisprudence and developments. We believe that further consultations are necessary and our text points to potential actions or processes that could be helpful to better curtail the scope of these exceptions going forward.

We thank you for considering this note and look forward to whatever feedback you may have.

II. Content of Article 11 of the modernised Convention 108

Article 11 – Exceptions and restrictions

1. No exception to the provisions set out in this Chapter shall be allowed except to the provisions of Article 5 paragraph 4, Article 7 paragraph 2, Article 8 paragraph 1 and Article 9, when such an exception is provided for by law, respects the essence of the fundamental rights and freedoms and constitutes a necessary and proportionate measure in a democratic society for:

a. the protection of national security, defence, public safety, important economic and financial interests of the State, the impartiality and independence of the judiciary or the prevention, investigation and prosecution of criminal offences and the execution of criminal penalties, and other essential objectives of general public interest;

b. the protection of the data subject or the rights and fundamental freedoms of others, notably freedom of expression.

2. Restrictions on the exercise of the provisions specified in Articles 8 and 9 may be provided for by law with respect to data processing for archiving

[4] Explanatory Report to the Council of Europe's Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data of 1981 and its Additional Protocol (CETS No. 108, paragraph 56)

purposes in the public interest, scientific or historical research purposes or statistical purposes when there is no recognisable risk of infringement of the rights and fundamental freedoms of data subjects

3. In addition to the exceptions allowed for in paragraph 1 of this article, with reference to processing activities for national security and defense purposes, each Party may provide, by law and only to the extent that it constitutes a necessary and proportionate measure in a democratic society to fulfill such aim, exceptions to Article 4 paragraph 3, Article 14 paragraphs 5 and 6 and Article 15, paragraph 2, litterae a, b, c and d.

This is without prejudice to the requirement that processing activities for national security and defense purposes are subject to independent and effective review and supervision under the domestic legislation of the respective Party.

III. Exceptions allowed for under Article 11, paragraph 1 of the modernised Convention 108

State Parties may have legitimate interests and needs to collect and to process personal data. As this may unduly interfere with fundamental rights and freedoms, the modernised Convention entails a wide range of safeguards to protect the individual. Only when the conditions in Article 11 are being met can State Parties derogate from some provisions of the modernised Convention 108.

3.1. Overview

Article 11 contains two exception regimes, namely those referred to in Article 11, paragraph 1 and those referred to in Article 11, paragraph 3. Taken together, one could paraphrase the challenge this guidance note seeks to address as follows:

How to ensure that

- Data processing (Art. 5.4)
- Notification of a personal data breach to the supervisory authority (Article 7(2))
- Transparency obligation (Article 8(1))
- Data subject rights (Art 9)
- Evaluation mechanism for legislation (Article 4(3))
- International transfer of data and data protection authority's scope of authority (Article 14(5) and 14(6))
- Powers of supervisory authorities (Article 15(2))

in the context of exceptions and restrictions pursuant to Article 11

a. the protection of **national security**, **defense**, **public safety**, **important economic and financial interests of the State**, the **impartiality and independence of the judiciary** or the **prevention, investigation and prosecution of criminal offences** and the execution of criminal penalties, and **other essential objectives of general public interest**;

b. the **protection of the data subject or the rights and fundamental freedoms of others**, notably freedom of expression.

adheres to the following provision as laid down by Article 11

- provided by law
- respect the essence of fundamental rights and freedoms
- constitute a necessary and proportionate measure in a democratic society
- are subject to independent and effective review and supervision under the domestic legislation of the respective Party

By and large, one general challenge that delegations face when they are trying to arrive at a common and more precise understanding of the terms of the Convention is to grasp the de facto utility of the safeguards in the context of the numerous exceptions allowed for under Article 11.

3.2. Outlook

A first step towards meeting this challenge, we take it, is to take the individual exceptions at face value and discuss their meaning and potential scope in the absence of further consultations.

In order to do this, we structured the ensuing discussion for each of the exceptions mentioned in Article 11 as follows:

- We describe the individual exception.
- Thereafter, the text offers a *general* problem statement for each exception with a view to provide further clarity. This includes our analysis, where suitable, of what the exception could entail in practice.
- Then, we will go deeper and focus on the individual litterae by
    - providing a problem statement that seeks to capture the essence of each exception using that particular littera
    - juxtaposing each of the individual litterae (e.g “processed fairly and in a transparent manner”) against the criteria
        - provided by law
        - respect the essence of fundamental rights and freedoms
        - constitute a necessary and proportionate measure in a democratic society
        - are subject to independent and effective review and supervision under the domestic legislation of the respective Party

- Finally, we summarise our findings for each exception followed by guidance as to possible actions that might help to prevent leaving State Parties an "unduly wide leeway with regard to the general application of the Convention."[5]

3.3. Exceptions under Article 11, paragraph 1

The first exception regime allows for a first degree interference with individuals' privacy by allowing State Parties to enact legislation which would lawfully authorise data controllers processing personal data for enumerated specific public interest purposes not to comply with certain data protection principles and provisions under the modernised Convention 108 if the objective criteria for their use (the exception is provided for by law, respect the essence of fundamental rights and freedoms and is necessary in a democratic society) are equally met.

This provision also means that State Parties cannot exempt or derogate from the application of other principles and provisions that are not listed under the first regime.

3.3.1 Article 5, paragraph 4: Data processing

3.3.1.1. Description:

This exception allows State Parties to derogate from Article 5 paragraph 4 of the modernised Convention provided the terms of Article 11 paragraph 1 are being met.

Thus, State Parties may enact legislation that does not comply with the provision that

> *4. Personal data undergoing processing shall be:*
>
> *a. processed fairly and in a transparent manner;*
> *b. collected for explicit, specified and legitimate purposes and not processed in a way incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes is, subject to appropriate safeguards, compatible with those purposes*
> *c. adequate, relevant and not excessive in relation to the purposes for which they are processed;*
> *d. accurate and, where necessary, kept up to date;*
> *e. preserved in a form which permits identification of data subjects for no longer than is necessary for the purposes for which those data are processed*

under the condition that such exceptions are

- provided by law,
- respect the essence of the fundamental rights and freedoms and
- constitute a necessary and proportionate measure in a democratic society for

[5] Ibid.

a. the protection of national security, defense, public safety, important economic and financial interests of the State, the impartiality and independence of the judiciary or the prevention, investigation and prosecution of criminal offences and the execution of criminal penalties, and other essential objectives of general public interest;

b. the protection of the data subject or the rights and fundamental freedoms of others, notably freedom of expression.

3.3.1.2. Problem Statement

This means that as long as the non-compliance with the important Article 5 paragraph 4 obligations is provided by law, respects the essence of fundamental rights and freedoms and constitutes a necessary and proportionate measure in a democratic society for a wide range of purposes, State Parties can conduct data processing that does not adhere to the principle safeguards that such processing needs to be fair and transparent. State Parties would also not be bound by purpose limitations, the principle of necessity, the duty of care and basic data retention obligations.

Given the wide array of general purposes (Article 11 paragraph 1 litterae a and b) which are allowed to trigger such derogations, it is of crucial importance to arrive at a common understanding when such exceptions would disrespect the essence of fundamental rights and freedoms and when they would not be constituting a necessary and proportionate measure in a democratic society. This will be discussed in further detail in the following sections.

In light of “unprecedented surveillance capacities” (Pierucci and Walter 2021) by national security agencies, one needs to be aware that a broad reading of this exception would leave an extremely high amount of data processing with billions of infringements of fundamental rights and freedoms without the protection of the important safeguards articulated in Article 5 paragraph 4 of the modernised Convention 108.

It should also be noted at the outset, that the exception pertains only to Article 5 paragraph 4 of the Convention, i.e. it does not expand on to the entire Article 5. Thus, all data processing falling under this category of exception must still comply with (a) the proportionality principle as well as the requirement that all stages of the processing reflect a fair balance between all interests concerned, (b) the requirement that data processing can be carried out on the basis of free, specific, informed and ambiguous consent of the data subject or on another valid legitimate basis laid down by law and (c) the requirement that personal data undergoing processing shall be processed lawfully.

The adherence to those principles should be verifiable and according to Article 10 the data “controllers and, where applicable, processors, take all appropriate measures to comply with the obligations of this Convention and be able to demonstrate, subject to the domestic legislation adopted in accordance with Article 11, paragraph 3, in particular to the competent supervisory authority provided for in Article 15, that the data processing under their control is in compliance with the provisions of this Convention.”

These safeguards should be seen as guaranteeing a set of minimum conditions for these types of data processing that would need to be applied in all data processing operations.

3.3.1.3. Article 5, paragraph 4, littera a

- Processed fairly and in a transparent manner

Problem Statement

Fairness and transparency are fundamental principles of data protection, the derogation to which would put the data subject in a genuinely vulnerable position. To counterbalance this and to ensure that the interference with data subjects' privacy and right to data protection that those types of data processing will result in is not arbitrary, clear indications are needed on how to use this exception in a lawful manner.

- Criteria "provided by law"

The law which gives the authorisation not to process personal data "fairly and in a transparent manner" needs to indicate the scope of the discretion allowed to the authorities and the manner of its exercise with "*sufficient clarity, having regard to the legitimate aim of the measure in question, to give the individual adequate protection against arbitrary interference*." The law should have exact terms on how and in which circumstances data processing can be unfair or non-transparent and also until when and where. The conditions of unfair and non-transparent data processing should also be spelled out in a way which is related to the legitimate aim of the processing.

- Criteria "essence of the fundamental rights and freedoms"

This criteria implies that the use of this exception should not lead to the breach of human rights and fundamental freedoms of an individual and in particular should not lead or cause an attempt to his or her right to life and right to human dignity. It shall furthermore not contribute to his or her inhumane treatment, bodily degradation, torture or unlawful discrimination. The use of this exception should be limited in time and space and therefore only serve the legitimate aim of the processing in a necessary and proportionate fashion.

- Criteria "necessary in a democratic society"

The use of the exception should only be a valid and legitimate response to a pressing social need and be proportionate to the legitimate aim pursued. In consequence, fairness and transparency should only be restricted in a way necessary to react to an urgent situation where important public interests are at stake and is proportionate to the legitimate aim pursued. Applying this exception for the entirety of operations, set of operations in an indefinite time or in an unproportionate way would not meet the prerogatives of this criteria.

Summary

The exception from processing personal data in a fair and transparent manner is one of the broadest, and potentially on the most abuse-prone, exceptions under this regime. With this data controllers can be allowed, in specific circumstances, to process personal data in an

unfair and opaque manner which is against the very reason of data protection and the modernised Convention 108 itself.

If we add to this the growing and widening technical and operational capacities by new processing techniques and technologies of data controllers potentially using this exception (law enforcement, financial institutions, national security services, military, immigration services, natural disaster response authorities, cybersecurity institutions and bodies, but even private companies acting in the public interest, etc.) the safeguard of fairness and transparency, if exceptions are not used diligently and narrowly, could disappear from data processing. This will have grave impact in various areas of everyday life and widely affect our open societies.

Question to the delegations: Can you point us to national legislation that has explicitly addressed the scope of this discretion in exemplary fashion?

How to avoid giving unduly wide leeway to State Parties?

Fair and transparent processing of personal data needs to include the following criteria:

- It must be clear and foreseeable under which condition personal data processing will be exempt from the fairness and transparency principle. For this, legal texts governing data processing as well as related legal interpretations should be easily accessible in a concise and understandable way.
- What is more, unfair and opaque data processing must neve take place so as to conceal violations of law.
- In addition, oversight bodies and government agencies are required by law to publish reports that inform parliament and, by extension, the public about the extent to which government agencies are complying with basic safeguards even in the context of this exemption.

3.3.1.4. Article 5, paragraph 4, littera b

- "collected for explicit, specified and legitimate purposes;
- not processed in a way incompatible with those purposes;
- further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes is, subject to appropriate safeguards, compatible with those purposes"

Problem statement

Purpose specification and purpose limitation are equally fundamental principles of data protection which contribute to the preservation of individuals' privacy and which are designed to allow data subjects to remain in control of their personal data. Yet, with this exception, State Parties may waive these essential data protection safeguards which are also meant to rein in abuse and to establish an individual's right to informational self-determination. The use and the conditions for this exception, therefore, have to be as detailed and tailored to the purpose as possible. This may be called in question, for example, if the exception includes the "prevention of breaches of ethics for regulated professions", which, according to the Explanatory Report of the modernised Convention (paragraph 95), can be subsumed under "other essential objectives of general public interest" (Article 11 paragraph 1 littera a). In other

words, might it suffice for State Parties to write a provision into their law that in the interest of preventing breaches of ethics for the profession of, say, high school teachers, states can do away with purpose limitation and use data collected for entirely different purposes, say money laundering investigation, also as a deterrent to prevent breaches of ethics (e.g. biased grading of term papers)?

More generally, in a global datafied context characterised by a constant multiplication of databases the general need for purpose specification and purpose limitation has only become more apparent. If data that was collected in bulk, say for the purposes of informing the government about the economic incentives of its adversaries, is not being purged but re-used for altogether different purposes, say offensive cyber security measures, than this would presuppose a separate authorisation process to ensure that the reuse of such data for a different purpose is lawful and adequately reviewed and supervised. Of course, there are infinite other examples of data reuse possible, not limited to formal government contexts but also more directly tied to the personal data of individual citizens. Add to this the widespread, albeit often legitimate and necessary data collection during global health crises, such as the Covid-19 pandemic. Stricter safeguards need to be in place to prevent State Parties from setting aside the general principle that personal data can only be used for a new purpose if either this is compatible with the original purpose, based on consent, or a specific obligation or function set out in law that specifically allows the reuse of data for a limited other purpose.

Else, this, too, would have grave risks to individuals' privacy and, also in a broader term, the functioning of society.

- Criteria "provided by law"

To use this exception lawfully, a law should describe the situations where the use of such measures could be foreseen. For this, the law needs to account where and when the "explicitness" and "specific nature" of the purposes could be restricted and must not authorise data processing for purposes which would not be legitimate. It would need, furthermore, to give indications as regards the scope and the duration of the exception from the purpose limitation principle.

- Criteria "essence of the fundamental rights and freedoms"

The measures taken under this exception need to be restricted to the extent possible and focused on specific individuals in relation to whom authorities can reasonably suspect that they might represent a risk to one of the public interests mentioned in littera a or b of Article 11, paragraph 1.

- Criteria "necessary in a democratic society"

The lawfulness of actions need to be verified, where possible, by an effective external oversight against its urgency to prevent serious harm or prejudice to important public interests and to their proportionality in light of the legitimate aim pursued.

Summary

Without proper checks and balances, democratic institutions and inclusive processes, the recourse to this exception alone might turn an open society into a surveillance state. If the objective criteria are not taken seriously and in close relation to the purpose for the intended data processing this could lead to the establishment of giant databases storing and interlinking personal data of individuals collected for different purposes.

Ideas or guidance to avoid unduly wide leeway for State Parties

The following remarks and ideas point to areas where further granularity and precision in legal frameworks may go a long way to avoid unduly wide leeway for State Parties. These points, obviously, are not exhaustive in character and interested people from various sectors are invited to contribute to the quest for ways to avoid undue recourse to this exception.

The criterion of hypothetical new collection

The German Constitutional Court's "*criterion of hypothetical new data collection"* may be an interesting aspect to consider here. Accordingly, when assessing the legitimacy of using data for different purposes than originally intended, it depends on whether the corresponding data may also be newly collected for the changed purpose with comparably highly intrusive means according to constitutional standards" (paragraph 216). Thus, it is not only the intended data processing that is of relevance but also the question whether the data could have been lawfully *collected* for that purpose (if it weren't already in the possession of the State Party).

Distinction between collection for information purposes and collection for threat protection purposes

The German Constitutional Court also demanded in May 2020 that future German intelligence legislation distinguish much more carefully between data collection administered for clearly identifiable threat protection purposes and collection administered for the primary purpose of "providing information to the Federal Government to prepare governmental decisions" (BVerfG, 19 May 2020, paragraph 177). Data collection following either rationale ought then to be treated differently as regards data protection standards, especially with regard to international data transfers.

Automated transfer of data in the context of intelligence cooperation

In addition, the German Constitutional Court made a number of requirements for future German foreign intelligence legislation that, we submit, might also be of interest in the context of this particular exception to Article 11 of the modernised Convention 108. For example, as regards potential rights infringements or abuse in the context of "*automated cooperation" with foreign intelligence partners*; e.g. when a national intelligence service opens interfaces to its own raw data stream, to be filtered with the use of "foreign" selectors or when metadata is automatically forwarded abroad. When using "foreign selectors", the Court stipulated that additional safeguards and oversight tasks need to be ensured prior to the transmission of data, such as a

- thorough review of “foreign” search terms and subsequent “hits” prior to transferal
- a separate review according to lists of persons with higher surveillance risk

Independent, written, ex ante authorisation process

More generally, especially as regards the potential waiver that personal data must be collected for an explicit, specified and legitimate purpose, it is important to emphasise the necessity of written, ex ante independent authorisation via warrants and ex-post effective independent oversight for a greater amount of measures than currently in place.

Warrants for foreign-foreign intelligence collection, for example, should include the type of automated processing that can be implemented, specifying its purpose. Stating exactly how a bulk dataset is processed and exploited may enable reviewers to better assess the privacy intrusions that are generated by the respective operation. The level of privacy intrusions and the effects on other fundamental rights may differ based on what kind of examination is performed, and for what aim.

According to the French foreign intelligence law (currently undergoing reform), only the services named in the warrant are allowed to process the collected data. This specification is a protection against subsequent interagency data-sharing. Furthermore, the provision determines that the purpose stated in the warrant may not be changed, and the data may not be used for other purposes. This rule limits the unforeseen spillovers of collected data from one intelligence service to another. Other agencies that may develop an interest in the collected data are prevented from performing unwarranted “searches on top of searches” (Renan 2016) with such a requirement.

In its recent jurisprudence, the European Court of Human Rights demanded that “enhanced safeguards should be in place when strong selectors linked to identifiable individuals are employed by the intelligence services. The use of every such selector must be justified – with regard to the principles of necessity and proportionality – by the intelligence services and that justification should be scrupulously recorded and be subject to a process of prior internal authorisation providing for separate and objective verification of whether the justification conforms to the aforementioned principles.” (ECHR, Centrum för Rättvisa v. Sweden, 25 May 2021, paragraph 269).

Oversight capacity building and training

Internal guidelines, recommendations, toolkits and automated audit programs operated by independent oversight bodies having full access to the operational databases and IT systems of government agencies engaged in data processing should all be considered to keep this exception focused to the strictest minimum. In addition, training and capacity building activities with the participation of supervisory authorities and/or data protection experts would also help to raise awareness and promote expertise.

Especially with regard to enormous amount of data processing by national security agencies, it is important that competent and sufficiently resourced oversight bodies are tasked by law to inspect that “end-to-end safeguards” (ECHR, Centrum för Rättvisa v. Sweden, 25 May 2021) are adhered to in actual practice. This requires access and the design and

implementation of supervisory technology aimed at detecting and rectifying instances of negligence, malfeasance or abuse.[6]

Independent verification of data minimisation

Some national security legislation mandates greater data protection safeguards for certain groups, say medical or religious professionals or journalists, when it comes to their professional communication data. To enforce these types of requirements, agencies carry out data minimisation processes, which are critical for legal compliance. However, these filters are rarely submitted to independent checks for accuracy and reliability.

When it comes to critical information regarding the accuracy of data minimisation processes, many intelligence oversight bodies in Europe often have no choice but to rely on the information that they receive from government or intelligence agencies. Genuine reviews of the accuracy of the filters that agencies use to comply with legal safeguards are rarely conducted. This poses a significant problem; after all, a huge volume of data might be processed incorrectly if the filters are not working properly. Moreover, a wide range of legal provisions need to be upheld by data minimisation procedures; failure to conduct sufficient reviews makes it difficult to ascertain whether said procedures are actually compliant. As such, oversight bodies would be well advised to strive for greater independence in reviewing and verifying data minimisation processes. Parliaments should incorporate provisions into intelligence laws to indicate what filters should achieve during the data collection phase.

Oversight bodies should perform randomized (yet regular) checks to test the accuracy of the data minimisation technology that intelligence services use.

- Due diligence reviews on stored data: This requires unfettered access to the stored data that is kept after the minimisation process. The results of these probes should be tracked over time so that oversight bodies can calculate a general error rate of an intelligence agency's filtering veracity. This would then enable the executive and lawmakers to make evidence-based decisions about the usefulness and feasibility of certain legal data protection categories.

- Precise and realistic minimisation rules: Taking independent reviews and technical feasibility as a basis, lawmakers may introduce clear legal requirements indicating what filters need to achieve and whether an error rate is permissible.

Automated internal compliance systems

In addition to reviews of data minimisation by independent supervisory authorities, the executive branch of government and its agencies (ie. executive oversight or internal controls) should make sure that computerised systems are in place for checking and searching for potentially non-compliant uses of the national security agencies' systems and premises. For example, when an authorised person selects a particular communication for examination, this person must demonstrate that the selection is necessary and

[6] See, for example, Vieth and Wetzling (2019) for a tentative agenda for data-driven intelligence oversight.

proportionate; this process is subject to internal audit." (FRA 2017, p. 59 and UK Home Office 2017, p. 47)

3.3.1.5. Article 5, paragraph 4, litterae c - e)

- adequate, relevant and not excessive in relation to the purposes for which they are processed (littera c)
- accurate and, where necessary, kept up to date (littera d)
- preserved in a form which permits identification of data subjects for no longer than is necessary for the purposes for which those data are processed (littera e)

Problem statement

Data quality is not only a data protection safeguard but a prerogative for effective and efficient data processing. Although, at an early stage of an investigation for example, some leeway could be required, the exception would need to be gradually phased out when approaching the final stage of an investigation.

- Criteria "provided by law"

The law needs to determine the details of this exception in terms of form and content. It should explicitly state that one, several or all data quality requirements are exempted. It needs to ensure that data subjects understand what to expect in a given situation.

- Criteria "essence of the fundamental rights and freedoms"

The measures taken should not result in the deprivation of the totality of the right to privacy or to data protection but should be limited in scope. It should not result in the creation of a database on a large part of the population to be kept without specific ongoing legitimate investigations or reasonable suspicion without any time limitation and specific search terms subject to an individual warrant from independent supervisory authority. Nor should this lead to instances where personal data are processed in bulk without specific search criteria and retained for an indefinite amount of time.

- Criteria "necessary in a democratic society"

Any operations carried out by using this exception should be subject to effective independent oversight, possibly also subject to judicial authorisation. Any derogation from the data quality requirements should have a demonstrable solid reason which is in direct contact with the risk of harm, prejudice that the operation intends to prevent. The risk should be high, imminent and in relation with important public interests.

Summary

This exception is used, at best, when it is temporarily limited. Moreover, an unnecessarily wide scope of this exception could undermine the entire purpose of the data processing safeguards. Hence it is important that State Parties are obliged to justify for each phase of an operation (consisting of several data processing phases) how they honour the necessary and proportionate criteria in actual practice.

How to avoid giving unduly wide leeway to State Parties?

Especially as regards littera c of Article 5 paragraph 4 of the modernised Convention, the recent jurisprudence by the European Court of Justice in the Schrems II case but also its judgments (Case C-623/17) and the joined Cases C-511/18, C-512/18 and C-520/18) of 6 October 2020 can be very useful for further guidance. This is because of the strict limits these judgements entail on permissibility of national security measures providing for access and retention to personal data in the field of electronic communications.

For example, the CJEU finds that

> national legislation requiring providers of electronic communications services to disclose traffic data and location data to the security and intelligence agencies by means of general and indiscriminate transmission exceeds the limits of what is strictly necessary and cannot be considered to be justified, within a democratic society, as required by Article 15(1) of Directive 2002/58.

In addition, one might find additional guidance in the European Commission's

- adequacy determinations which are meant enable the free flow of data with trust between the EU and the United Kingdom

Finally, the following safeguards would also help to ensure that the exception for State Parties to be exempt from Article 5 paragraph 4 obligations would not defy the very purpose of this Convention:

- Personal data is protected by an obligation to tag personally identifiable information (PII) and an obligation to safeguard against unauthorised access, destruction, use, modification or disclosure.
- Personal data is accessed and examined only by personnel who are authorised to do so, and who have received appropriate training on applicable limitations and restrictions.
- Personal data is only shared with or disclosed to other people or entities to the extent permitted by law and only for authorised purposes.

As regards the latter, the German Constitutional Court has mandated a "rule of law assurance" obligation upon the government prior to sharing personal data with foreign partners. This, too, appears to be a relevant additional safeguard that the European Court of Human Rights in its 25 May 2021 decisions (Big Brother Watch and Others v. The United Kingdom, 25 May 2021; Centrum för Rättvisa v. Sweden, 25 May 2021) has also expressed in very similar terms. The Constitutional Court called for better safeguards in legislation as regards the obligation of the executive to seek a reliable "rule of law assurance" from its foreign cooperation partners as regards their use of shared data.

> "This does not mean that institutional and procedural legal precautions must be guaranteed in the foreign legal system according to the German model; in particular, the formal and institutional safeguards required by data protection law for German authorities do not have to be in place. In this sense, it is necessary to ensure an adequate level of data protection in the recipient

country for the handling of the data transmitted. *In this respect, particular consideration must be given to whether the limits imposed on the use of the data - as communicated at the time of transmission - by purpose limitation and deletion obligations as well as fundamental requirements for control and data security are at least generally observed*. This assessment is based on national legislation and the international obligations of the recipient state and their implementation in daily practice (BVerfG, 19 May 2020, paragraph 141, 220 <344 f. marginal no. 334 f.> with further references.)."

As regards, littera d, and the data quality, one could demand that much more resources are being invested in the design and implementation of supervisory technology that would allow oversight bodies to

- monitor stored data for filter errors
- conduct more systematic pattern identification
- investigate and report on data deletion[7]

Duty of care as regards data processing, including the use of algorithms

In this regard it might also be noteworthy that the Dutch Intelligence Act imposes a general duty of care as regards data processing upon the heads of the security and intelligence services. It includes adequate measures against data breaches and ensures the validity and integrity of processed data. The Dutch intelligence services are also obliged to British, take sufficient measures to safeguard the quality of data processing, including the algorithms and (behavioral) models used. By covering algorithms and models, the legislator intends to take a technology-neutral approach The law requires all data to be examined as soon as possible to determine whether it is relevant to the operation for which it was obtained (Article 48). Data that has been determined not to be relevant shall be immediately destroyed. After one year, all data that has not been examined for relevance must also be destroyed. Taken together, these provisions create a legal umbrella that protects the privacy and the quality of the data. The Dutch oversight body CTIVD has the competence to monitor the measures taken to this effect and to control the design of the systems deployed to comply with these duties.

As regards the retention and deletion requirements, it needs to be decided on a case by case basis whether an obligation to delete personal data can align with the need to maintain the integrity of data that may arise when such data is required as evidence in court proceedings or for purposes of oversight and redress.

3.3.2. Article 7 paragraph 2: Notification of a personal data breach to the supervisory authority

3.3.2.1. Description

This exception provides the possibility for State Parties to enact legislation which exempts data controllers that are processing personal data for purposes specified in the first regime of exceptions (Article 11 paragraph 1 litterae a and b) to notify "*without delay, at least the competent supervisory authority within the meaning of Article 15 of this Convention, of those*

[7] See also (Vieth and Wetzling 2019) for a number of other ideas that might be turned into an agenda for more data-driven oversight.

data breaches which may seriously interfere with the rights and fundamental freedoms of data subjects."

In other words, governments may be entitled, in some circumstances and only when the safeguards of Article 11 paragraph 1 are being met, to withhold information about data breaches to competent supervisory authorities.

3.3.2.2. Problem statement

The rationale behind notifying the supervisory authority in case of a data breach which "*may seriously interfere with the rights and fundamental freedoms of data subjects"* is to minimise and prevent harm that such an event might cause to the rights and interests of data subjects whose data are involved in the data breach. In addition, notifications to supervisory authorities may also lead to further investigations of malfeasance which is important for public accountability.

Yet if this exception is too broad in its definition, competent supervisory authorities can be stone-walled quite conveniently.

It remains also an open question who, exactly, determines whether breaches may seriously interfere with the rights and fundamental freedoms of data subjects on the basis of what criteria? As with many other such decisions, we would encourage further discussion as to how such determinations can be subjected to independent and effective review? At the very minimum this would require scrupulous documentation for the purpose of internal and external reviews.

- Criteria "provided by law"

To reply to this condition the law needs to specify clearly and exhaustively data controllers that fall under the scope of this exception. The law should give enough information on all aspects of the exception and what it entails in practice and more importantly on who will be the responsible institution or body to handle the data breach and the underlying policy which would prevent or minimise harm to individuals.

- Criteria "essence of the fundamental rights and freedoms"

No other measure, which should be put in place to mitigate the risk and to prevent harm of an intended data processing might cause to the rights and freedoms of a data subject also in case of a data breach according to Article 10 should be covered by this exception, only the obligation to notify, or to notify without delay the supervisory authority. Data controllers should have publicly available policies in place which lay out procedures and processes to protect human rights and fundamental freedoms of data subjects.

- Criteria "necessary in a democratic society"

There should be factual reasons or clear and democratic policy determinations underpinning the choice to use this exception. As detailed above, the role of supervisory authorities in handling serious data breaches are to be meant in a supporting nature to prevent or minimise harm for data subjects in an unsecure and often uncontrolled, or even uncontrollable situation. There should be a high and urgent compelling social need to be demonstrated why such support should not be used. Any general or broad reference to classified information or the

disclosure of such to the supervisory authority would probably not meet those criteria, the latter also being part of the public administration of the State Party.

Summary

Supervisory authorities are important supporting authorities in handling serious data breaches. Without the involvement of the supervisory authority, these measures, which should be set forth by law, have to be taken on by the data controller alone and under its full responsibility. Using this exception therefore needs careful consideration also in view of expertise and competences at and of data controllers being subject to such measures in handling data breaches also in a cross-border situation (most of the time, this would require the cooperation that is foreseen for supervisory authorities in Article 17).

How to avoid giving unduly wide leeway to State Parties?

In this regard, one could discuss:

- a Memorandum of Understanding with the data protection authorities on their involvement if data breaches happen
- joint elaborations of data breach response plans, operations, contingency plans
- clearer policy on cross border data transfer regimes
- closer and more structured cooperation with cybersecurity authorities
- partnerships with domain name service registrars and registries as well as hosting providers, etc.

3.3.3. Article 8 paragraph 1: Transparency obligation

3.3.3.1. Description

This exception allows State Parties to derogate from the provisions of Article 8 paragraph 1 when the conditions of Article 11 paragraph 1 are being met.

Article 8 paragraph 1

1. Each Party shall provide that the controller informs the data subjects of:
   a. his or her identity and habitual residence or establishment;
   b. the legal basis and the purposes of the intended processing;
   c. the categories of personal data processed;
   d. the recipients or categories of recipients of the personal data, if any; and
   e. the means of exercising the rights set out in Article 9, as well as any necessary additional information in order to ensure fair and transparent processing of the personal data.

3.3.3.2. Problem Statement

Transparency regarding data processing is one of the oldest and most crucial principles of privacy and personal data protection. Without having adequate information on which actor is doing what, where and when with personal data, data subjects would be neither in a position of autonomy and integrity, nor be able to fully exercise their right to informational self-

determination. This way their very dignity might be impacted. However, as the right to privacy and to the protection of personal data is not an absolute right, exceptions from this principle are possible. Refraining from transparency regarding personal data processing is only permissible respecting the conditions set forth in Article 8.2 of the European Convention of Human Rights and further detailed in Article 11 of the modernised Convention 108.

- Criteria “provided by law”

The law needs to be very specific on which data controller, for which data processing operations or set of operations could use this exception and with regard to which element of Article 8, paragraph 1. It needs to be easily accessible and understandable and should also determine the scope of application of this exception exhaustively. Sunset clauses could be considered for the use of exceptions.

- Criteria “essence of the fundamental rights and freedoms”

This exception should not involve or imply any exemption from other rule of law or procedural safeguards such as the proportionality and necessity of measures, right to fair trial, right to defence, egality of arms, right to know the legal charges, and where applicable the probable cause for an investigation or other type of operation. The law allowing such exceptions should be considered in light of its impact on other human rights and fundamental freedoms (such as the right to freedom of expression, right to freedom of thought, religion, assembly, etc.) and also to democratic processes. It should allow the use of exceptions only to the extent to which they do not infringe or harm unnecessarily or in an unproportionate way other human rights and fundamental freedoms or democratic processes (such as political oversight of national security services).

- Criteria “necessary in a democratic society”

The exception should only be used where it is necessary and proportionate with regard to the legitimate aim pursued in which it needs to take into account the gravity of risk to society the measure intends to prevent or mitigate, the both geographical and temporary scope of operations intended, the possible repetitive or recurrent nature of the risk, the size of the population possibly impacted by it and the clear categories of terms for searches, tracking, profiling etc. Those measures should be subject to prior internal authorisation and effective ex-post review.

Summary

In many cases not giving out information on the processing can be as revealing as giving it to data subjects. Absolute secrecy should not be the norm. Furthermore, it should not impact on other rule of law conditions and safeguards (such as fair trial, equality of arms, legality of a criminal charge, right to know all legal charges, etc.).

How to avoid giving unduly wide leeway to State Parties?

In this regard one should develop tailored measures to better address the concerns and open questions raised above. In part, this could be rectified by

- Clear policy on transparency and on access to information

- Coupling the use of this exception to due regard to the appropriate level of protection of individuals especially when the processing involves cross-border transfer of data
- creating an obligation to actively issue notifications when it no longer jeopardises the purpose of the processing
- creating an obligation to take individuals' other rights and interests into account by human rights impact assessment when determinations about a data breach are being made
- Criteria should be established so as to ensure that the use of this exception cannot be used to conceal violations of the law.
- Government agencies should be required to report publicly on their use of this exception.
- Transparency goes further. When certain transparency is not possible this needs to be compensated.

3.3.4. Article 9: Rights of the data subject

3.3.4.1. Description

This exception allows Parties to the Convention to derogate from the provisions regulating the rights of data subjects. Parties to the Convention can thus enact legislation regarding the processing of data in the context of

the purposes listed in Article 11, paragraph 1, litterae a and b (first regime of exceptions)

- "a. the protection of national security, defence, public safety, important economic and financial interests of the State, the impartiality and independence of the judiciary or the prevention, investigation and prosecution of criminal offences and the execution of criminal penalties, and other essential objectives of general public interest;
- b. the protection of the data subject or the rights and fundamental freedoms of others, notably freedom of expression."

without according data subjects the following rights:

- *not to be subject to a decision significantly affecting him or her based solely on an automated processing of data without having his or her views taken into consideration;*
- *to obtain, on request, at reasonable intervals and without excessive delay or expense, confirmation of the processing of personal data relating to him or her, the communication in an intelligible form of the data processed, all available information on their origin, on the preservation period as well as any other information that the controller is required to provide in order to ensure the transparency of processing in accordance with Article 8, paragraph 1;*
- *to obtain, on request, knowledge of the reasoning underlying data processing where the results of such processing are applied to him or her;*
- *to object at any time, on grounds relating to his or her situation, to the processing of personal data concerning him or her unless the controller*

demonstrates legitimate grounds for the processing which override his or her interests or rights and fundamental freedoms;

- *to obtain, on request, free of charge and without excessive delay, rectification or erasure, as the case may be, of such data if these are being, or have been, processed contrary to the provisions of this Convention;*
- *to have a remedy under Article 12 where his or her rights under this Convention have been violated;*
- *to benefit, whatever his or her nationality or residence, from the assistance of a supervisory authority within the meaning of Article 15, in exercising his or her rights under this Convention*

provided that this

- respects the essence of fundamental rights and freedoms
- constitutes a necessary and proportionate measure in a democratic society
- is provided by law

3.3.4.2. Problem Statement

Data subject rights are the basis for the respect of the right to privacy and informational self-determination. As mentioned earlier, those rights are however not absolute rights and therefore exceptions are permissible if higher interests are at stake and the conditions in Article 11, paragraph 1 are respected.

In our view, more precision and granularity are needed regarding the exempt literae a, b, f and g relating to automated data processing, notification duties and the right to effective remedy.

3.3.4.3. The right of a data subject "*not to be subject to a decision significantly affecting him or her based solely on an automated processing of data without having his or her views taken into consideration;" (Article 9, paragraph 1, littera a)*

Decision-making based on automated processing of data in the context of the purposes listed in Article 11, paragraph 1, litterae a and b entails high risks of severe infringements with fundamental rights and freedoms. Nevertheless it can be permissible under the following criteria:

- Criteria "provided by law"

Decision-making based on automated data processing should be governed by clear and precise legislation regulating its scope and application. It should impose minimal safeguards to ensure that the essence of fundamental rights and freedoms as well as the necessity and proportionality criteria are respected.

- Criteria "essence of the fundamental rights and freedoms"

The law allowing such exceptions should be considered in light of its impact on other human rights and fundamental freedoms (such as the right to freedom of expression, right to freedom of thought, religion, assembly, etc) and also to democratic processes. It should allow the use of exceptions only to the extent to which they do not infringe or harm unnecessarily or in an unproportionate way other human rights and fundamental freedoms or democratic processes.

Automated processing always includes a margin of error as well as a risk of unintentional discrimination. We believe, to mitigate those risks, and to conserve the essence of fundamental rights and freedoms, a human-in-the-loop safeguard should be included when concrete action is to be taken against a data subject as a consequence of a decision based on automated data processing. In other words, before taking action against a data subject on the basis of automated data processing, the decision should be cross-checked by a human person.

- Criteria "necessary and proportionate in a democratic society"

Decision-making based solely on automated processing and that is significantly affecting the data subject should only be permissible under the condition of an urgent social need. It should moreover only take place when no less intrusive alternative is available.

Relevant case law by the ECHR has pointed out that the degree of interference with Article 8 rights increases depending on the stage of data processing. In the case of bulk intelligence collection, the Court identified the following four stages:

> "(a) the interception and initial retention of communications and related communications data (that is, the traffic data belonging to the intercepted communications);
> (b) the application of specific selectors to the retained communications/related communications data;
> (c) the examination of selected communications/related communications data by analysts; and
> (d) the subsequent retention of data and use of the "final product", including the sharing of data with third parties." (Centrum för Rättvisa v. Sweden, 25 May 2021, paragraph 239)

In order to satisfy the necessity and proportionality requirements regarding decisions based on automated data processing, we believe that a similarly graded approach is warranted. The stage of data processing and the subsequent severeness of fundamental rights interference should be taken into account.

3.3.4.4. The right of data subjects "*to obtain, on request, at reasonable intervals and without excessive delay or expense, confirmation of the processing of personal data relating to him or her, the communication in an intelligible form of the data processed, all available information on their origin, on the preservation period as well as any other information that the controller is required to provide in order to ensure the transparency of processing in accordance with Article 8, paragraph 1"(Article 9, paragraph 1, littera b)*

- Criteria "provided by law"

The conditions under which notifications can be omitted should be laid down in law in a clear and sufficiently detailed manner. Legislation needs to be accessible and written in such a way that foreseeability can be ensured.

- Criteria “essence of the fundamental rights and freedoms”

Subsequent notification after personal data processing is crucial to ensure effective remedy for data subjects – that is a fundamental requirement to the respect of fundamental rights and freedoms. However, in its recent jurisprudence, the ECHR has laid out that notification duties are not necessary “where the courts’ jurisdiction does not depend on notification to the interception subject that there has been an interception of his or her communications.”(Centrum för Rättvisa v. Sweden, 25 May 2021, paragraph 271) In other words, where remedy is possible without prior proof of affectedness, governments might abstain from the duty of notification.

To guarantee the effectiveness of the remedy, the nature and powers of the body before which remedy is possible are central. The ECHR demands that the body, “while not necessarily judicial, is independent of the executive and ensures the fairness of the proceedings, offering, insofar as possible, an adversarial process. The decisions of such authority shall be reasoned and legally binding with regard, inter alia, to the cessation of unlawful interception and the destruction of unlawfully obtained and/or stored intercept material.” (Centrum för Rättvisa v. Sweden, 25 May 2021, paragraph 273)

- Criteria “necessary and proportionate in a democratic society”

Exceptions from notification duties should only be permissible as a response to a pressing and legitimate social need and when access to remedy is guaranteed independently of proof of affectedness.

3.3.4.8. The right of data subjects “to have a remedy under Article 12 where his or her rights under this Convention have been violated” and “to benefit, whatever his or her nationality or residence, from the assistance of a supervisory authority within the meaning of Article 15, in exercising his or her rights under this Convention”*(Article 9, paragraph 1, litterae f and g)*

Without access to remedy, individual’s fundamental rights and freedoms are reduced to mere lines on paper. It is questionable how the exemption of litterae f and g can be compatible with the requirement to respect the “essence of fundamental rights and freedoms,” especially as they exclude access to remedy and assistance by a supervisory authority.

ECHR jurisprudence has confirmed on several occasions that each individual should have the right to remedy and - independently of nationality or residence - access to recourse to the supervisory authority (e.g. Centrum för Rättvisa v. Sweden, 25 May 2021, paragraph 271).

In the instances where the enforcement of data subject’s rights is significantly reduced in actual practice, if not downright impossible (for instance when the data subject in bulk collection for foreign intelligence purposes is a non-national abroad), the focus should lie on effective and independent oversight to also serve as a compensatory measure (BVerfG, 19 May 2020, paragraph 268-272). The amended German Federal Foreign Intelligence legislation (BND Act) now places strategic surveillance of non-nationals under judicial oversight within the newly created *Unabhängiger Kontrollrat* (Independent Control Council).

3.4. Additional exceptions allowed for processing activities for national security and defense purposes (Article 11, paragraph 3)

In addition to the four exceptions listed in Article 11 paragraph 1, a second regime of exceptions is provided for in Article 11 paragraph 3. It allows State Parties three more exceptions provided the conditions and safeguards are being respected. This will be discussed in further detail in this section. It adopts the same approach but adds to the discussion the important safeguard listed in the last sentence of Article 11:

> *"This is without prejudice to the requirement that processing activities for national security and defence purposes are subject to independent and effective review and supervision under the domestic legislation of the respective Party."*

3.4.1. Article 4, paragraph 3: evaluation mechanism

3.4.1.1. Description

Parties to the modernised Convention 108 commit actively to the evaluation of their compliance with their various commitments under this convention. However, the first exception mentioned in Article 11 paragraph 3 means that Parties may derogate from this obligation as regards processing activities for national security and defence purposes, as long as this exception is

- provided for by law
- constitutes a necessary and proportionate measure in a democratic society

In addition, this exception must also honour the requirement that processing activities for national security and defence purposes are subject to independent and effective review and supervision under the domestic legislation of the respective Party.

If these conditions are met, then State Parties can be exempt from the obligation to

- *allow the Convention Committee provided for in Chapter VI to evaluate the effectiveness of the measures it has taken in its law to give effect to the provisions of this Convention; and*
- *to contribute actively to this evaluation process*

3.4.1.2. Problem Statement

A significant number of government's data processing can, and will be exempt from the Convention Committee's mandate to evaluate the compliance of the State Parties with their various commitments under this convention.

Parties to the Convention would need to write specific provisions into their national security and defence legislative frameworks that they intend to make use of the exception under Art. 11 paragraph 3 when it comes to processing activities for national security and defence

purposes. They might also need to provide, at least in explanatory material, a justification as to why a general recourse to this exception in their legal framework constitutes a necessary and proportionate measure in a democratic society. Lastly, they may only do so provided that the processing activities for national security and defence purposes are subject to independent and effective review and supervision under the domestic legislation of the respective Party.

How to avoid giving unduly wide leeway to State Parties?

In order for this exception not to open the door to widespread disregard for the obligations under this convention, much depends on the caveat that "processing activities for national security and defense purposes are subject to independent and effective review and supervision under the domestic legislation of the respective Party"

The de jure and de facto conditions for independent and effective review and supervision are discussed in Section 3.4.3 (see also Annex Section 7.1.1.13). Given that this exception does not relate to Article 4 paragraph 1 of this Convention, we recall here that Parties to the Convention are generally obliged to ensure that their national law gives effect to the provisions of this Convention and to secure their application. In this context this could mean an obligation to include into the national legal frameworks governing the supervisory authorities an obligation for those bodies to perform their independent and effective review of processing activities for national security and defence purposes also in a manner that tests the government's compliance with the various obligations under the modernised Convention 108.

3.4.2. Article 14 paragraphs 5 and 6: international transfer of data and data protection authority's scope of authority

3.4.2.1 Description

As regards the international transfer of personal data in the context of processing activities for national security and defense purposes, this exception allows that each Party may derogate from the principle safeguard that

- their national competent supervisory authority (within the meaning of Article 15 of this Convention) is provided with all relevant information concerning the transfers of data regarding
  - ad hoc or approved standardised safeguards provided by legally-binding and enforceable instruments adopted and implemented by the persons involved in the transfer and further processing.
  - the specific interests of the data subject require it in the particular case; or
  - prevailing legitimate interests, in particular important public interests, are provided for by law and such transfer constitutes a necessary and proportionate measure in a democratic society

- the supervisory authority is entitled to request that the person who transfers data demonstrates the effectiveness of the safeguards or the existence of prevailing legitimate interests and that the supervisory authority may, in order

to protect the rights and fundamental freedoms of data subjects, prohibit such transfers, suspend them or subject them to conditions.

The exception needs to be

- provided for by law
- and constitute a necessary and proportionate measure in a democratic society to fulfill such aim,

Moreover, processing activities for national security and defence purposes need to be subject to independent and effective review and supervision under the domestic legislation of the respective Party.

3.4.2.2. Problem Statement

Transborder transfers of personal data in the context of national security and defence remains a domain particularly vulnerable to oversight and accountability gaps in many democracies. Intelligence agencies and other government bodies in the national security and defence context usually impose strong restrictions as to who may have access to the shared data in order to protect their sources and mitigate the risk that the data they share with foreign partners is misused. However, restrictions under the so-called "Third Party Rule" or "Originator Control Principle" should not mean that shared information is fully excluded from oversight. In this regard, we invite delegations to consider the findings of the German Constitutional Court in its decision 1 BvR 2835/17 (19 May 2020):

> "292. cc) Oversight must not be obstructed by the third party rule. In designing the oversight bodies and setting out requirements regarding agreements between the Federal Intelligence Service and other intelligence services, the legislator must ensure that the Federal Intelligence Service cannot prevent oversight by invoking the third party rule.
>
> Nevertheless, the third party rule is a rule of conduct that is based on agreements with foreign intelligence services and generally recognised by all intelligence services; according to this rule, based on informal arrangements, intelligence obtained from foreign intelligence services may not be shared with third parties without the consent of the intelligence service in question (cf. BVerfGE 143, 101 <150 paragraph 162; 151 paragraph 164>). The Federal Government can also invoke this rule, insofar as it has given assurances on the basis of which intelligence was shared by a foreign intelligence service and the question of whether this intelligence can be shared with "third parties" arises; for example, the Federal Government refused to provide certain information to a committee of inquiry of the Bundestag, i.e. a third party, on the grounds that it had given such assurances to the United States of America (cf. BVerfGE 143, 101 <152 paragraph 167; 155 et seq. paragraph 176 et seq.>). The bodies conducting the constitutionally required comprehensive oversight of the Federal Intelligence Service must be designed as independent oversight bodies that are strictly committed to secrecy and not integrated into Parliament and its political communication channels, so as to ensure that the third party rule cannot provide grounds for refusing to cooperate with them. There is no general definition setting out whether an oversight body must be considered a "third party" within the meaning of the third party rule; rather, this is

> determined on the basis of its organisational design and agreements between intelligence services (cf. BTDrucks 18/12850, pp. 98 and 99). The third party rule is an administrative practice that is not legally binding, but is merely based on agreements with other intelligence services; it is thus flexible and the Federal Government can influence its practical significance ([…]). The Federal Government and the Federal Intelligence Service do remain bound by the assurances they have given. However, in the future, it must be ensured, through the way the oversight bodies are designed and through changes in agreements with foreign services, that the bodies conducting legal oversight are no longer considered "third parties" (cf. also European Commission for Democracy through Law [Venice Commission], Report on the Democratic Oversight of Signals Intelligence Agencies, CDLAD[2015]011, p. 5 [no. 13]; Council of Europe, Parliamentary Assembly, Resolution 1838 [2011], p. 2 [no. 7]; Council of Europe, Commissioner for Human Rights, Democratic and effective oversight of national security services, 2015, p. 13 [Recommendation no. 16]).

In light of this, it seems questionable to us how to reconcile the present exception with the requirement in Article 11, paragraph 3 that "processing activities for national security and defence purposes need to be subject to independent and effective review and supervision under domestic legislation of the respective Party", unless the supervisory authorities named by each State Party under Article 15, paragraph 1 are not identical to those referred to in the sentence in Article 11, paragraph 3 (see also the discussion also in section 3.4.3 below).

Under the present exception, parties to the Convention would be allowed to not grant supervisory authorities provided for by State Parties under Article 15 paragraph 1 access to all relevant information concerning data transfers in the remit of national security and defence. However, given that no effective oversight can be guaranteed when supervisory authorities do not have comprehensive access to information necessary to fulfil their duties (ECHR, Centrum för Rättvisa v. Sweden, 25 May 2021, paragraph 270), at a minimum this requires that at least one other oversight entity in each State Party does have such access and the full palate of oversight powers referred to in Article 15 (see also section 3.4.3 below).

In addition, per the present exception, supervisory authorities cannot request proof of effectiveness of the safeguards and the existence of legitimate interests for data transfers. It is unclear how effective review, and especially the necessity and proportionality test, can be guaranteed when the supervisory body does not have the possibility to get access to information regarding the safeguards in place and the existence of a legitimate interest (Centrum för Rättvisa v. Sweden, 25 May 2021, paragraph 269). Again, in the absence of such powers by another oversight body at the national level, this provision risks to be incompatible with relevant ECHR case law as well as national and EU-law, as explained below.

By the exemption of paragraph 6 of Article 14, supervisory authorities also lose the power to issue binding decisions on data transfers in the context of national security and defence, be it their suspension or their subjection to certain conditions in order to protect the rights and fundamental freedoms of data subjects. Without binding powers it appears questionable to us how the rule of law and the respect of necessity and proportionality, that are fundamental in a democratic society, and a prerequisite for public trust, can effectively be ensured. In this

regard, we point to §52(4) of the German legislation on foreign intelligence (BND Act) which bestows such a binding power upon the Independent Control Council.

- Criteria “provided for by law”

Supervisory authorities shall, as a general rule, have access to all information that they consider relevant for their control activities. National law needs to ensure that processing of data in all contexts is supervised by a competent authority. The competences and powers (or lack thereof) of different oversight bodies need to be laid down in law in a clear and accessible manner and in a way that oversight gaps are precluded.

- Criteria “only to the extent that it constitutes a necessary and proportionate measure in a democratic society to fulfil such aim”

Withholding relevant information from supervisory authorities, as well as depriving them from binding powers, with regard to international data transfer in the remit of national security and defence should only be a valid and legitimate response to a pressing social need and be proportionate to the legitimate aim pursued. Applying this exception for the entirety of operations, set of operations in an indefinite time or in an unproportionate way would not meet the prerogatives of this criteria.

It has to be noted here, that in order to be able to assess the necessity and proportionality of the action taken, the supervisory authority needs access to all relevant information. The ECHR demands in this regard that “detailed records from every stage of the process” are kept for the supervisory authorities. (Centrum för Rättvisa v. Sweden, 25 May 2021, paragraph 270) To ensure proportionality and necessity of processing activities, effective review and supervision are crucial. This is reflected in relevant case law by the ECHR that demands that all data processing activities, including onward transmission, be supervised by an independent authority that is sufficiently robust to “*keep the “interference” to what is “necessary in a democratic society*”

- Criteria “This is without prejudice to the requirement that processing activities for national security and defence purposes are subject to independent and effective review and supervision under the domestic legislation of the respective Party.”

Supervision shall generally apply to all data processing activities, including transborder data transfers in the context of national security and defense (Centrum för Rättvisa v. Sweden, 25 May 2021, paragraph 325). In Rättvisa v. Sweden, paragraph 190, the ECHR clarifies that “supervision powers [...] should be exercised at the stages [...] where information is communicated to national authorities, foreign Governments or international organisations.” See more on effective oversight in the discussion in section 4.4.3.

How to avoid giving unduly wide leeway to State Parties?

Although transborder data transfers in the field of national security and defense are an important source of information, they are also a domain where the risk for accountability gaps and abuse is particularly high. The following safeguards should therefore be considered to ensure the respect of fundamental human rights and principles of democratic governance.

Effective safeguards and assurances for data sharing

Transferring data to international partners evidently always entails a loss of control over the data. Governments need to make sure that the data is not used for illicit purposes and the transfer does not undermine fundamental rights and freedoms. Effective guarantees and safeguards are needed to ensure the respect for human rights. A comprehensive risk assessment should take place prior to data transfers in order to ensure that the receiving country will not use the shared data for human rights abuses. Cooperation agreements that include caveats on how the data can be used should also be considered.
These requirements are common practice in several member States and also reflected in relevant national jurisprudence. The German Constitutional Court, for instance, established a mandatory obligation upon the executive (subject to oversight) to seek a "rule of law assurance" to ensure the respect of human rights as well as an adequate level of data protection in the recipient country (BVerfG, 19 May 2020, paragraph 236-238).

In order to be effective, such safeguards need to be overseeable by an independent supervisory authority (see also the discussion in section 4.4.3 below).

Shared data needs to be overseeable

Under the so-called "Third Party Rule" (or Originator Control Principle), national oversight bodies were traditionally often considered a third party which made it impossible for them to review (the processing of) shared data. This may have led to instances of 'collusive delegation' whereby core democratic principles were purposefully undermined by delegating powers to collect particular information to international partners as a means to circumvent domestic restrictions. More generally, as supervisory authorities rarely engage in direct cooperation with one another and given that there are, to date, few if any joint investigations, data transfers can easily elude nationally mandated review. However, the interference with fundamental rights is greater the more the data is shared with other agencies. Therefore, more needs to be done to avoid oversight and accountability gaps and we welcome recent case-law (see below) that has established more clearly that shared data should not be excluded from review.

One a national level, the ECHR demanded that States are prevented from circumventing domestic law or Convention obligations through intelligence sharing (Big Brother Watch and Others v. The United Kingdom, 13 September 2018). This has also been the general tenor in recent national jurisprudence by the German Constitutional Court on the Federal Foreign Intelligence Law (BVerfG, 19 May 2020) which ruled that "it must be ensured that oversight is not hindered by the 'Third Party Rule'" (BVerfG, 19 May 2020, paragraphs 282, 292, 294). Oversight bodies must therefore be designed in such a way that they do not fall under the 'Third Party Rule.'

On an international level, Parties should be encouraged to engage in oversight cooperation in order to mitigate accountability and oversight gaps. Examples are the European Intelligence Oversight Working Group and the Five Eyes Intelligence Oversight and Review Council (FIORC). This is also compatible with the requirements in Article 17 of the Convention on supervisory authority co-operation, provided the supervisory authorities in question include also those mentioned in Article 11, paragraph 3.

Multilateral oversight for joint intelligence databases

Transnational threats prompt closer trans-border cooperation among intelligence services, not least for neighboring countries. Intelligence data – both unevaluated and evaluated – is therefore not just shared bilaterally, but also stored in joint intelligence databases for different threats and purposes. Typically, joint databases are run multilaterally, with all participating services adding and accessing data. The European Counter Terrorism Group (CTG), for example, runs a database that facilitates the multilateral exchange of evaluated data on individuals who have traveled to and returned from certain conflict areas.

A 2018 report by the Dutch intelligence oversight body CTIVD concluded that safeguards for the protection of fundamental rights were not sufficiently addressed and recommended setting up additional safeguards and multilateral controls. This is a very important recommendation, we believe. Legal frameworks should account for the joint responsibility that governments have for joint databases, even if they are not hosted on their territory. Furthermore, as acknowledged by the Dutch government, there is a pressing need to ensure effective oversight over joint databases, possibly in the form of multilateral oversight.

> "Bearing joint responsibility also requires joint, multilateral oversight. After all, the different national oversight bodies will each face the question whether the service they are overseeing gives sufficient implementation to the joint responsibility that the service bears. National oversight alone is insufficient in this case. The government recently agreed that there must be multilateral oversight. Right now, there is no such multilateral oversight within the CTG. To an extensive degree, the oversight body will assess the exchange of data and its further processing on the basis of its own mandate and within its own national legal framework. This does not alter the fact that there is a joint aspect here that requires further embedding. For this reason, it is necessary that the safeguard of independent, adequate and effective joint oversight is included in a common data protection framework for the CTG database.
>
> [...] A more far reaching form of cooperation between the oversight bodies would therefore be necessary, so that such limitations may be put aside. This would need to be embedded in a common data protection framework. Another option would be to explicitly divide the oversight tasks, with one or a few oversight bodies being charged with organising the joint oversight. A parallel can be drawn with the relation between the "controller" and the "processor" under data protection law. One or more oversight bodies could be assigned the responsibility to perform the oversight on behalf of all of them. Again a common framework or instruction would have to form the basis for this. The controllers retain the primary responsibility in this. A third option would be to institute overarching, international oversight. To that end a new international oversight body would have to be created, to which certain oversight powers are assigned. This is the most far-reaching option and would require a public-law basis, such as a treaty between States. (TIB and CTIVD 2018)

An international legal instrument facilitating transborder data flows

The modernised Convention 108 was referred to as the legally binding international agreement that would be suited to solve many of the issues regarding international data transfer following the CJEU's Schrems II ruling: "*Some influential voices have been calling, in the aftermath of the Schrems II decision, for a legally binding international agreement for the protection of privacy and personal data. This instrument exists: it is Convention 108*+", (Pierucci and Walter 2020). In 'Schrems II', the CJEU held that personal data transferred outside of the EU must be guaranteed an equivalent level of protection to that set out by the General Data Protection Regulation (GDPR). This includes appropriate safeguards against disproportionate government access to data as well as enforceable rights and effective legal remedies, also in the areas of national security and defence.

In the absence of at least one national oversight body that possesses the powers that the present exception may allow State Parties to do away with, the exception regarding Article 14, paragraph 5 and 6 seems to be incompatible with the CJEU's demands in Schrems II. It would deprive supervisory authorities of binding powers and the possibility of reviewing safeguards when it comes to transborder data transfers in the context of national security and defense. In order to render the modernised Convention 108 a more effective international legal instrument to facilitate transborder transfers of data, this exception should be reconsidered and efforts should be in place to ensure that oversight bodies do possess the powers discussed in the section below at the national level.

3.4.3. Article 15 paragraph 2: powers of supervisory authorities

3.4.3.1. Description

This exception concerns the powers of supervisory authorities referred to in Article 15 paragraph 1. In the context of national security and defense, parties to the Convention may derogate from the provisions in litterae a-d of paragraph 2 of Article 15 which accord supervisory authorities the following (binding) powers:

- the powers of investigation and intervention;
- the power to perform the functions relating to transfers of data provided for under Article 14, notably the approval of standardised safeguards;
- the powers to issue decisions with respect to violations of the provisions of this Convention and may, in particular, impose administrative sanctions;
- the power to engage in legal proceedings or to bring to the attention of the competent judicial authorities violations of the provisions of this Convention.

It is also important to highlight at the outset of this discussion what parts of Article 15 are not covered by the exception in Article 11 paragraph 3 and which, therefore, may not be derogated from even in the context of data processing in the context of national security and defense purposes. This includes amongst other things reporting duties, the supervisory authorities' complete independence and impartiality, their confidentiality of the authorities as well as consultative powers.

3.4.3.2. Problem Statement

The first question that arises is how the central safeguard added in the last sentence of Article 11 paragraph 3, namely:

> *"This is without prejudice to the requirement that processing activities for national security and defence purposes are subject to independent and effective review and supervision under the domestic legislation of the respective Party." (Article 11 paragraph 3)*

can be ensured in cases where State Parties chose to derogate from provisions in Article 15 paragraph 2?

To provide further context, we recall that State Parties are obliged to provide "one or more authorities to be responsible for ensuring compliance with the provisions of this Convention" (Article 15 paragraph 1). Yet, provided the conditions and safeguards of Article 11 paragraph 3 are being met, State Parties may derogate from the obligations in Article 15 paragraph 2, namely that these authorities

> "a. shall have powers of investigation and intervention;
> b. shall perform the functions relating to transfers of data provided for under Article 14, notably the approval of standardised safeguards;
> c. shall have powers to issue decisions with respect to violations of the provisions of this Convention and may, in particular, impose administrative sanctions;
> d. shall have the power to engage in legal proceedings or to bring to the attention of the competent judicial authorities violations of the provisions of this Convention;
> e. shall promote:
> i. public awareness of their functions and powers as well as their activities;
> ii. public awareness of the rights of data subjects and the exercise of such rights;
> iii. awareness of controllers and processors of their responsibilities under this Convention; specific attention shall be given to the data protection rights of children and other vulnerable individuals.a. shall have powers of investigation and intervention"

Now, if the exception under Article 11 paragraph 3 can allow for such a wholesale degradation of review and supervisory authorities (i.e. they would in such instances cease their rights to investigate and to intervene, their right to issue decisions with respect to violations of the provisions of the modernised Convention 108 and their right to impose sanctions), then the one way to guarantee that this broad exception would not lead to wholesale abuse is to make sure that

- the bodies referred to in Article 15 paragraph 1 are not identical to the one performing "*independent and effective review and supervision under the domestic legislation of the respective Party"*
- *the independent and effective review and supervision bodies under the domestic legislation do satisfy all the requirements of Article 15, even in the context of situations that may give rise to exceptions according to Article 11 paragraph 3. In addition, as will be pointed out in the next section, these oversight bodies should also be designed to reflect the increasing criteria put forward in national and European jurisprudence on national surveillance practices and their oversight.*

Now, if the bodies referred to in Article 15 paragraph 1 and in the last sentence of Article 13 paragraph 3 are not identical, say the former is a data protection authority and the latter is a

judicial oversight body, than the question arises how to make sure that there is no undue duplication of control and supervisory efforts and, more importantly, that key supervisory tasks, including the design and implementation of new supervisory technology, are comprehensively put in charge and that accountability gaps are best addressed and rectified. This concern is genuine because sporting numerous oversight bodies can invite scepticism about the ability of the combined "oversight community" to keep abreast of relevant developments. Once the oversight landscape becomes too crowded and accountability gaps become too evident, observers have warned about *obfuscation by design*. In this regard, we point to Canada. It has recently redesigned its intelligence oversight architecture in part because "*the previously compartmentalised approach to review and accountability*" (NSIRA 2020: 16) was no longer deemed fit for purpose. The new Canadian oversight body, NSIRA, now has "*an additional and novel mandate to review any activity in the federal government that relates to national security or intelligence" which it characterises as "horizontal, in-depth interagency review*" (NSIRA 2020: 16).

Similarly, consider the Dutch oversight bodies CTIVD and TIB's memorandum on the modernised Convention 108. It concludes that it calls for oversight that is "all-inclusive" (TIB and CTIVD 2021), i.e. oversight bodies need to be competent for all national security agencies and activities, not just partial aspects thereof, say the foreign intelligence collection as it relates to the personal data of national citizens but not the privacy interests of non-nationals or, to give another example, the review of data processing by military forces that may have received (automated) transfers of personal data collected by intelligence services under the review of special oversight bodies. Thus, as CTIVD and TIB rightly point out, there is a valid concern that needs to be addressed, namely that not all agencies engaged in personal data collection and subsequent data processing for national security and defense purposes are subject to the same *density* of oversight and accountability mechanisms.

3.4.3.3. Supervisory authorities "shall have powers of investigation and intervention" (Article 15, paragraph 2, littera a)

- Criteria "provided for by law"

The exemption from granting supervisory authorities (referred to under Article 15 paragraph 1) powers of investigation and intervention needs to be written down in a law.

Nota bene, this presupposes that the competent body performing "independent and effective review and supervision under the domestic legislation of the respective Party" (Article 11 paragraph 3) is not deprived of these key powers. We cannot imagine an "effective review" worthy of its name without such powers.

This said, there may be instances when certain oversight body powers, for example to review the data processing of personal data that originated from foreign partners and which may thus be protected under the "originator control principle/third party principle" can be withheld from one set of oversight bodies (say a data protection authority or parliamentary oversight bodies) solong as at least one independent oversight body can access such information and can independently investigate the executive's data processing thereon.

We recall also here what the European Court of Human Rights recently stipulated in its Centrum för rättvisa v. Sweden judgment (25 May 2021) (which considered bulk collection and processing of communication data by national intelligence services, i.e. a possible subset of activities to be considered under Article 11 paragraph 3). It stated that

> "264. [...] "end-to-end safeguards" [...] "are fundamental safeguards which will be the cornerstone of any Article 8 compliant bulk interception regime"
>
> "270. Each stage of the bulk interception process – including the initial authorisation and any subsequent renewals, the selection of bearers, the choice and application of selectors and query terms, and the use, storage, onward transmission and deletion of the intercept material – should also be subject to supervision by an independent authority and that supervision should be sufficiently robust to keep the "interference" to what is "necessary in a democratic society" (see *Roman Zakharov*, cited above, § 232; see also *Klass and Others*, cited above, §§ 49, 50 and 59; *Weber and Saravia*, cited above, § 106; and *Kennedy*, cited above, §§ 153 and 154). In particular, the supervising body should be in a position to assess the necessity and proportionality of the action being taken, having due regard to the corresponding level of intrusion into the Convention rights of the persons likely to be affected. In order to facilitate this supervision, detailed records should be kept by the intelligence services at each stage of the process"

- Criteria "only to the extent that it constitutes a necessary and proportionate measure in a democratic society to fulfill such aim"

Again, and with reference to the findings of the European Court of Human Rights cited above, it is essential that oversight bodies's supervision should be "sufficiently robust" so as to "assess the necessity and proportionality of the action being taken" and this cannot be done in the absence of investigation and inspection powers.

Summary

There may certainly be legitimate national security interests at stake and they may mean that State Parties can avail themselves of powerful resources and authorities to counter a rising number of threats.

Yet, in democracies, no national security threat may be countered in a manner that resembles the (dystopian) playbook of techno-authoritarian regimes. Instead, the powers of the executive in democracies are subject to thorough and regular independent review and supervision, which obviously has to include investigation and inspections in order to be effective.

Independent authorisation procedures and effective end-to-end safeguards may need to be subjected to special rules, however, in limited and documented cases of urgency and national emergencies.

4.4.3.4. Supervisory authorities "shall perform the functions relating to transfers of data provided for under Article 14, notably the approval of standardised safeguards" (Article 15, paragraph 2, littera b)

- Criteria "provided for by law"

Here, for example, the national law may waive the obligation that "the transfer of data may only take place where an appropriate level of protection based on the provision of this Convention is secured" (Article 14 paragraph 2) provided the law is very specific and that it needs to be easily accessible and understandable. It should also determine the scope of application of this exception exhaustively. Sunset clauses could be considered for the use of exceptions.

However, while the above may generally be true, State Parties are invited to discuss the compatibility of this finding with the recent jurisprudence of the European Court of Justice in the Schrems II case. It annulled the Privacy Shield agreement which was meant to secure the free flow of data with trust between the EU and the United States. It found that data transfers from the EU to the US under that agreement were not sufficiently protected by essentially equivalent safeguards in the US, especially as regards redress for European data subjects.

- Criteria "only to the extent that it constitutes a necessary and proportionate measure in a democratic society to fulfill such aim"

See the discussion below.

- Criteria "This is without prejudice to the requirement that processing activities for national security and defence purposes are subject to independent and effective review and supervision under the domestic legislation of the respective Party."

See the discussion below.

In the aftermath of the CJEU Schrems II jurisprudence and the findings of the European Court of Human Rights regarding the Convention compatibility of international intelligence cooperation under bulk interception regimes (Big Brother Watch and Others v. The United Kingdom, 25 May 2021; Centrum för Rättvisa v. Sweden, 25 May 2021), the Council of Europe may need also to revisit the continued usefulness of the "Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data regarding supervisory authorities and transborder data flows" (CETS 181) and, in particular, its Article 2 paragraph 2 whereby

"each Party may allow for the transfer of personal data :

a- if domestic law provides for it because of :
– specific interests of the data subject, or
– legitimate prevailing interests, especially important public interests, or

b- if safeguards, which can in particular result from contractual clauses, are provided by the controller responsible for the transfer and are found adequate by the competent authorities according to domestic law.

3.4.3.5. Supervisory authorities "shall have powers to issue decisions with respect to violations of the provisions of this Convention and may, in particular, impose administrative sanctions" (Article 15, paragraph 2, littera c)

- Criteria "provided for by law"
- Criteria "only to the extent that it constitutes a necessary and proportionate measure in a democratic society to fulfill such aim"
- Criteria "This is without prejudice to the requirement that processing activities for national security and defence purposes are subject to independent and effective review and supervision under the domestic legislation of the respective Party."

In this regard it may be necessary to discuss that when State Parties use this exception and when, therefore, the entities referred to in Article 15 paragraph 1 must do without powers to decide on Convention violations and to impose sanctions, that the other oversight entities referred to in Article 13 paragraph 3 must have specific sanctioning powers.

This is not the case for all State Parties to the European Convention on Human Rights.

3.4.3.6. Supervisory authorities "shall have the power to engage in legal proceedings or to bring to the attention of the competent judicial authorities violations of the provisions of this Convention" (Article 15, paragraph 2, littera d)

- Criteria "provided for by law" needs to be respected
- Criteria "only to the extent that it constitutes a necessary and proportionate measure in a democratic society to fulfill such aim" needs to be respected
- Criteria "This is without prejudice to the requirement that processing activities for national security and defence purposes are subject to independent and effective review and supervision under the domestic legislation of the respective Party."

In this regard it may be necessary to discuss that when State Parties use this exception and when, therefore, the entities referred to in Article 15 paragraph 1 must do without powers to engage in legal proceedings or to bring to the attention of the competent judicial authorities violations of the provisions of this Convention, that the other oversight entities referred to in Article 13 paragraph 3 must have those specific powers.

This is not the case for all State Parties to the European Convention on Human Rights. For example, the German G10-Commission, was not able to bring the German Constitutional Court to consider the merits of its case for access to the list of foreign selectors used by the German Foreign Intelligence agencies because it had not sufficient standing before the court to initiate an *Organstreitverfahren* (proceedings on a dispute between supreme federal bodies, see the decision by the German Constitutional Court 2 BvE 5/15 of 20 September 2016.

How to avoid giving unduly wide leeway to State Parties?

In this regard, it is important that at least one set of independent review and supervisory authority in each State Party meets the following criteria - some of which are corresponding with the provisions in Article 15 of the modernised Convention:

State Parties put in place a range of complementary mechanisms for independent and effective oversight to ensure adherence to the domestic legal framework and with regard to international legal obligations. Such oversight is characterised first and foremost by its independence and its effectiveness.

As regards independence of oversight bodies, this can be demonstrated, for example, by their composition. This pertains to the appointment process including safeguards against outside pressures and conflict of interests. Another key aspect to consider is oversight resources. Oversight bodies should be composed of full-time staff members with sufficient legal and technological expertise, including persons qualified to hold judicial office. These bodies should have a sufficient budget for performing investigations and to develop and to maintain technical tools and programmes for automated auditing. In addition, oversight bodies ought to have the fullest possible ownership of their resources and processes. This can mean autonomy over the sequence and focus of investigations, their expenditure and personnel decisions, their reporting as well as their use of oversight tools and supervisory technology, their ability to reach out to civil society and the private sector (within the limits of their obligation to confidentiality and government secrets) as well as the possibility to incorporate an adversary/amicus or special advocate in their decision-making/deliberation process to present another perspective. In addition, the reporting of oversight bodies is important and can also be seen as an aspect of their independence. Oversight bodies should be obliged to document their activities or findings in detailed and regular reports. These may be published in whole or in part and can also inform about incidents of non-compliance.

As regards the effectiveness of oversight bodies, this presupposes, amongst other factors, a broad oversight mandate. Oversight bodies need to continuously review both the legality and the effectiveness and propriety of government conduct when it comes to data collection, data processing, deletion and transfers. This includes the ability to assess the need for surveillance measures that is particularly intrusive in order to determine whether the application for such measures is in accordance with the law and to examine whether the state is facing a serious threat to national security that proves to be genuine and present or foreseeable and thus, justify a higher degree of intrusion and interference. Oversight bodies can subject all of law enforcement and intelligence agencies' activities to review, and their remit covers all stages of access and subsequent data processing including international data transfers and automated submissions to joint databases where relevant to the core activities of the oversight authority. In addition, the possession and regular use of investigative powers are key. Such

powers include elements such as the ability to: a) order the production of evidence from the government actors; b) supervise and enforce compliance with their decisions and orders and accompanying procedures including, for example and as relevant, that the government take remedial action where necessary and, c) subpoena agents of the government. As indicated, oversight bodies need binding powers to declare measures unlawful, order the termination of an activity, or impose sanctions or remedial actions. All of this presupposes sufficient access to information to review the legality and effectiveness of data processing. For this oversight bodies have comprehensive access to the information and data they need to carry out oversight. Depending on the sensitivity of the information, this may require appropriate security clearance. Access should be such that it enables oversight bodies on their own initiative to randomly scrutinise the entire processes of government access as to its lawfulness; this concerns individual decisions, processes, digital security, the design of (automated audits) to review data processing and filtering mechanisms as well as the technical resources used for them.

IV. Key challenges and recommendations

The modernised Convention 108 has great potential in enhancing the de facto and de jure protection of individuals with regard to the processing of personal data. As discussed in the previous sections, much depends, however, on the scope and the compatibility of the exceptions and restrictions under Article 11. They need to be sufficiently curtailed so as "to avoid giving Parties unduly wide leeway with regard to the general application of the Convention".[8]

To ensure a robust and consistent application of the Convention, more should be done to promote a common understanding among State Parties both with regards to the key terms invoked by the Convention and with regard to the scope of the permissible exceptions and restrictions under Article 11.

As regards the former, we created a unique knowledge base on key terms (see Annex) that includes both guidance from the explanatory material, international law and recent jurisprudence related to these terms by key European Courts.

As regards the latter, our analysis in the previous sections offered a critical suitability review of both exception regimes under Article 11. In so doing, we pointed to several discrepancies, inconsistencies and risks that now merit further consultations, in our view, by State Parties. In this regard we reiterate in the following three of the main challenges:

Importance of effective supervision and review mechanisms

Throughout this guidance note, the importance of effective supervision and review mechanisms as a key safeguard curtailing the exceptions in Article 11 has become more than apparent. Yet, what exactly constitutes the effectiveness of what kind of supervisory authority? On this crucial point, the explanatory material does not provide sufficient clarity. Especially in

[8] Explanatory Report to the Council of Europe's Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data of 1981 and its Additional Protocol (CETS No. 108, paragraph 56)

light of the recent ECtHR jurisprudence, we reiterate that what that court has recently called "the cornerstone of any Article 8 compliant bulk interception regime" (Centrum för Rättvisa v. Sweden, 25 May 2021, paragraph 264), namely

> "end-to-end safeguards", "meaning that at the domestic level, an assessment should be made at each stage of the process of the necessity and proportionality of the measures being taken; that bulk interception should be subject to independent authorisation at the outset, when the object and the scope of the bulk operation are being defined; and that the operation should be subject to supervision and independent ex post facto review".

We encourage State Parties to make sure that all supervision and review mechanisms under their domestic legislation fulfill at least the criteria put forward in Article 15 of the Convention. In addition, we invite State Parties to consider the list of criteria discussed at the end of Section 3.4.3 as well as the important findings of the European Court of Human Rights on end-to-end safeguards. What must be avoided, we caution, is that key obligations for State Parties with regard to the design and functioning of supervisory authorities under Chapter IV and V of this Convention are not being mirrored by those bodies referred to in Article 11 paragraph 3.

Enhanced international cooperation of supervisory authorities

It has long been argued that national oversight structures by themselves are insufficient for the comprehensive protection of fundamental human rights. Therefore, international oversight cooperation has been a central demand by many groups, including the Intelligence Oversight Working Group (de Ridder: 2019; EOS-Committee et al. 2018). This need has become all the more pressing in the context of ever-closer intelligence sharing.

It is of fundamental importance, therefore, that Article 17 of the modernised Convention 108 identifies co-operation as a key step for the protection of personal data and encourages co-operation between supervisory authorities of Parties to the Convention. Given the numerous challenges and risks identified in the section on the powers of supervisory authorities (see section 3.4.3), State Parties should be encouraged to ensure that at least one entity under their domestic legislation meets the requirements of Article 15 of the Convention in full and that such bodies incorporate what recent jurisprudence has called "end-to-end safeguards" from which there can be no derogation.

International transfers of personal data

The modernised Convention 108 has, on several occasions, been referred to as a legal instrument that could facilitate international data transfers. The UN Special Rapporteur on Privacy, Joe Cannataci, has recommended "to all UN Member States to adhere to Convention 108+." (Report of the Special Rapporteur on the right to privacy to the Human Rights Council 2019, A/HRC/40/63). The modernised Convention 108 is also explicitly mentioned in the Recital 105 of the GDPR that states that accession to the Convention should be taken into account when it comes to adequacy decisions with third countries.

However, we argue that Article 11 of the Convention in its current form might not be compatible with the CJEU's demands in Schrems II, that personal data transferred outside of the EU must

be guaranteed an equivalent level of protection to that set out by the General Data Protection Regulation (GDPR). The exception regarding Article 14, paragraph 5 and 6 would deprive supervisory authorities of binding powers and the possibility to review safeguards when it comes to transborder data transfers in the context of national security and defense.

In order to render the modernised Convention 108 a more effective international legal instrument to facilitate transborder transfers of data, more caveats should be added to the exceptions in Article 11. In particular, more effort should be undertaken to ensure that supervisory authorities do possess all necessary powers to ensure effective oversight and respect of fundamental rights when it comes to transborder data transfers.

V. The Committee's Interpretation on Article 11 of the Convention 108+

n/a

VI. Conclusion

The preparation of this guidance note allowed us to familiarise ourselves even more with this ambitious Convention. We applaud State Parties who have ratified the modernised Convention 108 and hope that others will follow suit. It remains, to date, the single most important instrument that regulates the processing of personal data even in the context of national security and defense.

We are thus immensely grateful for the opportunity given to us by the Secretariat of the Council of Europe's Data Protection Unit to reflect on possible steps that could make this instrument even stronger. This requires, first and foremost, a sober analysis of where the Convention's current exception regime under Article 11 falls short to protect individuals with regard to the processing of their personal data.

As alluded to by Alessandra Pierucci and Jean-Philippe Walter in their joint statement, the modernised Convention 108 "does not fully and explicitly address some of the challenges posed in our digital era by unprecedented surveillance capacities" (Pierucci and Walter 2020). In order to get a firmer grasp of existing challenges and where and how they might not be fully addressed, we looked at the various possible exceptions under Article 11 and found that the risk of broad exceptions is, unfortunately, very real and present. In its current state, the modernised Convention 108 permits State Parties too much undue leeway to avoid adhering to the general principles that this Convention seeks to promote. We therefore listed a number of ideas and potential measures that might help to further unleash the power of this unique Convention in the interest of our open societies.

We look forward to any comments received from delegations and look forward to our next exchange of views.

VII. Annex

7.1. Current knowledge base regarding the scope of permissible exceptions and restrictions under Article 11

7.1.1. Towards a common understanding of key notions invoked by Article 11

The following text tries to provide further information as regards the meaning of key terms used in Article 11. For this, we refer to the explanatory notes and discuss what, if any, questions remain open with respect to the precise meaning of these terms. Searching for more clarity, we then refer to the relevant case-law of the European Court of Human Rights and, for further illustration, we also discuss pertinent findings of the European Court of Justice.

Table 1: Overview of terms (bold font) further discussed in this section

Article 11 – Exceptions and restrictions

1. No exception to the provisions set out in this Chapter shall be allowed except to the provisions of Article 5 paragraph 4, Article 7 paragraph 2, Article 8 paragraph 1 and Article 9, when such an exception is **provided for by law**, r**espects the essence of the fundamental rights and freedoms** and constitutes a **necessary and proportionate measure in a democratic society** for:

a. the protection of **national security**, **defense**, **public safety**, **important economic and financial interests of the State**, the **impartiality and independence of the judiciary** or the **prevention, investigation and prosecution of criminal offences** and the execution of criminal penalties, and **other essential objectives of general public interest**;

b. the **protection of the data subject or the rights and fundamental freedoms of others**, notably **freedom of expression**.

2. Restrictions on the exercise of the provisions specified in Articles 8 and 9 may be provided for by law with respect to data processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes when there is no recognisable risk of infringement of the rights and fundamental freedoms of data subjects

3. In addition to the exceptions allowed for in paragraph 1 of this article, with reference to processing activities for national security and defense purposes, each Party may provide, by law and only to the extent that it constitutes a necessary and proportionate measure in a democratic society to fulfill such aim, exceptions to Article 4 paragraph 3, Article 14 paragraphs 5 and 6 and Article 15, paragraph 2, litterae a, b, c and d.

4. This is without prejudice to the requirement that processing activities for national security and defense purposes are subject to **independent and effective review and supervision** under the domestic legislation of the respective Party.

7.1.1.1. "Provided for by Law"

#1 What does the CoE draft explanatory material say about this?

"91. No exceptions to the provisions of Chapter II are allowed except for a limited number of provisions (...) on condition that such exceptions are provided for by law, (…) Such a measure must be prescribed by an accessible and foreseeable law, which must be sufficiently detailed".

#2 Is this sufficient or are there open questions?

What conditions have to be met in order for provisions in the law to be deemed sufficiently accessible, foreseeable and detailed? More broadly, what exactly constitutes "a law"? Does this include only primary legislation enacted by parliament or can it also include secondary legislation and perhaps also executive decrees, internal service manuals?

#3 Where might one find further clarity?

The jurisprudence of the European Court of Human Rights offers significant guidance as regards the open questions posed above. For example, we quote below from the G*uide on Article 8 of the Convention – Right to respect for private and family life* (ECHR 2018)

> **"C. In the case of a negative obligation, was the interference conducted "in accordance with the law"?**
>
> 14. The Court has repeatedly affirmed that any interference by a public authority with an individual's right to respect for private life and correspondence **must be in accordance with the law** (see notably *Klaus Müller v. Germany,* §§ 48-51). This expression does not only necessitate compliance with domestic law but also relates **to the quality of that law**, requiring it to be **compatible with the rule of law** (*Halford v. the United Kingdom*, § 49).
>
> 15. **The national law must be clear, foreseeable, and adequately accessible** (*Silver and Others v. the United Kingdom*, § 87). It must be **sufficiently foreseeable to enable individuals to act in accordance with the law** (*Lebois v. Bulgaria*, §§ 66-67 with further references therein, as regards internal orders in prison), and it must **demarcate clearly the scope of discretion for public authorities**. For example, as the Court articulated in the surveillance context, the law must be sufficiently clear in its terms to give citizens an **adequate indication of the conditions and circumstances in which the authorities are empowered to resort to any measures of secret surveillance and collection of data** (*Shimovolos v. Russia*, § 68). In *Vukota-Bojić v. Switzerland* the Court found a violation of Article 8 due to the lack of clarity and precision in the domestic legal provisions that had served as the legal basis of the applicant's surveillance by her insurance company after an accident.

16. The clarity requirement applies to the scope of discretion exercised by public authorities. Domestic law **must indicate with reasonable clarity the scope and manner of exercise of the relevant discretion conferred on the public authorities so as to ensure to individuals the minimum degree of protection to which they are entitled under the rule of law in a democratic society** (*Piechowicz v. Poland*, § 212).

17. **With regard to foreseeability, the phrase "in accordance with the law" thus implies, inter alia, that domestic law must be sufficiently foreseeable in its terms to give individuals an adequate indication as to the circumstances in which, and the conditions on which, the authorities are entitled to resort to measures affecting their rights under the Convention** (*Fernández Martínez v. Spain* [GC], § 117). Foreseeability need not be certain. In *Slivenko v. Latvia* [GC], the applicants must have been able to foresee **to a reasonable degree, at least with the advice of legal experts, that they would be regarded as covered by the law** (see also *Dubská and Krejzová v. the Czech Republic* [GC], § 171).

Absolute certainty in this matter could not be expected (§ 107). It should also be noted that **the applicant's profession may be a factor to consider as it provides an indication as to his or her ability to foresee the legal consequences of his or her actions** (*Versini-Campinchi and Crasnianski v. France*, § 55). In determining whether the applicable law could be considered as foreseeable in its conse- quences and as enabling the applicant to regulate his conduct in his specific case, the Court may be confronted **with a situation of divergences in the case-law of different courts at the same level of jurisdiction** (*Klaus Müller v. Germany,* §§ 54-60).

20. A finding that the measure in question **was not "in accordance with the law" suffices for the Court to hold that there has been a violation of Article 8 of the Convention**. It is not therefore necessary to examine whether the interference in question pursued a "legitimate aim" or was "necessary in a democratic society" (*M.M. v. the Netherlands*, § 46; *Solska and Rybicka v. Poland*, § 129). In *Mozer v. the Republic of Moldova and Russia* [GC], the Court found that, regardless of whether there was a legal basis for the interference with the applicant's rights, the interference did not comply with the other conditions set out in Article 8 § 2 (§ 196). The interference can also be considered not to be "in accordance with the law", as a result of an unlawful measure under Article 5 § 1 (*Blyudik v. Russia*, § 75)"

In addition, we invite delegates to also consider the case *Kruslin v France (ECHR 1990)* as a suitable reference for further clarity as regards the requirement that the law ought to be *sufficiently clear*. It states

"27. The expression "in accordance with the law", [...] requires firstly that the impugned measure should have some basis in domestic law; it also refers to the quality of the law in question, requiring that it should be accessible to the person concerned, who must moreover be able to foresee its consequences for him, and compatible with the rule of law."
28: "[...] By "law" as referred to in Article 8 § 2 (art. 8-2) of the Convention was meant the law in force in a given legal system [...]. The Delegate of the Commission

considered that[...] only a substantive enactment of general application - whether or not passed by Parliament - could amount to a "law" for the purposes of Article 8 § 2 (art. 8-2) of the Convention. Admittedly the Court had held that "the word 'law' in the expression 'prescribed by law' cover[ed] not only statute but also unwritten law" (see the Sunday Times judgment of 26 April 1979, Series A no. 30, p. 30, § 47, the Dudgeon judgment of 22 October 1981, Series A no. 45, p. 19, § 44, and the Chappell judgment of 30 March 1989, Series A no. 152, p. 22, § 52), but in those instances the Court was, so the Delegate maintained, thinking only of the common-law system. That system, however, was radically different from, in particular, the French system. In the latter, case-law was undoubtedly a very important source of law, but a secondary one, whereas by "law" the Convention meant a primary source.
29. [...] In relation to paragraph 2 of Article 8 (art. 8-2) of the Convention and other similar clauses, the Court has always understood the term "law" in its "substantive" sense, not its "formal" one; [...] (see, in particular, the De Wilde, Ooms and Versyp judgment of 18 June 1971, Series A no. 12, p. 45, § 93) and unwritten law. [...] [I]t would be wrong to exaggerate the distinction between common-law countries and Continental countries, as the Government rightly pointed out. Statute law is, of course, also of importance in common-law countries. Conversely, case-law has traditionally played a major role in Continental countries[...]. The Court has indeed taken account of case-law in such countries on more than one occasion (see, in particular, the Müller and Others judgment of 24 May 1988, Series A no. 133, p. 20, § 29, the Salabiaku judgment of 7 October 1988, Series A no. 141, pp. 16-17, § 29, and the Markt Intern Verlag GmbH and Klaus Beermann judgment of 20 November 1989, Series A no. 165, pp. 18-19, § 30). Were it to overlook case-law, the Court would undermine the legal system of the Continental States almost as much as the Sunday Times judgment of 26 April 1979 would have "struck at the very roots" of the United Kingdom's legal system if it had excluded the common law from the concept of "law" (Series A no. 30, p. 30, § 47). In a sphere covered by the written law, the "law" is the enactment in force as the competent courts have interpreted it in the light, if necessary, of any new practical developments. "

As regards the law's "foreseeability" one can refer to the Malone judgment of 2 August 1984. It stated that

" Article 8 § 2 (art. 8- 2) of the Convention "does not merely refer back to domestic law but also relates to the quality of the law, requiring it to be compatible with the rule of law". It "thus implies ... that there must be a measure of legal protection in domestic law against arbitrary interferences by public authorities with the rights safeguarded by paragraph 1 (art. 8-1) ... Especially where a power of the executive is exercised in secret, the risks of arbitrariness are evident ... Undoubtedly ..., the requirements of the Convention, notably in regard to foreseeability, cannot be exactly the same in the special context of interception of communications for the purposes of police investigations" - or judicial investigations - "as they are where the object of the relevant law is to place restrictions on the conduct of individuals. In particular, the requirement of foreseeability cannot mean that an individual should be enabled to foresee when the authorities are likely to intercept his communications so that he can adapt his conduct accordingly. Nevertheless, the law must be sufficiently clear in its terms to give citizens an adequate indication as to the circumstances in which and

the conditions on which public authorities are empowered to resort to this secret and potentially dangerous interference with the right to respect for private life and correspondence.

[In its judgment of 25 March 1983 in the case of Silver and Others the Court] held that 'a law which confers a discretion must indicate the scope of that discretion', although the detailed procedures and conditions to be observed do not necessarily have to be incorporated in rules of substantive law (ibid., Series A no. 61, pp. 33-34, §§ 88-89). The degree of precision required of the 'law' in this connection will depend upon the particular subject-matter ... Since the implementation in practice of measures of secret surveillance of communications is not open to scrutiny by the individuals concerned or the public at large, it would be contrary to the rule of law for the legal discretion granted to the executive" - or to a judge - "to be expressed in terms of an unfettered power. Consequently, the law must indicate the scope of any such discretion conferred on the competent authorities and the manner of its exercise with sufficient clarity ... to give the individual adequate protection against arbitrary interference." (Series A no. 82, pp. 32-33, §§ 67-68)

What is more, one can find further clarifications as regards the meaning of foreseeability in the context of secret surveillance in the recent European Court of Human Rights judgement in Centrum för Rättvisa v Sweden (25 May 2021)

247. The meaning of "foreseeability" in the context of secret surveillance is not the same as in many other fields. In the special context of secret measures of surveillance, such as the interception of communications, "foreseeability" cannot mean that individuals should be able to foresee when the authorities are likely to resort to such measures so that they can adapt their conduct accordingly. However, especially where a power vested in the executive is exercised in secret, the risks of arbitrariness are evident. It is therefore essential to have clear, detailed rules on secret surveillance measures, especially as the technology available for use is continually becoming more sophisticated. The domestic law must be sufficiently clear to give citizens an adequate indication as to the circumstances in which and the conditions on which public authorities are empowered to resort to any such measures (see *Roman Zakharov*, cited above, § 229; see also *Malone v. the United Kingdom*, 2 August 1984, § 67, Series A no. 82; *Leander*, cited above, § 51; *Huvig v. France*, 24 April 1990, § 29, Series A no. 176- B; *Valenzuela Contreras v. Spain*, 30 July 1998, § 46, Reports of Judgments and Decisions 1998- V; *Rotaru*, cited above, § 55; *Weber and Saravia*, cited above, § 93; and *Association for European Integration and Human Rights and Ekimdzhiev v. Bulgaria*, no. 62540/00, § 75, 28 June 2007). Moreover, the law must indicate the scope of any discretion conferred on the competent authorities and the manner of its exercise with sufficient clarity to give the individual adequate protection against arbitrary interference (see *Roman Zakharov*, cited above, § 230; see also, among other authorities, *Malone*, cited above, § 68; *Leander*, cited above, § 51; *Huvig*, cited above, § 29; and *Weber and Saravia*, cited above, § 94).

Finally, as regards the questions what needs to be stated in primary legislation and what may be the subject of executive decrees, we invite you to consult the findings of the German Constitutional Court (19 May 2020)

> 192. This basic framework to be determined by the legislator includes the requirement that the Federal Intelligence Service analyse intercepted data without undue delay [...], the applicability of the principle of proportionality to the selection of search terms – which is already provided for in the existing intelligence service manual –, provisions governing the use of intrusive methods of data analysis, in particular complex forms of data cross-checking [..]. The legislator may also have to lay down how algorithms may be used, in particular to ensure that their use can generally be reviewed by the independent oversight regime.

7.1.1.2. "Respects essence of the fundamental rights and freedoms"

#1 What does the CoE draft explanatory material say about this?

"91. No exceptions to the provisions of Chapter II are allowed except for a limited number of provisions (Article 5 paragraph 4, Article 7 paragraph 2, Article 8 paragraph 1 and Article 9) on condition that such exceptions are provided for by law, that they respect the essence of the fundamental rights and freedoms, and are necessary in a democratic society for the grounds listed in litterae a. and b. of the first paragraph of Article 11. [...]"

#2 Is this sufficient or are there open questions?

Under which conditions and to what extent is interference in those rights and freedoms legitimate and which requirements must be fulfilled for the fundamental rights and freedoms to be respected in their essence. What exactly is their essence?

#3 Where might one find further clarity?

An example where a regulation was seen as compromising the essence of the fundamental right to respect for private life was provided in the CJEU Schrems I judgment:

> In C-362/14 *Schrems*, the CJEU held that "*legislation permitting public authorities to have access on a generalised basis*" violated the essence of the EU fundamental right to privacy under Article 7 of the EU Charter of Fundamental Rights (CFR).

7.1.1.3. "Necessary and Proportionate in a democratic society"

#1 What does the CoE draft explanatory material say about this?

"91. A measure which is "necessary in a democratic society" must pursue a legitimate aim and thus meet a pressing social need which cannot be achieved by less intrusive means.
Such a measure should, furthermore, be proportionate to the legitimate aim being pursued and the reasons adduced by the national authorities to justify it should be relevant and

adequate. Such a measure must be prescribed by an accessible and foreseeable law, which must be sufficiently detailed."

#2 Is this sufficient or are there open questions?

What distinguishes a matter that is proportionate to the legitimate aim from a measure that is disproportionate to the legitimate aim?

#3 Where might one find further clarity?

As regards the "legitimate aim"

- "must meet the objectives of general interest … or the need to protect the rights and freedoms of others" (art. 52. 1 EU Charter)

As regards proportionality, the principle of purpose limitation ought to be considered and applied:

- "shall not be applied for any purpose other than those for which they have been prescribed." (Article 16 of the ECHR)

Here, we also point to the European Court of Human Rights' judgement in the case of Centrum för Rättvisa vs. Sweden (25 May 2021):

> "249. In this regard it should be reiterated that in its case-law on the interception of communications in criminal investigations, the Court has developed the following minimum requirements that should be set out in law in order to avoid abuses of power: (1) the nature of offences which may give rise to an interception order; (2) a definition of the categories of people liable to have their communications intercepted; (3) a limit on the duration of interception; (4) the procedure to be followed for examining, using and storing the data obtained; (5) the precautions to be taken when communicating the data to other parties; and (6) the circumstances in which intercepted data may or must be erased or destroyed (see *Huvig*, cited above, § 34; *Valenzuela Contreras*, cited above, § 46; *Weber and Saravia*, cited above, § 95; and *Association for European Integration and Human Rights and Ekimdzhiev*, cited above, § 76). In *Roman Zakharov* (cited above, § 231) the Court confirmed that the same six minimum safeguards also applied in cases where the interception was for reasons of national security; however, in determining whether the impugned legislation was in breach of Article 8, it also had regard to the arrangements for supervising the implementation of secret surveillance measures, any notification mechanisms and the remedies provided for by national law (see *Roman Zakharov*, cited above, § 238)."

Also, we draw attention to the CJEU findings in La Quadrature du Net and Others (6 October 2020):

> 131. Specifically, it follows from the Court's case-law that the question whether the Member States may justify a limitation on the rights and obligations laid down, inter alia, in Articles 5, 6 and 9 of Directive 2002/58 must be assessed by measuring the seriousness of the interference entailed by such a limitation and by verifying that the

> importance of the public interest objective pursued by that limitation is proportionate to that seriousness (see, to that effect, CJEU, Ministerio Fiscal, 2 October 2018, paragraph 55 and the case-law cited).

As regards necessity, we point to the CJEU's remarks on the "strict necessity test"

> For limitations on the rights to respect for private life and protection of personal data, the CJEU applies a strict necessity test, holding that "derogations and limitations must apply only in so far as strictly necessary"(CJEU, Schrems I, 6 October 2015, paragraph 92; see also CJEU, Tele2 Sverige AB, 21 December 2016, paragraph 96)

As regards an example where legislation exceeds that what is strictly necessary in a democratic society, we point to the CJEU finding in the Quadrature du Net case:

> For example, according to the CJEU, legislation is not limited to what is strictly necessary where it authorises, on a generalised basis, storage of all the personal data of all persons "without any differentiation, limitation or exception being made in the light of the objective pursued and without an objective criterion being laid down by which to determine the limits of the access of the public authorities to the data, and of its subsequent use, for purposes which are specific, strictly restricted and capable of justifying the interference which both access to that data and its use entail" (See CJEU, Schrems I, 6 October 2015, para 93, with further references. See also CJEU, Tele2 Sverige AB, 21 December 2016, paragraphs 105-111)

7.1.1.4. "National Security"

#1 What does the CoE draft explanatory material say about this?

94.The notion of "national security" should be interpreted on the basis of the relevant case law of the European Court of Human Rights.

Footnote: The relevant case law includes in particular the protection of state security and constitutional democracy from, inter alia, espionage, terrorism, support for terrorism and separatism. Where national security is at stake, safeguards against unfettered power must be provided. Relevant decisions of the European Court of Human Rights can be found at the Court's website (hudoc.echr.coe.int).[9]

#2 Is this sufficient or are there open questions?

To date, the European Court of Human Rights has not comprehensively defined the concept of "national security." Also on a national level the term mostly refers to broad concepts that are not used uniformly across Member States (See ECHR, Regner v. The Czech Republic [GC], 19 September 2017, paragraph 67 and FRA 2017, p. 53)

[9] See, for example, European Court of Human Rights Research Division, National security and European case-law, November 2013, available at http://www.coe.int/t/dghl/standardsetting/dataprotection/judgments_EN.asp?

> "67. In the light of the comparative information available to the Court concerning thirty member States, protection of national security is a matter of concern in every State whose legislation was examined. Whilst the concept of "national safety" or "national security" is not uniformly defined, the legislation in each member State allows the executive, in particular the authorities responsible for national security, to restrict access to classified information, including in judicial, criminal and administrative proceedings, where this is deemed necessary to protect the State's interests."

Further guidance, we think, is needed on what "national security" entails with regard to its meaning both in the books and on the ground.

#3 Where might one find further clarity?

The ECHR has held that it is difficult to precisely define the concept of national security. Yet, even broadly defined, and leaving a large margin of appreciation to Council of Europe Member States, in its case-law, the court assigns to the notion of national security various concepts that need to have a factual basis. It is clear from the examples listed in the box on ECHR case law on national security that the latter goes beyond the protection of the territorial integrity of a state and protection of its democratic institutions – extending to major threats to public safety and including cyber-attacks on critical infrastructures.

'National Security' in the ECHR case-law (selection)

The principal cases in which interferences in fundamental rights have been justified with the protection of 'National Security' "indicate that it concerns the security of the state and the democratic constitutional order from threats posed by enemies both within and without" (Greer 1997, p.19).

National Security defence can be invoked "in relation to the right to respect for private and family life, home and correspondence (Article 8 paragraph 2), the right to freedom of expression (Article 10, paragraph 2), and the rights to peaceful assembly and association (Article 11, paragraph 2)" (Greer 1997, p.18f.).

"It justified its position by underlining the fact that 'many laws, which by their subject-matter require to be flexible, are inevitably couched in terms which are to a greater or lesser extent vague and whose interpretation and application are questions of practice' (Ibid.; referring to: ECHR, Esbester v. the UK, 2 April 1993)".

"Throughout its jurisprudence, the ECtHR has accepted, among others, as threats to national security:

- espionage (Roman Zakharov v. Russia, 4 December 2015, Klass v. Germany, 6 September 1978)
- terrorism (Klass v. Germany, 6 September 1978; Weber and Saravia v. Germany, 29 June 2006)
- incitement to/approval of terrorism (Zana v. Turkey, 25 November 1997)

- subversion of parliamentary democracy (Leander v. Sweden, 23 August 2011)
- separatist extremist organisations that threaten the unity or security of a state by violent or undemocratic means (United Communist Party of Turkey and Others v. Turkey, 30 January 1998)
- inciting disaffection of military personnel (Arrowsmith v. United Kingdom, 12 October 1978) (FRA 2017, p. 53)"

'National Security' in the EU (selection)

In the CJEU Case law

- The CJEU "has not established a clear definition or developed the concept of national security beyond stating that 'national security [...] constitutes activities of the State or of State authorities unrelated to the fields of activity of individuals'" (CCBE 2019, p.9 refering to Productores de Música de España (Promusicae) v Telefónica de España SAU, 29 January 2008, paragraph 51)
- In Fahimian v. Germany (4 April 2017) the CJEU "stated that the concept of 'public security' covers both the internal security of a Member State and its external security Moreover, in ZZ v. Secretary for the Home Department (4 June 2013), the CJEU implicitly held that the notion of state security as used in EU secondary legislation is equivalent to the notion of 'national security' as used in national law". The use in national law however varies from country to country – as shows the survey conducted by the CCBE (2019, p.10-17)
- "The Court seldom challenges the legitimate national security aim adduced by the state. We might, however, mention the example of Castells v. Spain, where a Senator had accused the Government of involvement in the murders of Basque nationalists. The domestic courts had not permitted him to produce evidence in support of his allegations, as their veracity was irrelevant to the offence of insulting the Government. According to the Spanish courts, the Government's reputation, at a time when the country was still grappling with its post-Franco democratic transition, was a national security problem. The Court, on the other hand, considered that it was more a question of preventing disorder." (ECHR 2013, p.17)

In EU Secondary Legislation:

- "In some EU secondary legislation, 'national security' is explained as state security – for instance, in Article 15(1) of the e-Privacy Directive 2002/58/EC. In other EU secondary legislation – for example, in Article 6(1)(d) of the Admission of Third-Country Nationals for the Purposes of Studies Directive 207 – 'national security' is referred to as 'public security' (FRA 2017, p. 53)."

In addition, we would like to draw your attention to the observation made by the Dutch intelligence oversight bodies CTIVD and TIB, namely that

> "*the (modernised) Convention (108) takes a conceptual/holistic approach when it refers to 'national security and defence'. National legislative frameworks do not always take that approach and sometimes exclude certain areas, for example limiting the scope of oversight to certain intelligence and security organisations or to domestic activities or national citizens.* However, Convention 108+ does not allow

that type of exclusion. *When implemented nationally, the entire security domain must therefore be included, i.e. it must be all-inclusive. That means that when appointing the oversight body/supervisory authority (i.e. Article 11.3, 15, and 16(2) of the Convention), it must be clear that the entire national security domain falls under the responsibility of the oversight body or bodies to be appointed*." (CTIVD and TIB 2021, p. 2)

7.1.1.5. "Defense"

#1 What does the CoE draft explanatory material say about this?
Nothing. Some guidance can be found in the UN Charter, Article 51:
"Nothing in the present Charter shall impair the inherent right of individual or collective self-defence if an armed attack occurs against a Member of the United Nations, until the Security Council has taken measures necessary to maintain international peace and security. Measures taken by Members in the exercise of this right of self-defence shall be immediately reported to the Security Council and shall not in any way affect the authority and responsibility of the Security Council under the present Charter to take at any time such action as it deems necessary in order to maintain or restore international peace and security."

#2 Is this sufficient or are there open questions?
The term "defense" appears to be sufficiently clear. However, depending on the reference object of defense, ie. land, air, space, sea and cyber) it might become necessary to spell out in further detail the territorial reach of this concept and to focus on accountability aspects of civil-military cooperation and the cooperation between state agencies with actors of the private sector.

#3 Where might one find further clarity?

In ECtHR Case Law[10] and in the Case Law Database of the European Union Agency for Fundamental Rights.[11]

7.1.1.6. "Public safety"

#1 What does the CoE draft explanatory material say about this?

92. All processing of personal data must be lawful, fair and transparent in relation to the data subjects, and only processed for specific purposes. This does not in itself prevent the law enforcement authorities from carrying out activities such as covert investigations or video surveillance. Such activities can be done for the purposes of the prevention, investigation, detection or prosecution of criminal offences and the execution of criminal penalties, including the safeguarding against and the prevention of threats to national security and public safety,

[10] See, **https://www.echr.coe.int/documents/fs_armed_conflicts_eng.pdf**
[11] See, **https://fra.europa.eu/en/case-law-database.**

as long as they are laid down by law and constitute a necessary and proportionate measure in a democratic society with due regard for the legitimate interests of the data subjects.

#2 Is this sufficient or are there open questions?

The explanatory material does give guidance on how the term "public safety" is used within the scope of the modernised Convention 108. It does not, however, provide more comprehensive specification on what "public safety" entails in the books and on the ground.

#3 Where might one find further clarity?

According to the jurisprudence of the European Court of Human Rights, notably in the case S.A.S v. France (1 July 2014) the *Court stated:*

> 115. As regards the first of the aims invoked by the Government, the Court first observes that "public safety" is one of the aims enumerated in the second paragraph of Article 9 of the Convention (*sécurité publique* in the French text) and also in the second paragraph of Article 8 (*sûreté publique* in the French text). It further notes the Government's observation in this connection that the impugned ban on wearing, in public places, clothing designed to conceal the face satisfied the need to identify individuals in order to prevent danger for the safety of persons and property and to combat identity fraud. Having regard to the case file, it may admittedly be wondered whether the Law's drafters attached much weight to such concerns. It must nevertheless be observed that the explanatory memorandum which accompanied the bill indicated – albeit secondarily – that the practice of concealing the face "could also represent a danger for public safety in certain situations" (see paragraph 25 above), and that the Constitutional Council noted that the legislature had been of the view that this practice might be dangerous for public safety (see paragraph 30 above). Similarly, in its study report of 25 March 2010, the *Conseil d'État* indicated that public safety might constitute a basis for prohibiting concealment of the face, but pointed out that this could be the case only in specific circumstances (see paragraphs 22-23 above).
>
> 139. As regards the question of necessity in relation to public safety, within the meaning of Articles 8 and 9 (see paragraph 115 above), the Court understands that a State may find it essential to be able to identify individuals in order to prevent danger for the safety of persons and property and to combat identity fraud.

It is, moreover, crucial to make the distinction with the term "national security". In contrast to the term "national security", that relates solely to one specific State, public security, it has been argued, can be understood as more general and inclusive, comprising the security of more than one state.[12] In the context of the Council of Europe, if one were to subscribe to this rationale, one might thus speak of 47 national securities and one common public security.

[12] J. Pauget, "sécurité nationale et protection des données personnelles en Droit de l'Union Européenne", sous la direction de Loïc Robert et de Gaëlle Marti, 2020.

7.1.1.7. “Important economic and financial interests of the state”

#1 What does the CoE draft explanatory material say about this?

95.The term “important economic and financial interests” covers, in particular, tax collection requirements and exchange control.

#2 Is this sufficient or are there open questions?

The authors did not have time to look into this.

#3 Where might one find further clarity?

It might be of interest to delegations to discuss the extent to which some states have added provisions in their national legislation covering foreign intelligence collection that certain types of data may not be collected and further processed, if this amounts to economic espionage.

7.1.1.8. “Impartiality and independence of the judiciary”

#1 What does the CoE draft explanatory material say about this?

The authors did not have time to look into this.

#2 Is this sufficient or are there open questions?

The authors did not have time to look into this.

#3 Where might one find further clarity?

> “Instead, independence is a key requirement which means both independence from the executive and independence from the parties (*Zand v Austria* 1978). It must be impartial, which denotes the absence of prejudice or bias (*Piersack v Belgium* 1982). Key to determining whether a body is independent is the manner of appointment of its members, their terms of office, the existence of guarantees against outside pressures and the question whether the body presents an appearance of independence. Lack of independence is apparent where the role or duties of the members make them vulnerable to outside pressure, whether there are insufficient legal guarantees of their independence and if they can be removed or their terms ended, or their tasks and duties changed substantially by the body which appointed them (*Lukas v Romania* 2009). “ **(**Guild and Wetzling 2021)

7.1.1.9. “Prevention, investigation and prosecution of criminal offences”

#1 What does the CoE draft explanatory material say about this?

92. All processing of personal data must be lawful, fair and transparent in relation to the data subjects, and only processed for specific purposes. This does not in itself prevent the law enforcement authorities from carrying out activities such as covert investigations or video

surveillance. Such activities can be done for the purposes of the prevention, investigation, detection or prosecution of criminal offences and the execution of criminal penalties, including the safeguarding against and the prevention of threats to national security and public safety, as long as they are laid down by law and constitute a necessary and proportionate measure in a democratic society with due regard for the legitimate interests of the data subjects.

95. [...] The term “prevention, investigation and prosecution of criminal offences and the execution of criminal penalties” in this littera includes the prosecution of criminal offences and the application of sanctions related thereto.

#2 Is this sufficient or are there open questions?

The authors did not have time to look into this.

#3 Where might one find further clarity?

From the European Law Enforcement Directive:

> 11) It is therefore appropriate for those fields [of judicial cooperation in criminal matters and police cooperation] to be addressed by a directive that lays down the specific rules relating to the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security, respecting the specific nature of those activities. Such competent authorities may include not only public authorities such as the judicial authorities, the police or other law-enforcement authorities but also any other body or entity entrusted by Member State law to exercise public authority and public powers for the purposes of this Directive. […]
>
> 12) The activities carried out by the police or other law-enforcement authorities are focused mainly on the prevention, investigation, detection or prosecution of criminal offences, including police activities without prior knowledge if an incident is a criminal offence or not. Such activities can also include the exercise of authority by taking coercive measures such as police activities at demonstrations, major sporting events and riots. They also include maintaining law and order as a task conferred on the police or other law-enforcement authorities where necessary to safeguard against and prevent threats to public security and to fundamental interests of the society protected by law which may lead to a criminal offence. [...]
>
> 27) For the prevention, investigation and prosecution of criminal offences, it is necessary for competent authorities to process personal data collected in the context of the prevention, investigation, detection or prosecution of specific criminal offences beyond that context in order to develop an understanding of criminal activities and to make links between different criminal offences detected. [...]
>
> 29) Personal data should be collected for specified, explicit and legitimate purposes within the scope of this Directive and should not be processed for purposes incompatible with the purposes of the prevention, investigation, detection or

prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security. [...]

34) The processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security, should cover any operation or set of operations which are performed upon personal data or sets of personal data for those purposes, whether by automated means or otherwise, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, alignment or combination, restriction of processing, erasure or destruction. [...]

35) In order to be lawful, the processing of personal data under this Directive should be necessary for the performance of a task carried out in the public interest by a competent authority [...] for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security. Those activities should cover the protection of vital interests of the data subject. The performance of the tasks of preventing, investigating, detecting or prosecuting criminal offences institutionally conferred by law to the competent authorities allows them to require or order natural persons to comply with requests made. In such a case, the consent of the data subject, as defined in Regulation (EU) 2016/679, should not provide a legal ground for processing personal data by competent authorities. Where the data subject is required to comply with a legal obligation, the data subject has no genuine and free choice, so that the reaction of the data subject could not be considered to be a freely given indication of his or her wishes. This should not preclude Member States from providing, by law, that the data subject may agree to the processing of his or her personal data for the purposes of this Directive, such as DNA tests in criminal investigations or the monitoring of his or her location with electronic tags for the execution of criminal penalties.

In addition, delegates are invited to consider ECHR M.K. v. France (18 April 2013): Procedures for the retention data and absence of safeguards. (For the exception under Article 5(4) of the Convention 108)

7.1.1.10. "Other Essential Objectives of General Public Interest"

#1 What does the CoE draft explanatory material say about this?

95. [...] The term "other essential objectives of general public interest" covers inter alia, the prevention, investigation, detection and prosecution of breaches of ethics for regulated professions and the enforcement of civil law claims.

#2 Is this sufficient or are there open questions?

The authors did not have time to look into this.

#3 Where might one find further clarity?

The authors did not have time to look into this.

7.1.1.11. "The protection of data subjects or rights and fundamental freedoms of others"

#1 What does the CoE draft explanatory material say about this?

96. Littera b. (of Article 11) concerns the rights and fundamental freedoms of private parties, such as those of the data subject himself or herself (for example when a data subject's vital interests are threatened because he or she is missing) or of third parties, such as freedom of expression, including freedom of journalistic, aca-demic, artistic or literary expression, and the right to receive and impart information, confidentiality of correspondence and communications, or business or commercial secrecy and other legally protected secrets. This should apply in particular to processing of personal data in the audio-visual field and in news archives and press libraries. In order to take account of the importance of the right to freedom of expression in every democratic society, it is necessary to interpret notions relating to that freedom, such as journalism, broadly.

#2 Is this sufficient or are there open questions?

The authors did not have time to look into this.

#3 Where might one find further clarity?

Delegates are invited to consider ECHR L.B. v. Hungary (12 January 2012)

7.1.1.12. "Freedom of expression"

#1 What does the CoE draft explanatory material say about this?

11. The right to data protection is for instance to be considered alongside the right to 'freedom of expression' as laid down in Article 10 of the European Convention on Human Rights (ETS No. 5), which includes the freedom to hold opinions and to receive and impart information.

"Everyone has the right to freedom of expression. This right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers. This Article shall not prevent States from requiring the licensing of broadcasting, television or cinema enterprises.

The exercise of these freedoms, since it carries with it duties and responsibilities, may be subject to such formalities, conditions, restrictions or penalties as are prescribed by law and are necessary in a democratic society, in the interests of national security, territorial integrity or public safety, for the prevention of disorder or crime, for the protection of health or morals, for the protection of the reputation or rights of others, for preventing the disclosure of information received in confidence, or for maintaining the authority and impartiality of the judiciary."

Article 10 of the European Convention on Human Rights.

"You have the freedom to express yourself online and to access information and the opinions and expressions of others. *This includes political speech, views on religion, opinions and expressions that are favourably received or regarded as inoffensive, but also those that may offend, shock or disturb others. You should have due regard to the reputation or rights of others, including their right to privacy.*

Restrictions may apply to expressions which incite discrimination, hatred or violence*. These restrictions must be lawful, narrowly tailored and executed with court oversight.*

You are free to create, re-use and distribute content *respecting the right to protection of intellectual property, including copyright.*

Public authorities have a duty to respect and protect your freedom of expression and your freedom of information*. Any restrictions to this freedom must not be arbitrary, must pursue a legitimate aim in accordance with the European Convention on Human Rights such as, among others, the protection of national security or public order, public health or morals, and must comply with human rights law. Moreover, they must be made known to you, coupled with information on ways to seek guidance and redress, and not be broader or maintained for longer than is strictly necessary to achieve a legitimate aim.*

Your Internet service provider and your provider of online content and services have corporate responsibilities to respect your human rights and provide mechanisms to respond to your claims*. You should be aware, however, that online service providers, such as social networks, may restrict certain types of content and behaviour due to their content policies. You should be informed of possible restrictions so that you are able to take an informed decision as to whether to use the service or not. This includes specific information on what the online service provider considers as illegal or inappropriate content and behaviour when using the service and how it is dealt with by the provider.*

You may choose not to disclose your identity online*, for instance by using a pseudonym. However, you should be aware that measures can be taken, by national authorities, which might lead to your identity being revealed ."(Council of Europe n.d.)*

#2 Is this sufficient or are there open questions?

Further guidance is needed on how this right can be balanced with the right to privacy (Article 8, ECHR).
Issues revolve around hate speech, intellectual property rights, blocking and filtering (by service providers/by public authorities), lawful restriction of the right to freedom of expression by public authorities, and anonymity.

#3 Where might one find further clarity?

Balancing with the right to privacy

The ECHR considers, since its judgment on Axel Springer AG v. Germany (7 February 2012), that where the right to freedom of expression is being balanced with the right to respect for private life, the relevant criteria in the balancing exercise include the following elements: contribution to a debate of general interest, how well known the person concerned is, the subject of the report, the prior conduct of the person concerned, the method of obtaining the information and its veracity, the content, form and consequences of the publication, and the severity of the sanction imposed. Therefore the Internet user should have due regard to the reputation of others, including their right to privacy.

Hate speech

There is expression that does not qualify for protection under Article 10 of the **ECHR** such as hate speech. The Court has found that certain forms of expression which amount to hate speech or which negate the fundamental values of the ECHR are excluded from the protections afforded by Article 10 of the Court. In this connection the Court applies Article 17 of the ECHR. Although there is no universally acceptable definition of hate speech, the Council of Europe's Committee of Ministers has stated that the term "**hate speech**" shall be understood as covering all forms of expression which spread, incite, promote or justify racial hatred, xenophobia, anti-Semitism or other forms of hatred based on intolerance, including: intolerance expressed by aggressive nationalism and ethnocentrism, discrimination and hostility against minorities, migrants and people of immigrant origin." Paragraph 2 of the section on freedom of expression provides concise information which is formulated in simple language for the user with regard to the point that hate speech is not dealt with under Article 10 of the ECHR. This paragraph does not attempt to explain in legal terms the different ways in which article 10 and article 17 of the ECHR might apply to hate speech. Given the legal nature of this distinction it was considered that information on this point is more appropriate for the explanatory memorandum.

IPRs

Users have the right to receive and impart information on the Internet, in particular to create, re-use and distribute content using the Internet. The Court has examined the relationship between intellectual property protection and freedom of expression in relation to cases of criminal conviction for copyright infringements. The Court has considered such convictions as interferences with the right to freedom of expression which in order to be justified must be prescribed by law, pursue the legitimate aim of protecting the rights of others, and be considered necessary in a democratic society. The sharing or allowing others to share files on the Internet, even copyright-protected material and for profit-making purposes, is covered by the right to receive and impart information as provided in Article 10 of the ECHR. This is a right which is not absolute and so there is a need to weigh, on the one hand, the interest of sharing information with, on the other hand, the interest in protecting the rights of copyright holders. The Court has stressed that intellectual property benefits from the protection afforded by Article 1 of Protocol to the ECHR. Thus, it is a question of balancing two competing interests which are both protected by the ECHR.

The Committee of Ministers recommendation to its member States to promote the **public service value of the Internet** includes specific guidance on measures and strategies regarding freedom of communication and creation on the Internet regardless of frontiers. In particular, measures should be taken to facilitate, where appropriate, "re-uses" of Internet content, which means the use of existing digital content resources to create future content or services done in a manner that is compatible with respect for intellectual property rights.

Restriction of Article 10

In compliance with Article 10, paragraph 2, of the ECHR, any interference must be prescribed by law. This means that the law must be accessible, clear and sufficiently precise to enable individuals to regulate their behaviour. The law should provide for sufficient safeguards against abusive restrictive measures, including effective control by a court or other independent adjudicatory body. An interference must also pursue a legitimate aim in the interests of national security, territorial integrity or public safety, for the prevention of disorder or crime, for the protection of health or morals, for the protection of the reputation or rights of others, for preventing the disclosure of information received in confidence, or for maintaining the authority and impartiality of the judiciary. This list is exhaustive yet its interpretation and scope evolves with the case law of the Court. An interference must also be necessary in a democratic society which means that it should be proven that there is a pressing social need for it, that it pursues a legitimate aim, and that it is the least restrictive means for achieving that aim. These requirements are summarised in a language that is accessible for the user i.e. any restrictions to the freedom of expression must not be arbitrary and must pursue a legitimate aim in accordance with the ECHR such as among others, the protection of national security or public order, public health or morals and must comply with human rights law.

Blocking and filtering

Nationwide general **blocking or filtering** measures might be taken by State authorities only if the filtering concerns specific and clearly identifiable content, based on a decision on its illegality by a competent national authority which can be reviewed by an independent and impartial tribunal or regulatory body in accordance with the requirements of Article 6 of the ECHR. State authorities should ensure that all filters are assessed both before and during their implementation to ensure that their effects are proportionate to the purpose of the restriction and thus necessary in a democratic society, in order to avoid unjustified blocking of content.

Measures taken to block specific Internet content must not be arbitrarily used as a means of general blocking of information on the Internet. They must not have a collateral effect in rendering large quantities of information inaccessible, thereby substantially restricting the rights of Internet users. They should be prescribed by law. There should be strict control of the scope of blocking and effective judicial review to prevent any abuse of power. Judicial review of such a measure should weigh-up the competing interests at stake, strike a balance between them and determine whether a less far-reaching measure could be taken to block access to specific Internet content. The requirements and **principles** mentioned above do not prevent the installation of filters for the protection of minors in specific places where minors access the Internet such as schools or libraries.

Filtering and de-indexation of Internet content by **search engines** entails the risk of violating the freedom of expression of Internet users. Search engines have freedom to crawl and index information available on the World Wide Web. They should not be obliged to monitor their networks and services proactively in order to detect possibly illegal content and should not conduct any ex-ante filtering or blocking activity unless mandated by a court order or by a competent authority. De-indexation or filtering of specific websites at the requests of public authorities should be transparent, narrowly tailored and reviewed regularly subject to compliance with due process requirements.

This section also identifies some of the guarantees that Internet users should be afforded when restrictions apply, focusing notably on information to the user and possibilities to challenge these restrictions. This is referred to in the Council of Europe's Committee of Ministers **recommendation** on **filtering and blocking** measures. Internet users should be given information about when filtering has been activated, why a specific type of content has been filtered and to understand how, and according to which criteria, the filtering operates (for example black lists, white lists, keyword blocking, content rating, de-indexation or filtering of specific websites or content by search engines). They should be given concise information and guidance regarding the manual overriding of an active filter, namely who to contact when it appears that content has been unjustifiably blocked and the means which may allow a filter to be overridden for a specific type of content or website. Users should be afforded effective and readily accessible means of recourse and remedy, including the suspension of filters, in cases where users claim that content has been blocked unjustifiably.

It is possible that companies, such as **social networks**, remove content created and made available by Internet users. These companies may also deactivate users' accounts (e.g. a user's profile or presence in social networks) justifying their action on non-compliance with their terms and conditions of use of the service. Such actions could constitute an interference with the right to freedom of expression and the right to receive and impart information unless the conditions of Article 10, paragraph 2 of the ECHR as interpreted by the Court, are met.

According to the **United Nations Guiding Principles on Business and Human Rights Business** (which are not a binding instrument) enterprises have a responsibility to respect human rights, which requires them to avoid causing or contributing to adverse impacts on human rights and to provide for or cooperate in the remediation of such impacts. The duty to protect and to provide access to effective remedy is essentially incumbent on States. This is echoed in paragraph 5 of the section on **freedom of expression**. The corporate social responsibility of online service providers includes a commitment to combating hate speech and other content that incites violence or discrimination. Online service providers should be attentive to the use of, and editorial responses to, expressions motivated by racist, xenophobic, anti-Semitic, misogynist, sexist (including as regards Lesbian Gay Bisexual and Transgender people) or other bias. These providers should also be ready to help Internet users report content or expression of views and/or behaviour that may be considered illegal.

The **Guide** alerts Internet users that online service providers that host user-created content are entitled to exercise different levels of editorial judgment over the content on their services. Without prejudice to their editorial freedom, they should ensure that Internet users' right to seek, receive and impart information is not infringed upon in accordance with Article 10 of the ECHR. This means that any restriction on user-generated content should be specific, justified for the purpose it is restricted, and communicated to the Internet user concerned.

The Internet user should be able to make an informed decision as to whether to use the online service or not. In practice, the Internet user should be fully informed about any foreseen measures to remove content created by her/him or to deactivate her/his account before these are taken. Internet users should also be provided with accessible (in a language that the user understands), clear and precise information on the facts and grounds for taking measures on content removal and account deactivation. This includes the legal provisions on which they are based and other elements used to assess the proportionality and legitimacy of the aim pursued. They should also be able to request a review of the content removal and/or account deactivation, done within a reasonable time and subject to the possibility to complain against the decision to a competent administrative and/or judicial authority.

Anonymity

The answer should be based on the case law of the Court, the Budapest Convention and other instruments of the Committee of Ministers. The Court considered the issue of confidentiality of Internet communications in a case involving the failure of a Council of Europe member State to compel an Internet service provider to disclose the identity of a person who placed an indecent advertisement concerning a minor on an Internet dating website (KU v Finland). The Court held that although freedom of expression and confidentiality of communications are primary considerations and users of telecommunications and Internet services must have a guarantee that their own privacy and freedom of expression will be respected, such guarantee cannot be absolute and must yield, on occasion, to other legitimate imperatives, such as the prevention of disorder or crime or the protection of the rights and freedoms of others. The State has a positive obligation to provide a framework which reconciles those competing interests.

The **Budapest Convention** does not criminalise the use of computer technology for purposes of anonymous communication. According to its **Explanatory Report**, "the modification of traffic data for the purpose of facilitating anonymous communications (e.g. activities of anonymous remailer systems) or the modification of data for the purposes of secure communications (e.g. encryption) should in principle be considered a legitimate protection of privacy, and, therefore, be considered as being undertaken with right. However, Parties [to the **Budapest Convention**] may wish to criminalise certain abuses related to anonymous communications, such as where the packet header information is altered in order to conceal the identity of the perpetrator in committing a crime."

The Council of Europe's Committee of Ministers affirmed the principle of anonymity in its **Declaration on Freedom of Communication on the Internet**. Accordingly, in order to ensure protection against online surveillance and to enhance freedom of expression; Council of Europe member States should respect the will of Internet users not to disclose their identity. However, respect for anonymity does not prevent member States from taking measures in order to trace those responsible for criminal acts, in accordance with national law, the ECHR and other international agreements in the fields of justice and the police.

7.1.1.13. “Independent and effective review and supervision”

#1 What does the CoE draft explanatory material say about this?

"129. Paragraph 5 (of Article 15) clarifies that supervisory authorities cannot effectively safeguard individual rights and freedoms unless they exercise their functions in complete independence. A number of elements contribute to safeguarding the independence of the supervisory authority in the exercise of its functions, including the composition of the authority; the method for appointing its members; the duration of exercise and conditions of cessation of their functions; the possibility for them to participate in relevant meetings without undue restrictions; the option to consult technical or other experts or to hold external consultations; the availability of sufficient resources to the authority; the possibility to hire its own staff; or the adoption of decisions without being subject to external interference, whether direct or indirect."

#2 Is this sufficient or are there open questions?

The Explanatory note to the modernised Convention 108 provides helpful guidance as regards the "independence" of review and supervision, yet less so as regards its "effectiveness".

#3 Where might one find further clarity?

The 25 May 2021 Grand Chamber judgment of the European Court of Human Rights in the case Centrum för Rättvisa v. Sweden (25 May 2021) offers further clarity as regards requirements for effective review and supervision. It should be noted, however, that the case concerns the compatibility of a legal framework for bulk interception with the European Convention on Human Rights. Thus, not every criteria for "end-to-end safeguards" and "end-to-end judicial oversight" that the Court spelled out in this particular judgment might be readily transferable so as to form general effective review and supervision criteria of all forms of data processing by Member States.

Still, we list it here because the judgment spells out specific attributes of effective review and supervision that delegations might find helpful for arriving at a common and better understanding of the term "effective supervision and review": For example, this might include that (the paragraphs listed below are those in the Centrum för Rättvisa v. Sweden (25 May 2021) case, our emphasis)

- an *assessment* should be made at *each stage* of the (data) process(ing) of the necessity and proportionality of the measures being taken (paragraph 264)
- the independent authorising body should be informed of both the purpose of the interception and the bearers or communication routes likely to be intercepted (paragraph 266)
- justifications should be *scrupulously recorded* and be subject to a process of *prior internal authorisation* providing for s*eparate and objective verification* of whether the justification conforms to the principles of necessity and proportionality (269)
- the initial authorisation and any subsequent renewals, the selection of bearers, the choice and application of selectors and query terms, and the use, storage, *onward transmission and deletion* of the intercept material – should also be subject to supervision by an independent authority" (paragraph 270)
- supervision should be sufficiently robust to keep the "interference" to what is "necessary in a democratic society" (paragraph 270)

- the supervising body should be in a position to assess the necessity and proportionality of the action being taken, having due regard to the corresponding level of intrusion into the Convention rights of the persons likely to be affected. In order to facilitate this supervision, *detailed records should be kept* by the intelligence services at *each stage of the process*. (paragraph 270)

7.1.2. Key notions used in the articles exempt by Art. 11

7.1.2.1. “processed fairly and in a transparent manner” (Article 5 paragraph 4)

7.1.2.2. “scientific or historical research purposes or statistical purposes” (Article 5 paragraph 4)

7.1.2.3. “competent supervisory authority” (Articles 7 paragraph 2 and Article 14 paragraph 5 and 6)

7.1.2.4. “means of exercising the rights” (Article 8 paragraph 1)

7.1.2.5. “take into consideration the subjects view” (Article 9 paragraph 1 littera a)

7.1.2.6. “Reasonable intervals and without excessive delay or expense” (Article 9 paragraph 1 littera b)

7.1.2.7. “intelligible form” (Article 9 paragraph 1 littera b)

7.1.2.8. “remedy” (Article 9 paragraph 1 littera f)

7.1.2.9. “effectiveness of the measures (Article 4 paragraph 3 littera a)

7.1.2.10. “effectiveness of safeguards” (Article 14 paragraph 6)

7.1.2.11. “contribute actively to this evaluation process“ (Article 4 paragraph 3 littera b)

7.1.2.12. “relevant information” (Article 14 paragraph 5)

7.1.2.13. “prevailing legitimate interests” (Article 14 paragraph 6)

7.1.2.14. “supervisory authorities’ powers of investigation and intervention” (Article 15 paragraph 2 littera a)

7.1.2.15. “administrative sanctions” (Article 15 paragraph 2 littera c)

7.2. Further Explanatory Material on Art. 11 of the Convention 108+

7.2.1. Extract of the Explanatory report

32.The term “law of the Parties” denotes, according to the legal and constitutional system of the particular country, all enforceable rules, whether of statute law or case law. It must meet the qualitative requirements of accessibility and previsibility (or “foreseeability”). This implies that the law should be sufficiently clear to allow individuals and other entities to regulate their own behaviour in light of the expected legal consequences of their actions, and that the persons who are likely to be affected by this law should have access to it. It encompasses rules that place obligations or confer rights on persons (whether natural or legal) or which govern the organisation, powers and responsibilities of public authorities or lay down procedure. In particular, it includes States' constitutions and all written acts of legislative authorities (laws in the formal sense) as well as all regulatory measures (decrees, regulations, orders and administrative directives) based on such laws. It also covers international conventions applicable in domestic law, including EU law. Furthermore, it includes all other statutes of a general nature, whether of public or private law (including the law of contracts), together with court decisions in common law countries,or in all countries, established case law interpreting a written law. In addition, it includes any act of a professional body under powers delegated by the legislator and in accordance with its independent rule-making powers.

91. No exceptions to the provisions of Chapter II are allowed except for a limited number of provisions (Article 5 paragraph 4, Article 7 paragraph 2, Article 8 paragraph 1 and Article 9) on condition that such exceptions are provided for by law, that they respect the essence of the fundamental rights and freedoms, and are necessary in a democratic society for the grounds listed in litterae a. and b. of the first paragraph of Article 11. A measure which is "necessary in a democratic society" must pursue a legitimate aim and thus meet a pressing social need which cannot be achieved by less intrusive means. Such a measure should, furthermore, be proportionate to the legitimate aim being pursued and the reasons adduced by the national authorities to justify it should be relevant and adequate. Such a measure must be prescribed by an accessible and foreseeable law, which must be sufficiently detailed.

92. All processing of personal data must be lawful, fair and transparent in relation to the data subjects, and only processed for specific purposes. This does not in itself prevent the law enforcement authorities from carrying out activities such as covert investigations or video surveillance. Such activities can be done for the purposes of the prevention, investigation, detection or prosecution of criminal offences and the execution of criminal penalties, including the safeguarding against and the prevention of threats to national security and public safety, as long as they are laid down by law and constitute a necessary and proportionate measure in a democratic society with due regard for the legitimate interests of the data subjects.

93. The necessity of such exceptions needs to be examined on a case-by-case basis and in light of the essential objectives of general public interest, as is detailed in litterae a. and b. of the first paragraph. Littera a. lists some objectives of general public interest of the State or of the international organisation which may require exceptions.

94. The notion of "national security" should be interpreted on the basis of the relevant case law of the European Court of Human Rights. (footnote 13)

Footnote 13: The relevant case law includes in particular the protection of state security and constitutional democracy from, inter alia, espionage, terrorism, support for terrorism and separatism. Where national security is at stake, safeguards against unfettered power must be provided. Relevant decisions of the European Court of Human Rights can be found at the Court's website (hudoc.echr.coe.int).

95. The term "important economic and financial interests" covers, in particular, tax collection requirements and exchange control. The term "prevention, investigation and prosecution of criminal offences and the execution of criminal penalties" in this littera includes the prosecution of criminal offences and the application of sanctions related thereto. The term "other essential objectives of general public interest" covers inter alia, the prevention, investigation, detection and prosecution of breaches of ethics for regulated professions and the enforcement of civil law claims.

96. Littera b. concerns the rights and fundamental freedoms of private parties, such as those of the data subject himself or herself (for Example when a data subject's vital interests are threatened because he or she is missing) or of third parties, such as freedom of expression, including freedom of journalistic, academic, artistic or literary expression, and the right to receive and impart information, confidentiality of correspondence and communications, or business or commercial secrecy and other legally protected secrets. This should apply in particular to processing of personal data in the audio-visual field and in news archives and press libraries. In order to take account of the importance of the right to freedom of expression in every democratic society, it is necessary to interpret notions relating to that freedom, such as journalism, broadly.

97. The second paragraph leaves open the possibility of restricting the provisions set out in Articles 8 and 9 with regard to certain data processing carried out for archiving purposes in the public interest, scientific or historical research purposes, or statistical purposes which pose no recognisable risk of infringement to the rights and fundamental freedoms of data subjects. For instance, this could be the case with the use of data for statistical work, in the public and private fields alike, in so far as this data is published in aggregate form and provided that appropriate data protection safeguards are in place (see paragraph 50).

98. The additional exceptions allowed to Article 4 paragraph 3, Article 14 paragraphs 5 and 6, and Article 15 paragraph 2, litterae a., b., c., and d., in respect of processing activities for national security and defence purposes are without prejudice to applicable requirements in relation to the independence and effectiveness of review and supervision mechanisms. (Footnote 14)

Footnote: 14: For Parties that are Council of Europe member States, such requirements have been developed by the case law of the European Court of Human Rights under Article 8 of the ECHR (see in particular ECHR, Roman Zakharov v. Russia, 4 December 2015, paragraph 233; Szabó and Vissy v. Hungary, 12 January 2016, paragraphs 75 et seq.)

7.2.2. Extracts from the Draft Explanatory Report (CAHDATA(201-6)02)

89. Exceptions to the principles for protection of personal data are allowed in a strictly restrictive manner, for a limited number of provisions when such exceptions are provided for

by law and are necessary in a democratic society for the specific grounds exhaustively listed in litterae a. and b. of the first paragraph of Article 9. A measure which is "necessary in a democratic society" must pursue a legitimate aim and thus meet a pressing social need which cannot be achieved by less intrusive means. Such a measure should furthermore be proportionate to the legitimate aim being pursued and the reasons adduced by the national authorities to justify it should be relevant and sufficient. Such a measure must be prescribed by an accessible and foreseeable law, which must be sufficiently detailed.

90. The necessity of such measures needs to be examined on a case-by-case basis and in light of limited legitimate aims only, as is detailed in litterae a and b of the first paragraph. Littera a lists the major interests of the State or of the international organisation which may require exceptions. These exceptions are very specific to avoid giving Parties unduly wide leeway with regard to the general application of the Convention.

91. The notion of "national security" should be restrictively understood in the sense of protecting the national sovereignty of the concerned Party against internal or external threats, including the protection of the international relations of the Party, and interpreted on the basis of the relevant case-law of the European Court of Human Rights which includes in particular the protection of state security and constitutional democracy from espionage, terrorism, support for terrorism and separatism. Where national security is at stake, safeguards against unfettered power must be provided.[1] Any measure affecting human rights must be subject to a form of adversarial proceedings before an independent body competent to review the reasons for the decision and relevant evidence.[2] The individual must be able to challenge the executive's assertion that national security is at stake[3]. Everyone affected by a measure based on national security grounds has to be guaranteed protection against arbitrariness[4]. The long-term storage of information in security files must be supported by reasons relevant and sufficient with regard to the protection of national security[5].

92. The term "important economic and financial interests" should be read restrictively and covers, in particular, tax collection requirements and exchange control. The term "prevention, investigation and suppression of criminal offences" in this littera includes the prosecution of criminal offences.

93. Littera b. concerns major interests of private parties, such as those of the data subject himself or herself (for Example when a data subject's vital interests are threatened because he or she is missing) or of third parties, such as freedom of expression, including freedom of academic, artistic or literary expression, and the right to receive and impart information, confidentiality of correspondence and communications, or else business or commercial secrecy and other legally protected secrets.

94. The third paragraph leaves open the possibility of restricting the rights with regard to certain data processing carried out for historical, statistical or scientific purposes which pose no identifiable risk to the protection of personal data and where restrictions to the data subject's rights are justified. For instance, the use of data for statistical work, in the public and private fields alike, in so far as this data is published in aggregate form and having all their identifiers stripped enters into that hypothesis provided that appropriate data protection safeguards are in place (see paragraph 51).

Bibliography

CCBE (Council of Bars & Law Societies of Europe). (2019). Recommendations on the Protection of Fundamental Rights in the Context of 'National Security' 2019. Available at: https://www.ccbe.eu/fileadmin/speciality_distribution/public/documents/SURVEILLANCE/SVL_Guides_recommendations/EN_SVL_20190329_CCBE-Recommendations-on-the-protection-of-fundamental-rights-in-the-context-of-national-security.pdf.

Council of Europe. (n.d.). Freedom of expression and information. Available at: https://www.coe.int/en/web/freedom-expression/freedom-of-expression-and-information

CTIVD. (2018). Review Report: The multilateral exchange of data on (alleged) jihadists by the AIVD, Nr. 56. Available at: https://english.ctivd.nl/documents/review-reports/2018/04/24/index

de Ridder, Wouter. (2019). A simple yet existential demand: let oversight bodies work together. Available at: https://aboutintel.eu/simple-oversight-demands/

EOS-Committee, Comiteri, CTIVD, IPCO, OA-IA. (2018). Charter of the Intelligence Oversight Working Group. Available at: https://eos-utvalget.no/wp-content/uploads/2020/01/Charter-Intelligence-Oversight-Working-Group_signed-12-December-2019.pdf

ECHR (European Court of Human Rights). (2013). National security and European case-law. Available at: https://rm.coe.int/168067d214

FRA (European Union Agency for Fundamental Rights). (2017). Surveillance by intelligence services: fundamental rights safeguards and remedies in the EU - Volume II: field perspectives and legal update. Available at: https://fra.europa.eu/sites/default/files/fra_uploads/fra-2017-surveillance-intelligence-services-vol-2_en.pdf

Greer, Steven. (1997). The exceptions to Articles 8 to 11 of the European Convention on Human Rights. Human rights files No. 15. Available at: https://www.echr.coe.int/LibraryDocs/DG2/HRFILES/DG2-EN-HRFILES-15(1997).pdf

Guild, Elspeth and Thorsten Wetzling. (2021). Germany's BND Act & recent CJEU case law. Available at: https://aboutintel.eu/bnd-reform-cjeu/

Pierucci, Alessandra and Jean-Philippe Walter. (2020). Better protecting individuals in the context of international data flows: the need for democratic and effective oversight of intelligence services, Joint Statement by the Council of Europe's Chair of Convention 108 and the Council of Europe's Data Protection Commissioner. Available at: https://rm.coe.int/statement-schrems-ii-final-002-/16809f79cb

Renan, Daphne. (2016). The Fourth Amendment as Administrative Governance, Available at: http://www.stanfordlawreview.org/wp-content/uploads/sites/3/2016/06/68_Renan_-_68_Stan._L._Rev._1039.pdf

Special Rapporteur on the right to privacy to the Human Rights Council. (2019). Right to Privacy - Report of the Special Rapporteur on the right to privacy to the Human Rights Council 2019, A/HRC/40/63. Available at: https://rm.coe.int/40th-hrc-session-report-of-the-special-rapporteur-on-the-right-to-priv/1680933f08

TIB and CTIVD. (2021). Council of Europe Convention 108+ and oversight on national security. Available at: https://english.ctivd.nl/latest/news/2021/02/17/index

UK Home Office. (2017). Interception of Communications. Draft Code of Practice. Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/593748/IP_Act_-_Draft_Interception_code_of_practice_Feb2017_FINAL_WEB.pdf