Strasbourg, 13 December 2024 **CDL-AD(2024)043**

Or. Engl.

EUROPEAN COMMISSION FOR DEMOCRACY THROUGH LAW

(VENICE COMMISSION)

REPORT

ON

A RULE OF LAW AND HUMAN RIGHTS COMPLIANT REGULATION OF SPYWARE

Adopted by the Venice Commission
at its 141st Plenary Session
(Venice, 6-7 December 2024)

On the basis of comments by

Mr Iain CAMERON (Member, Sweden)
Mr David A. KAYE (Member, United States of America)
Mr Tuomas OJANEN (Member, Finland)
Mr Timothy OTTY (Member, United Kingdom)
Ms Tamar KALDANI (Expert, Georgia)

Table of Contents

I. Introduction

1. By letter of 6 December 2023, the then-President of the Parliamentary Assembly of the Council of Europe (PACE), Mr Tiny Kox, requested the Venice Commission, pursuant to Resolution 2513 (2023) of PACE on "Pegasus and similar spyware and secret state surveillance",[1] to conduct a study on the legislative framework and practice on targeted surveillance of all Council of Europe member States (in priority Poland, Hungary, Greece, Spain and Azerbaijan; and then Germany, Belgium, Luxembourg, the Netherlands and all the other member States).

2. By Resolution 2513(2023) PACE had requested some member States to inform it and the Venice Commission about the use of Pegasus and similar spyware[2] or to clarify the legal framework for its use and any applicable oversight mechanisms.[3] In particular, PACE requested the Venice Commission to assess the legislative framework and practice on targeted surveillance of all member States (in priority those concerned by the Resolution), in order to assess if such frameworks contained adequate and effective guarantees against any possible abuse of spyware, having regard to the Convention and other Council of Europe standards.[4]

3. Messrs Iain Cameron, David A. Kaye, Tuomas Ojanen and Timothy Otty acted as rapporteurs for this report. Ms Tamar Kaldani, former First Vice-Chair and elected member of the Consultative Committee of the Council of Europe Convention 108, was invited to join the working group as an expert.

4. In reply to the request, the Venice Commission has conducted a comparative study to assess the existing rules on targeted surveillance and notably on the use of spyware in its member States. The Venice Commission has considered the legal provisions of the States that sent official information to PACE[5] and of those on which the members of the Venice Commission/experts provided information by replying to a questionnaire which was prepared by the rapporteurs (CDL-PI(2024)014).[6] Further information has been collected through desk research.[7] The material collected is available by country and by question.

5. This report was drafted on the basis of the comments by the rapporteurs and the results of the comparative research. It was adopted by the Venice Commission at its 141st Plenary Session (Venice, 6-7 December 2024).

---

[1] PACE, Resolution 2513(2023), *Pegasus and similar spyware and secret state surveillance*, 11 October 2023. As explained in the Resolution and further detailed below Pegasus is a spyware product developed by an Israeli company, NSO and is now perhaps the most widely known of the different spyware products to have been in use by States in recent years.

[2] Poland, Hungary, Greece, Spain, and Azerbaijan, § 11 of the Resolution.

[3] Germany, Belgium, Luxembourg and the Netherlands, § 13 of the Resolution.

[4] § 15 of the Resolution.

[5] PACE shared with the Venice Commission the responses it received, namely from Azerbaijan, Germany, Greece, Luxembourg, the Netherlands, Poland, and Spain. Belgium and Hungary did not send replies.

[6] Replies to this questionnaire and to a more general request for information, sent in February 2024, in which the rapporteurs enquired about the legal framework regulating the use of Pegasus and other equivalent spyware, were received from Austria, Belgium, Bulgaria, Bosnia and Herzegovina, Canada, Croatia, Cyprus, Denmark, Estonia, Finland, France, Germany, Greece, Iceland, Ireland, Italy, Kosovo, Kyrgyzstan, Liechtenstein, Lithuania, Malta, the Republic of Moldova, Monaco, Morocco, the Netherlands, North Macedonia, Norway, Poland, Portugal, Romania, San Marino, Serbia, the Slovak Republic, South Korea, Spain, Sweden, Switzerland, Türkiye, Ukraine, the United Kingdom, the United States of America.

[7] *See notably* European Parliament, *The use of Pegasus and equivalent surveillance spyware - The existing legal framework in EU Member States for the acquisition and use of Pegasus and equivalent surveillance spyware* ("PEGA Study"), 5 December 2022 and the report of the Fundamental Rights Agency, *Surveillance by intelligence services: Fundamental rights safeguards and remedies in the EU - 2023 update* ("FRA Report"), 24 May 2023. The FRA Report provides a partial update of the 2015 and 2017 FRA reports.

II. Background and scope of the report

6. There exist several terms which refer to the kind of targeted surveillance at issue: "spyware", "intrusive surveillance software", or the more neutral term "computer network exploitation". In this report, the Venice Commission will use the term "spyware" which is also used in the PACE request.

7. The term spyware is an umbrella term which embraces intrusive surveillance software that can be used for interference with electronic devices, notably smartphones or computers, without the user's knowledge, and which allows the operator to penetrate the device and, depending on the specific tool, track geolocation in real-time, read all data stored and all communications made (bypassing possible safeguards, such as encryption), and take control of whatever hardware and software is available on the device, including microphones or cameras.[8] Contrary to conventional wiretapping, spyware can potentially provide full, retroactive access to files and messages created in the past, passwords, and metadata about past communications. EU Regulation 2024/1083 (European Media Freedom Act), Article 2 § 20 defines "intrusive surveillance software"[9] as "*any product with digital elements specially designed to exploit vulnerabilities in other products with digital elements that enables the covert surveillance of natural or legal persons by monitoring, extracting, collecting or analyzing data from such products or from the natural or legal persons using such products, including in an indiscriminate manner*".[10]

8. Spyware can infect the targeted devices through a variety of mechanisms: it can be planted through physical access to a device, but also by means of remotely planting a "trojan", a virus or programme. This may involve sending a message (such as SMS, e-mail or online messaging applications) that includes a link to a website that, if visited, will infect the device. Some tools use the so-called "zero-click attack", in which the mere receipt of a message causes the spyware infection, while no user interaction is required. Spyware infections require high-level technical expertise to detect, and their presence on a device can be difficult to prove.[11] The most intrusive spyware, such as Pegasus, can secretly turn a mobile phone or a personal computer into a 24-hour surveillance device, enabling an operator to gain complete access to all sensors and information on the personal device.

9. The abuse of commercial spyware has resulted in very serious human rights violations. It has been reported by an international coalition of investigative journalists that more than 50,000 individuals, including human rights defenders, political opponents, lawyers, diplomats, Heads of State and nearly 200 journalists from 24 countries had been identified as potential targets of state spyware.[12] The PACE Report found that there is mounting evidence that Pegasus and similar spyware have been used illegally or for illegitimate purposes by several member States, including against journalists, political opponents, human rights defenders and lawyers.[13] PACE has also pointed to evidence that Council of Europe member States have exported intrusive surveillance with characteristics similar to Pegasus to third countries with authoritarian regimes and a high risk of human rights violations.

10. Several different spyware tools have been developed, used, and exported by or for States around the globe. The huge expansion of digital communications has driven States to find tools

[8] The term "spyware" as such is not used in the legislation the Venice Commission has assessed. See also paragraph 40 below.
[9] Recital 25 of the European Media Freedom Act (see below) includes "spyware" within the meaning of "intrusive surveillance software".
[10] Regulation (EU) 2024/1083 of the European Parliament and of the Council of 11 April 2024 establishing a common framework for media services in the internal market and amending Directive 2010/13/EU (European Media Freedom Act). The Media Freedom Act entered into force on 7 May 2024 and will fully apply as of 8 August 2025.
[11] *Ibidem*, p. 7 ff.
[12] Forbidden stories, *The Pegasus project: a worldwide collaboration to counter a global crime*, 18 July 2021.
[13] Parliamentary Assembly of the Council of Europe, Report no. 15825, *Pegasus and similar spyware and secret state surveillance* ("PACE Report"), 20 September 2023, Explanatory memorandum §§ 6-63.

to enable surveillance in law enforcement and intelligence environments. With national telecommunications networks, States have enacted obligations on telecommunications providers to provide law enforcement and intelligence agencies with access to communications in an accessible form, bypassing the encryption that has become standard for telecommunications providers and device manufacturers. In some jurisdictions, particularly when the suspect is aware that s/he is being investigated, it can be possible for a court to order the manufacturer or provider to "open" the device. However, law enforcement and intelligence agencies have argued that when a court is not in a position to enforce such an order against the manufacturer or provider, and therefore a court-mandated access is unavailable, it is necessary to obtain access in some way to the communication devices (laptops, mobile phones, etc.) themselves.

11. States further assert a need to use spyware to defend national and public security against threats, including crime, and against activities aimed at destabilising their fundamental constitutional, political, economic, or social structures. Technological developments limit the ability of law enforcement authorities to access data through previously established methods. As a result, some states claim that intrusive surveillance of a suspect's device is necessary to execute their investigations, in particular in order to gain access to data otherwise protected by encryption.[14]

12. However, as will be apparent from the preliminary description of the capacities of spyware made above, the potential for unjustified or disproportionate intrusive surveillance using such a tool is significant. If left unregulated, spyware is a potent surveillance weapon that can be used to curtail human rights, censor and criminalise criticism and dissent and harass (or even suppress) journalists, human rights activists, political opponents and repress civil society organisations. Substantial forensic reporting by civil society organisations – by Citizen Lab[15], Amnesty Tech[16], and AccessNow[17], among others – has identified significant evidence of abusive surveillance using spyware technologies.

13. The use of spyware by a law enforcement or an intelligence agency constitutes an instance of "targeted surveillance" since it focuses on identified individuals or groups. Targeted

---

[14] As found by the Belgian Standing Committee for oversight of intelligence and security services: "*[W]ithout denying the continuing importance of more traditional intelligence methods and techniques such as human intelligence gathering and analysis "HUMINT" (Human Intelligence), it is indisputable that the use of technological intelligence and security tools such as Remote Infection Technologies is likely to significantly strengthen the information position of the services. […] [I]t has to be said that the declining effectiveness of more traditional communications interception measures is demonstrated by the growing complexity of information gathering and processing. This situation is increasingly hindering, if not preventing, the intelligence cycle and its objectives of anticipating security risks and providing the authorities with adequate advice on how to deal with threats, or even hinder them directly*"; *see* Comité permanent de contrôle des services de renseignement et de securite, *Enquête de contrôle à la suite des révélations sur l'utilisation du logiciel PEGASUS*, 17 October 2022. See also House of Commons, Canada, *Device investigative tools used by the Royal Canadian Mounted Police and related issues – Report of the Standing Committee on Access to Information, Privacy and Ethics*, November 2022, section on Benefits of Technological Investigative Tools, pp. 8-9.

[15] *See, e.g.*, Citizen Lab, *Pay No Attention to the Server Behind the Proxy: Mapping FinFisher's Continuous Proliferation*, 15 October 2015; "*The Million Dollar Dissident: NSO Group's iPhone Zero-Days used against a UAE Human Rights Defender*", 24 August 2016; "*HIDE AND SEEK: Tracking NSO Group's Pegasus Spyware to Operations in 45 Countries*, 18 September 2018; *Pegasus vs. Predator Dissident's Doubly-Infected iPhone Reveals Cytrox Mercenary Spyware*, 16 December 2021; "*GeckoSpy: Pegasus Spyware Used against Thailand's Pro-Democracy Movement*, 17 July 2022; "*PREDATOR IN THE WIRES: Ahmed Eltantawy Targeted with Predator Spyware After Announcing Presidential Ambitions*", 22 September 2023.

[16] *See, e.g.*, Amnesty Tech, *Forensic Methodology Report: How to catch NSO Group's Pegasus*, 18 July 2021; *Dominican Republic: Pegasus spyware discovered on prominent journalist's phone*, 2 May 2023; *Global: A Web of Surveillance – Unravelling a murky network of spyware exports to Indonesia*, 2 May 2024.

[17] *See, e.g.,* Access Now, *Hacking in a war zone: Pegasus spyware in the Azerbaijan-Armenia conflict*, 25 May 2023; *Hacking Meduza: Pegasus spyware used to target Putin's critic*, 13 September 2023; *New spyware attacks exposed: civil society targeted in Jordan*, 1 February 2024; *Exiled, then spied on: Civil society in Latvia, Lithuania, and Poland targeted with Pegasus spyware*, 30 May 2024.

surveillance in the present report means the deliberate monitoring of specific individuals or groups by a law enforcement or an intelligence agency.[18]

14. Traditionally, targeted surveillance has been resource intensive. This still appears to be the case for the use of spyware. Spyware exploits vulnerabilities in device security or particular applications, which are then employed to give the "hacker" control over the device as such.[19] Because of the significant technical expertise required, some governments purchase spyware services from a commercial operator, which can be expensive.[20] Having said this, as noted by the Venice Commission in its Rule of Law Checklist, technical developments make surveillance "easier and easier to use".[21] This means that surveillance technology becomes accessible to a range of states which may lack domestic technical expertise as well as systematic human rights safeguards. It is therefore crucial that the strict safeguards which uphold human rights and the rule of law are applied to the development and use of technologies such as spyware, to avoid providing States with the power to interfere with the safeguards and the guarantees that are necessary in democratic society.

15. On the basis of the results of the comparative study on the legal frameworks governing use of spyware in its member States and having as a benchmark the jurisprudence of the European Court of Human Rights (ECtHR) on targeted surveillance, the Venice Commission has attempted to identify the minimum safeguards that should be in place, when dealing with such intrusive measures of targeted surveillance, to prevent unlawful surveillance practices. The complexity of the legislative frameworks in question, the lack of comprehensive and practical information on the implementation of existing international standards, such as Article 9 of Convention 108, as well as the scarce specific regulation of spyware were important factors to consider when preparing the report. The examples quoted in the report are not meant to be exhaustive and are presented for comparative purposes only. The fact that they are mentioned does not mean that the Venice Commission tacitly endorses them as compatible with human rights and the rule of law. Ultimately, it will be for the ECtHR, in the context of adjudicating upon "spyware"-related cases,[22] to set the applicable minimum standards in this domain. An important contribution to define those standards at global level may also be provided by the Committee of Convention 108+ in relation to its work on the interpretation of Article 11 and to the evaluation and follow-up mechanism to be carried out under Convention 108+.

[18] As opposed to strategic or "bulk" surveillance, which rather consists of blanket collection of very large amounts of electronic content data and metadata which are then subjected to computer analysis with the help of selectors.
[19] Apps are normally designed so as to be "sealed" from one another. Even if a vulnerability can be found, it may not be capable of being exploited sufficiently. Repeated "attacks" may have to be made, and even then they may not be successful. There is often a considerable element of chance involved whether or not the spyware will be effective or not. As the actual process of remotely executing spyware will be highly technical and usually very time-consuming, it requires a team of specialists to do it.
[20] In 2016, it was reported that NSO charged government agencies $650,000 to use Pegasus on ten targets, plus a $500,000 installation fee
[21] Venice Commission, CDL-AD(2016)007, *Rule of law Checklist*, § 118.
[22] See ECtHR *Brejza v. Pologne and 8 others* (communication), no 27830/23 and 8 others, 3 July 2024; see also, *Koukakis v. Greece* (communication), no. 37659/22, 10 January 2024; for a factual background of the case *see Report of the investigation of alleged contraventions and maladministration in the application of Union law in relation to the use of Pegasus and equivalent surveillance spyware* (2022/2077(INI)) ("PEGA Report"), 22 May 2023, §§ 202-210 and PACE Report, cited above, Explanatory memorandum §§ 31-35. The case has eventually been declared inadmissible by the ECtHR because of abuse of the right of application, *see* ECtHR, *Koukakis v. Greece* (decision), no. 37659/22, 11 June 2024.

III. The case-law of the ECtHR and other European and international standards concerning spyware[23]

A. The case-law of the ECtHR on the right to respect for private life and previous work of the Venice Commission

16. It is not disputed that personal data contained in a device, including one's mobile/telephone communications, are covered by the notions of "private life" and "correspondence". The use of spyware directly interferes with the right to respect for one's private life as enshrined in Article 8 of the European Convention on Human Rights (ECHR) and Article 17 of the International Covenant on Civil and Political Rights (ICCPR). Such interference may only be allowed under three conditions: the conditions under which the interference may occur must be defined clearly by law, in legislation or regulations which must be accessible to the individual concerned and protect that individual from arbitrariness through, inter alia, precision and foreseeability; it shall further one of the legitimate aims listed in Article 8 § 2 of the ECHR;[24] and it must correspond to a pressing social need[25] and be proportionate to the legitimate aim pursued so that it can be considered necessary in a democratic society. The three conditions listed above are cumulative, and each has an autonomous function to fulfil. Disproportionate interferences with the right to respect for one's private life are not compatible with the Convention, even for the sake of achieving legitimate and highly pressing objectives.

17. Depending on the circumstances of individual cases, the use of spyware may also impinge on several other human rights and freedoms (e.g. the right to a fair trial, freedom of religion, freedom of expression, freedom of assembly and association, freedom of movement, right to free elections, the right to freedom from discrimination,[26] the right not to be subjected to inhuman/degrading treatment[27]) either directly or through a "chilling effect" resulting from a first-order intrusion into privacy rights that also impacts the individuals' enjoyment or exercise of their

---

[23] An extensive overview of existing and applicable Council of Europe and international standards is found in the PACE Report, cited above, Explanatory memorandum §§ 64-80.

[24] Or, in the framework of the ICCPR, comply with the provisions, aims and objectives of the Covenant, see Office of the High Commissioner for Human Rights, *CCPR General Comment No. 16: Article 17 (Right to Privacy) The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation*, 8 April 1988, §§ 3-4.

[25] ECtHR, *Dudgeon v. the United Kingdom*, no. 7525/76, 22 October 1981, § 51.

[26] Issues can indeed arise when surveillance is based on algorithms or on other methods to "profile" individuals for targeted surveillance on account of their membership in a racial, ethnic cultural, religious, political or other group. Non-discriminatory profiling in a criminal law context is, in principle, a permissible means of law-enforcement activity: detailed profiles based on factors that are statistically proven to correlate with certain criminal conduct may be effective tools in order to better target limited law-enforcement resources. However, a difference in treatment on the basis of a criterion such as race, ethnicity, national origin or religion will only be compatible with the principle of non-discrimination if it is supported by objective and reasonable grounds. Thus, the difference in treatment must pursue a legitimate aim. In addition, there has to be a reasonable relationship of proportionality between the difference in treatment and the legitimate aim sought to be realised. It follows that if law-enforcement authorities use broad profiles that reflect unexamined generalisations, their practices of targeted surveillance may constitute disproportionate interferences with human rights. In particular, profiling based on stereotypical assumptions that persons of a certain "race", national or ethnic origin or religion are particularly likely to commit crime may lead to practices that are incompatible with the principle of non-discrimination. If selective targeting occurs, it should be based on individual conduct, not inborn characteristics or membership in a group. *See* Fundamental Rights Agency, *Preventing unlawful profiling today and in the future: a guide*, 5 December 2018, in particular section 2 on "Lawful profiling: principle and practice"; see also EU Network of Independent experts on Fundamental Rights, *Ethnic profiling*, December 2006; European Commission against Racism and Intolerance, *ECRI General Policy Recommendation n° 11 on combating racism and racial discrimination ijn policing*, 29 June 2007; Committee on the Elimination of Racial Discrimination, *General recommendation no. 36 (2020) on preventing and combating racial profiling by law enforcement officials*, 17 December 2020.

[27] In at least one jurisdiction – the United Kingdom – it has been alleged that the use of spyware has caused psychiatric harm to its victim so as to fall within an exemption to sovereign immunity and to allow civil proceedings to be brought against the foreign state allegedly responsible (see *Al Masarir v Kingdom of Saudi Arabia [2023] 2 WLR 549*, 19 August 2022; *Shehabi v The Kingdom of Bahrain [2024] EWCA Civ 1158*, 4 October 2024).

other rights.[28] Moreover, spyware may affect not only the human rights of direct targets but also of other persons, including children, in contact with them. As the right to the protection of private life (and the right to the protection of personal data which is recognised as an important attribute of the right to private life in the case law of the ECtHR) tends to be the fundamental right most often and most directly affected by the use of spyware, this report focuses on interferences with Article 8 of the ECHR.

18. The ECtHR has yet to develop case-law specifically on the proportionality of the use of spyware. However, it has already produced a substantial body of case-law in the field of surveillance in general, where it has differentiated between targeted surveillance and bulk interception.[29] In the case of *Roman Zakharov v. Russia*, the Court's Grand Chamber has codified the following minimum safeguards that should be set out in law, when dealing with measures of (secret) targeted surveillance, in order to avoid abuses of power: (i) a clear statement of the nature of offences which may give rise to an interception order; (ii) a definition of the categories of people liable to have their telephones tapped; (iii) a limit on the duration of the interception; (iv) the procedure to be followed for examining, using and storing the data obtained; (v) the precautions to be taken when communicating the data to other parties; and (vi) the circumstances in which recordings may or must be erased or destroyed.[30] In the same judgment, the ECtHR has also laid down a general obligation of retrospective notification, subject to exceptions.[31] Applying the above-mentioned jurisprudence, the ECtHR has recently assessed the Polish national legislation on secret surveillance and found three separate violations of Article 8 ECHR.[32]

19. By contrast, bulk or mass surveillance enables the security services to adopt a proactive approach, looking for hitherto unknown dangers rather than investigating known ones. The ECtHR dealt with the issue of bulk interception in the landmark cases of *Big Brother Watch and Others v. the United Kingdom* [GC] and *Centrum För Rättvisa v. Sweden* [GC]. The ECtHR found that bulk interception is "a valuable technological capacity to identify new threats in the digital domain"[33] and of vital importance to contracting States in identifying threats to their national security.[34] While Article 8 ECHR does not prohibit the use of bulk interception to protect national security and other essential national interests against serious external threats, and States enjoy a wide margin of appreciation in deciding what type of interception regime is necessary, for these purposes, the discretion afforded to them in operating such a system must necessarily be narrow and a number of safeguards will have to be present.[35]

---

[28] Council of Europe, *Pegasus spyware and its impacts on human rights* ("DGI Spyware report"), 2022, chapter 5: "[…] *Targeted or mass surveillance also creates a climate of self-censorship. Fearing that each action and move is under scrutiny, people will be less likely to communicate about specific topics online or offline. The chilling effect of surveillance could also lead to social isolation. Targets, as well as their relatives and friends, might refrain from interactions in fear of being harmed or surveilled. More importantly, real-time access to location and communication data could also pose a life-threatening risk to the individual and endangers its physical and mental integrity* […]."

[29] For targeted and secret surveillance, *see*, among many others, ECtHR, *Roman Zakharov v. Russia* [GC], no. 47143/06, 4 December 2015 and *Kennedy v. the United Kingdom*, no. 26839/05, 18 May 2010; for bulk interception *see* ECtHR, *Big Brother Watch and Others v. the United Kingdom* [GC], nos.58170/13 and 2 others, 25 May 2021 and *Centrum För Rättvisa v. Sweden* [GC], no. 35252/08, 25 May 2021.

[30] ECtHR, *Roman Zakharov v. Russia* [GC], cited above, § 231.

[31] *Ibid*., §§ 286 et ff., see Section V.H below.

[32] ECtHR, *Pietrzak and Bychawska-Siniarska and Others v. Poland*, nos. 72038/17 and 25237/18, 28 May 2024.

[33] ECtHR, *Big Brother Watch and Others v. the United Kingdom* [GC], cited above, § 323

[34] *Ibidem*, § 424; *see also* Venice Commission, CDL-AD(2015)011, *Report on the democratic oversight of Signals Intelligence Agencies*, § 47.

[35] ECtHR, *Big Brother Watch and Others v. the United Kingdom* [GC], cited above § 347. In particular, the Court has examined whether the domestic legal framework clearly defined: (i) the grounds on which bulk interception may be authorised; (ii) the circumstances in which an individual's communications may be intercepted; (iii) the procedure to be followed for granting authorisation; (iv) the procedures to be followed for selecting, examining and using intercept material; (v) the precautions to be taken when communicating the material to other parties; (vi) the limits on the duration of interception, the storage of intercept material and the circumstances in which such material must be erased and destroyed; (vii) the procedures and modalities for supervision by an independent authority of compliance with the above safeguards and its powers to address non-compliance; (viii) the procedures for

20. Drawing on the ECtHR's case law, it is noted that despite the differences, in practice there can be several overlaps between targeted and bulk interception. Any intrusion caused by the acquisition of associated communications data is multiplied by bulk interception, since such data can now be analysed and researched, making it possible to paint an intimate portrait of the person concerned by tracking his or her activities on social networks, their movements, internet browsing and communication habits, as well as their contacts.[36] Bulk material can be analysed to identify individual devices of interest which can then be the subject of targeted interception.

21. The Venice Commission has also previously considered surveillance issues. In 2015, it updated its Report on the democratic oversight of the Security Services[37] and produced a report on the democratic oversight of Signals Intelligence Agencies.[38] The present report should therefore be read in conjunction with these reports, which will be referred to in Section V. The Venice Commission has also adopted opinions on laws on targeted surveillance.[39]

B. Personal data protection

22. Although the right to the protection of personal data is not an autonomous right under the ECHR, the ECtHR has acknowledged that the protection of personal data is of fundamental importance to a person's enjoyment of his or her right to respect for private and family life, home and correspondence.[40]

23. The Council of Europe Convention 108,[41]the only legally binding international treaty in the personal data protection field with global relevance, sets the basic principles for data protection, safeguards for individuals, and supervision over the data processing operations, which are particularly important in the context of surveillance technologies, such as spyware.[42] Modernised Convention 108+[43] opened for signatures and ratifications in October 2018.[44]

1. Key requirements of Convention 108+

24. Convention 108+ establishes stronger requirements regarding the lawfulness of the processing, necessity, proportionality, purpose limitation, data quality and data minimisation, recalling that personal data processed should be adequate, relevant, and not excessive. The proportionality principle also applies in respect of the means and methods deployed during the surveillance. Convention 108+ provides individuals with greater control over their personal data and enhanced rights.[45] Furthermore, it is made clear that the requirement for a valid legal basis

---

independent ex post facto review of such compliance and the powers vested in the competent body in addressing instances of non-compliance, see § 361.

[36] ECtHR, *Pietrzak and Bychawska-Siniarska and Others v. Poland*, cited above, § 249.

[37] Venice Commission, CDL-AD(2015)010, *Report on the Democratic Oversight of the Security Services*.

[38] CDL-AD(2015)011, cited above.

[39] *See, among others*, Venice Commission, CDL-AD(2016)012, *Poland – Opinion on the Act of 15 January 2016 amending the Police Act and certain other acts*.

[40] ECtHR, *Satakunnan Markkinapörssi Oy and Satamedia Oy v. Finland*, no. 931/13, 27 June 2017, § 137.

[41] Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108)

[42] DGI Spyware report, cited above, p. 14.

[43] Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data as it will be amended by its Protocol CETS No. 223.

[44] 31 countries have so far ratified the Protocol amending Convention 108. The Modernised Convention will enter into force once ratified by all the 55 Parties to Convention 108 or, as from 11 October 2023, once 38 Parties to the Convention have ratified the Protocol.

[45] In its Article 9, the modernised Convention extends the catalogue of information to be transmitted to data subjects when they exercise their right of access. Furthermore, data subjects are entitled to obtain knowledge of the reasoning underlying the data processing, the results of which are applied to her/him. The right not to be subject to a decision which significantly affects the data subject which is based solely on an automated processing, without the data subject having her/his views taken into consideration. Lastly, data subjects have a right to object at any time to their personal data being processed, unless the controller demonstrates compelling legitimate grounds for

for processing applies in all circumstances without exception. Along with other obligations, data controllers must implement "privacy by design" and "privacy by default" in product or service development[46] and must carry out a prospective examination of the likely impact of data processing on human rights and fundamental freedoms.

25. A key requirement of Convention 108+ and the new generation of data protection laws is that personal data controllers (including intelligence and police) and, where applicable, data processors (including developers and service providers) must be able to demonstrate that the processing of personal data under their control complies with the principles (including lawfulness, purpose limitation, data minimisation, storage limitations, data quality) and obligations as set out in the Convention, including privacy by design, privacy by default and data protection impact assessment. Moreover, Article 6 of Convention 108+ provides that personal data revealing racial origin, political opinions or religious or other beliefs, as well as personal data concerning health or sexual life, may not be processed automatically unless domestic law provides appropriate safeguards. The same shall apply to personal data relating to criminal convictions. Thus, this provision effectively limits the direct use of the enumerated criteria in surveillance practices, although the use of such criteria in surveillance is not always forbidden. For instance, these criteria can be applied to targeted surveillance where there is specific intelligence suggesting that an indentifiable individual fulfilling these characteristics is preparing a specific serious crime or act amounting to a grave threat to national security.

26. The Privacy Impact Assessment (PIA) provided for in Article 10 § 2 of Convention 108+ is critical in the context of spyware, as it is a process designed to describe the processing of personal data, assess its necessity and proportionality, identify the impact of intended data processing on the rights and fundamental freedoms of data subjects and mitigate the risks arising out of the processing. A PIA does not have to indicate that all risks have been eradicated, but it should minimise the risks as far and as early as possible and assess whether any residual risks are justified.

27. The requirement that the grounds on which the processing of personal data is allowed should be clearly and precisely laid down by the law is one of the fundamental principles pertaining to the protection of personal data. The "quality" of the law requirement can also be derived from Article 11 of Convention 108+ to the extent that it explicitly requires that exceptions and restrictions are "provided for by law".[47]

28. It follows from these requirements that legislation giving authorities the power to interfere with privacy and personal data by using spyware and then further processing personal data obtained from the use of spyware should contain explicit and detailed provisions concerning the persons authorised to consult the data, the nature and category of the data, the procedure to be followed or the use that may be made of the information thus obtained. The requirement of explicit and sufficiently detailed and precise legal provisions also constitutes an essential guarantee against arbitrariness and abuse of power, which is of particular importance with regard to the use of spyware, due to the heightened potential for intrusive interference of such surveillance technologies.

---

the processing which override their interests or rights and fundamental freedoms, *see also* Council of Europe, *The modernised Convention 108: novelties in a nutshell*.

[46] The concept of "privacy by design" according to which the protection of every user's privacy must start at the design stage of IT systems. It was codified by Regulation (EU) 2016/679 (GDPR). It enables maximum protection of personal data rights from the design stage and during every use of a new technology. The principle entails that protection of personal data is no longer an option for companies but an obligation inherent in each of their activities.

[47] Paragraph 91 of the Explanatory Report of Convention 108+ furthermore specifies that "*such a measure must be prescribed by an accessible and foreseeable law, which must be sufficiently detailed*".

2. National security and personal data protection

29. By contrast to the provisions of Convention 108, under Convention 108+, data processing for reasons related to national security (and defence) can no longer be entirely exempted from the scope of application of the Convention (Article 11). The possible exceptions to a limited number of principles (Article 5 paragraph 4, Article 7 paragraph 2, Article 8 paragraph 1 and Article 9), are subject to the conditions set by the Convention. Namely, such exceptions must: (i) be provided by law; (ii) respect the essence of fundamental rights and freedoms and (iii) constitute a necessary measure in a democratic society on the basis of specified and limited grounds, including "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".

30. Also, under Article 11 § 3, processing activities for national security and defence purposes should be subject to independent and effective review and supervision under the domestic legislation of the respective State Party.

C. Work of international institutions and tribunals related to spyware

31. In addition to the work done by PACE, a thorough examination of the use of Pegasus and other spyware has been carried out by the European Parliament which established a committee of inquiry to investigate the use of the Pegasus and equivalent surveillance spyware (PEGA Committee).[48] The Committee produced a study on the use of Pegasus and equivalent surveillance spyware,[49] a report[50] and a recommendation to the European Council and the Commission.[51] In 2019, the United Nations Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression published a report on surveillance and human rights, which referred to the Pegasus spyware as an example of mobile device hacking used as a targeted surveillance tool in 45 countries.[52] In 2022, the United Nations Human Rights Commissioner for Human Rights found that the use of spyware "*should be limited to cases where it would serve to prevent or investigate a specific serious crime or act amounting to a grave threat to national security. Its use should be narrowly targeted to an investigation of the person or persons suspected of committing or having committed such acts. This should be a last resort […] all less intrusive measures should have been exhausted or have been shown to be futile and should be strictly limited in scope and duration. Only relevant data should be accessed and collected. The measures should also be subjected to rigorous independent oversight; prior approval by a judicial body is essential*. […]"[53] In 2023 the Council of Europe Commissioner for Human Rights issued a comment calling on Council of Europe member states to impose a strict moratorium on the export, sale, transfer, and use of highly intrusive zero-click spyware tools such

[48] European Parliament, *Decision of 10 March 2022 on setting up a committee of inquiry to investigate the use of the Pegasus and equivalent surveillance spyware, and defining the subject of the inquiry, as well as the responsibilities, numerical strength and term of office of the committee* (2022/2586(RSO)), 10 March 2022.
[49] PEGA Study, cited above.
[50] PEGA Report, cited above.
[51] *European Parliament recommendation of 15 June 2023 to the Council and the Commission following the investigation of alleged contraventions and maladministration in the application of Union law in relation to the use of Pegasus and equivalent surveillance spyware* (2023/2500(RSP)) ("EP Recommendation").
[52] United Nations, General Assembly, Human Rights Council, A/HRC/41/35, *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression* ("2019 UN SR Report"), 28 May 2019. *See also* United Nations Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms while Countering Terrorism, *Global Regulation of the Counter-Terrorism Spyware Technology Trade: Scoping Proposals for a Human-Rights Compliant Approach* (April 2023).
[53] Human Rights Council, *The Right to privacy in the digital age*, Report of the Office of the United Nations High Commissioner for Human Rights, A/HRC/51/17, 4 August 2022

as Pegasus, and to put in place a precise, human rights compliant legislative framework for the use of modern surveillance technology.[54]

32. Other relevant material, among others, include the 2023 Fundamental Rights Agency updated report on "Surveillance by intelligence services",[55] which partly updated the 2015 and 2017 reports by the same agency and provides a comprehensive review of the oversight mechanisms in place in the EU countries, and the 2022 Council of Europe report on Pegasus spyware and its impacts on human rights.[56]

33. In 2024, the aforementioned European Media Freedom Act, in its Recitals 25 and 26 has laid down some safeguards that shall be respected in order to permit the lawful use of intrusive surveillance software against media professionals.[57] Article 4 § 3 of the Act, in keeping with the broad protection of journalists recognised by international human rights law as democratic society's public "watchdog", provides the default standard that Member States ensure the protection of journalistic sources and confidential communications and not deploy spyware against media service providers or others that might result in disclosure of sources and communications. Article 4 § 5 provides for derogation from this standard protection, i.e. for the deployment of intrusive surveillance software, only in specific circumstances (see paragraph 95 below).

34. The Court of Justice of the European Union (CJEU) has also dealt with the use of surveillance technologies and their impact on fundamental rights in a number of landmark cases.[58]

---

[54] Council of Europe, Commissioner for Human Rights, *Highly intrusive spyware threatens the essence of human rights*, 27 January 2023.
[55] FRA Report, cited above.
[56] DGI Spyware report, cited above, p. 14.
[57] Recitals 25 and 26 read: *"(25) Intrusive surveillance software, including, in particular, what is commonly referred to as 'spyware', represents a particularly invasive form of surveillance over media professionals and their sources. It can be deployed to secretly record calls or otherwise use the microphone of an end-user device, film or photograph natural persons, machines or their surroundings, copy messages, access encrypted content data, track browsing activity, track geolocation or collect other sensor data, or track activities across multiple end-user devices. It has dissuasive effects on the free exercise of economic activities in the media sector. It jeopardises, in particular, the trusted relationship of journalists with their sources, which is the core of the journalistic profession. Given the digital and intrusive nature of such software and the use of devices across borders, it has a particularly detrimental impact on the exercise of economic activities by media service providers in the internal market. It is therefore necessary to ensure that media service providers, including journalists, operating in the internal market for media services can rely on robust harmonised protection in relation to the deployment of intrusive surveillance software in the Union, including where Member State authorities resort to private parties to deploy it;*
(26) Intrusive surveillance software should only be deployed where it is justified by an overriding reason of public interest, it is provided for in Union or national law, it is in compliance with Article 52(1) of the Charter as interpreted by the Court of Justice and with other Union law, it has been authorised ex ante or, in exceptional and urgent cases, subsequently confirmed by a judicial authority or an independent and impartial decision-making authority, it occurs in investigations of offences listed in Article 2(2) of Council Framework Decision 2002/584/JHA (9) punishable in the Member State concerned by a custodial sentence or a detention order of a maximum period of at least three years or in investigations of other serious offences punishable in the Member State concerned by a custodial sentence or a detention order of a maximum period of at least five years, as determined by the national law of that Member State, and provided that no other less restrictive measure would be adequate and sufficient to obtain the information sought. According to the principle of proportionality, limitations can be made to an individual's rights and freedoms only if they are necessary and genuinely meet objectives of general interest recognised by the Union. Thus, as regards specifically the deployment of intrusive surveillance software, it is necessary to ascertain whether the offence in question attains a threshold of seriousness as laid down in this Regulation, whether, following an individual assessment of all the relevant circumstances in a given case, the investigation and prosecution of that offence merit the particularly intrusive interference with fundamental rights and economic freedoms consisting in the deployment of intrusive surveillance software, whether there is sufficient evidence that the offence in question has been committed, and whether the deployment of intrusive surveillance software is relevant for the purpose of establishing the facts related to the investigation and prosecution of that offence."
[58] Among others, CJEU, *Digital Rights Ireland and Seitlinger and Others*, Joined cases C-293/12 and C-594/12, 8 April 2014; *Tele2 Sverige AB v Post- och telestyrelsen and Secretary of State for the Home Department v Tom Watson and Others*, Joined Cases C-203/15 and C-698/15, 21 December 2016; *Maximillian Schrems v. Data Protection Commissioner*, Case C-362/14, 6 October 2015; *Privacy International v Secretary of State for Foreign and Commonwealth Affairs and Others*, Case C-623/17, 6 October 2020; *La Quadrature du Net and Others v*

IV. Comparative findings concerning spyware law and practice

35. In order to conduct a comparative study on the legislative framework of its member states concerning the use of spyware, the Venice Commission based itself on the safeguards that have been developed by the ECtHR in its case-law on targeted surveillance.[59] In particular, it has asked its members to provide information on: (i) whether domestic legal frameworks allow for the use of spyware as a tool of targeted surveillance either in criminal or intelligence investigations; (ii) whether there are specific rules (covering notably the scope ratione *materiae*, *temporis* and *personae*) in place or whether the general rules on targeted surveillance (interception of communications) apply; (iii) the kind of data, if any, that could be collected with spyware; (iv) the existence of any official evaluation of the need for, or added value of, spyware; (v) the bodies in charge of authorising/approving measures of targeted surveillance in criminal and intelligence investigations; (vi) the national oversight mechanisms in place for the activities of the security services; and (vii) the availability of a post-surveillance notification mechanism or any other remedies.

36. The examples reported are not exhaustive and are only based on the available data, notably the replies provided to the questionnaire and the information that has been otherwise collected by the rapporteurs. Moreover, the Venice Commission reiterates that the examples quoted in the report are presented for comparative purposes only and not by way of endorsement of any particular approach taken.

A. Legal basis of use of spyware as a tool of targeted surveillance

37. Based on the above-mentioned safeguards, the Venice Commission firstly examined the existing legal framework for the use of spyware in its member states. It emerged that relatively few States have developed legislation that specifically regulates the use of intrusive surveillance tools/spyware: **Canada**, **Denmark**, **Finland**, **Germany**, **Italy**, **Luxembourg**, the **Netherlands**, **Norway**, **Spain**, **Sweden**, **Switzerland**, and the **United Kingdom**. In **Austria**, legislation on the use of spyware had been initially introduced in the context of criminal investigations. However, it was then struck down by the Constitutional Court which found that it constituted a disproportionate interference with human rights.[60] In some of the above States, specific rules (*ratione materiae, ratione personae and ratione temporis*), which deviate from the general framework in place for targeted surveillance measures, have been set up (see below section IV.C). In **Belgium**, **Bulgaria**, **Estonia**, **France**, **Hungary**, **Lithuania**, the **Republic of Moldova**, **North Macedonia**, **Poland**, **Romania**, and the **Slovak Republic**, while not separately and autonomously regulated, the use of spyware would be allowed under the notion of "special technical means/special investigative measures". In cases of countries with no specific spyware legislation in place, on the basis of information available, where the use of spyware is *prima facie*

Premier ministre and Others, Joined Cases C-511/18, C-512/18 and C-520/18, 6 October 2020. The FRA Reports of 2015, 2017 and 2023 include comprehensive lists of the judgments by the CJEU on issues of surveillance. A recent judgment of the Grand Chamber of the CJEU (*CG v. Bezirkshauptmannschaft Landeck*, Case C-548/21, 4 October 2024) dealt with access by the police to data contained in a mobile telephone, a related yet less intrusive interference with the deployment of an intrusive surveillance software. While recognising that personal data stored on a mobile telephone may constitute a particularly serious, interference with the fundamental rights of the data subject, the Court found that to consider that only the fight against serious crime is capable of justifying access to data contained in a mobile telephone would unduly limit the investigative powers of the competent authorities. This would result in an increased risk of impunity for criminal offences in general and therefore in a risk for the creation of an area of freedom, security and justice in the European Union. The Court nevertheless found that such an interference with private life and data protection must be provided for by law, which implies that the national legislature must define the factors to be taken into account for such access, such as the nature or categories of the offences concerned. In order to ensure compliance with the principle of proportionality in each specific case, data access must be subject to prior authorisation by a court or an independent authority, save in duly substantiated cases of urgency. Lastly, the data subject must be informed of the grounds for the authorisation as soon as the provision of this information is no longer likely to jeopardise the investigations.

[59] See paragraph 18 above.

[60] *See* paragraph 70 below.

not expressly prohibited, a possibility is that the general rules on targeted surveillance apply, and spyware could be seen as one method of obtaining relevant data, without specific rules governing it. While not specifically regulated, the case-law of courts of the **United States** shows that the domestic deployment of any surveillance technology should be governed by strict warrant requirements and its use have a restricted scope.[61]

38. The legislation in place in the countries which specifically regulate spyware mostly predates the "Pegasus" revelations. Only in **Greece** was specific legislation introduced following revelations that spyware had been misused, providing, *inter alia*, for a new legal framework for waiving the privacy of communications and allowing for the purchase of spyware by State authorities.[62]

39. In countries where the use of spyware is explicitly regulated, it can normally be used both by law enforcement agents in the context of criminal investigations and by security agencies in the context of intelligence investigations aimed at preventing threats to national security.[63] Sometimes, the legal authorisation to use spyware can be found in the same statute, sometimes in separate statutes.

40. Among the countries permitting the use of spyware, data is not available as to which exact tool the authorities are using,[64] in particular whether commercially developed spyware is used or whether the state has developed its own tools. States with extensive experience and resources in signals intelligence are likely to have developed their own tools. Based on the replies received, the Venice Commission could observe the following: in the **Netherlands** the Research and Data Centre of the Dutch Ministry of Justice and Security published an evaluation report on the Dutch surveillance powers for law enforcement authorities; this report clarified that the Dutch police used a commercial tool in the "vast majority" of cases. However, the name of the commercials tool(s) used is not public. In **Switzerland**, the Federal Administrative Court, in a ruling of 9

[61] The Fourth Amendment to the United States Constitution provides the foundation for the U.S. legal framework governing surveillance in the criminal justice system. A landmark decision is the Supreme Court 2018 *Carpenter v. United States*, which found unconstitutional the warrantless use of cell site location information, thus providing individuals with protections against the government seeking personal data from third parties. *Carpenter* provided a set of factors to assess the constitutionality of such surveillance practices when conducted without a judicial warrant, including factors of particular relevance to spyware, such as inter alia the revealing nature of the information collected and the amount of data sought by the government. Lower courts have found Fourth Amendment protections constrain government use of technologies that may be similar to spyware as defined above. For instance, in *United States v. Wilson*, the US Court of Appeals for the Ninth Circuit found that law enforcement installation of surveillance malware on a defendant's computer without a warrant was an illegal search and seizure. In *United States v. Saboonchi* courts held that law enforcement use of malware to remotely activate the defendant's laptop webcam was an unconstitutional search. These cases lead to the conclusion that spyware, given its intrusiveness, would likely be governed strictly by warrant requirements and scope of use. That said, the law's applicability generally to digital surveillance may be in some flux. For instance, an appellate court in *Tuggle v. United States* found the long-term use of a pole camera to monitor a person's home to be reasonable under the Fourth Amendment.

[62] The use of spyware by State agencies may be permitted, under the terms of a presidential decree which, has not been issued to this day (Article 13 of law 5002 of 2022).

[63] In Italy the law makes no explicit reference to the possibility of using spyware as a means of carrying out intelligence interceptions; some authors however, by way of interpretation, allow this possibility; in Norway, the Intelligence Service cannot use targeted surveillance, or other surveillance, on persons in Norway; in Spain, there is no specific regulation on the use of any spyware (including Pegasus) by intelligence services.

[64] Though in countries where it is used, spyware is called with different names: software/programme in Finland (Section 42 of the Coercive Measures Act; and Section 42 of the Act on Military Intelligence), Norway (Article 216 p of the Criminal Procedure Act) and Spain, (Chapter IX, Title VIII of the Code of Criminal Procedure); computer interceptor in Italy ("*captatore informatico*", as defined in Article 1(m) of the Ministerial Decree of 6 October 2022 as "*any disguised system, inoculated remotely, which, by eliminating the effects that prevent the knowledge of the communication or data, allows the interception of the audio-video contents and of the data exchanged or allows the interception face-to-face conversations, and remotely collects the positions taken by the equipment in the territory*"); on-device investigative tool/implant in Canada; technical device in the Netherlands (Regulation of Technical Devices in Criminal Procedural Law published on 11 July 2018 and Article 45 of the Dutch Act on Security and Intelligence Services); "Government software" or "GovWare" in Switzerland (as indicated in the government's explanatory report on the amendments to the Swiss Criminal Code).

January 2022,[65] ruling upon an appeal of a lawyer who demanded access to the contract for the spyware used by the Federal Office of Police and the Federal Intelligence Service, stated that there is a significant public interest in determining whether the software acquired by Switzerland is Pegasus. The Court found that knowledge of the information requested could put the measures taken by Switzerland at risk in the event of a concrete threat to its internal and external security, which would in turn hinder the work of the law enforcement authorities.

B. Type of information that may be collected through spyware

41. The Venice Commission further collected information on which kind of data could be collected through spyware in the countries that specifically regulate it. In **Canada** data that can be collected is limited to private communications, transmission data and/or the acquisition of static data from electronic devices. In **Denmark** the law does not set up any specific limitations in this respect. In **Finland** the law does not allow technical surveillance for collecting information on live communication nor on its identification data.[66] In **Germany**, "technical infiltrations/online searches" (as defined by the Federal Constitutional Court) have been considerably limited in their scope following a landmark ruling of the Federal Constitutional Court (Decision BvR 370/07).[67] In particular Articles 100d of the Code of Criminal Procedure and Article 49 § 7 the Federal Criminal Police Office Act provide that if there are factual indications for assuming that an online search measure will only lead to findings from the core area of private life, the measure shall be inadmissible. Moreover, as far as possible, technical measures shall be taken to ensure that data relating to the core area of private life are not collected. Following July 2021 Law "to adapt the constitutional protection law" (*Gesetz zur Anpassung des Verfassungsschutzrechts*), all 19 German intelligence services have the right to use state trojans to read ongoing communication on computers or smartphones and even past communication data.[68] In **Italy**, while the intrusive surveillance software has a potential for great intrusiveness,[69] the Italian Parliament has only expressly regulated the use of that investigative tool to carry out the interception of face-to-face conversation and only on mobile devices. In **Luxembourg** the Police can use spyware to capture computer data, whereas the Security Services can seek, in a targeted manner, information necessary for the performance of one of its missions, or monitor and control communications which cannot be technically intercepted using normal telecommunications networks.[70] In the **Netherlands** the law does not define which data can be collected by law enforcement authorities, but rather refers to the methods data can be collected or altered.[71] The General Intelligence and Security Service and the Military Intelligence and Security Service are authorised to intercept, receive, record, and listen to any form of conversation, telecommunications, or data transmission using a technical tool through an automated work, regardless of its location. This

[65] Available here; judgement is not yet final - the case is pending before the Federal Supreme Court.
[66] Article 23 § 2 of the Coercive Measure Act, Article 23 § 2 of the Police Act and Article 32 § 2 of the Military Intelligence Act.
[67] BVerfG, Judgment of the First Senate of 27 February 2008 - 1 BvR 370/07 -, (Engl. transl), paras 166 et seq. This authority is however limited to communication surveillance and does not allow access to other information on the hard drive or cloud. The software used must be strictly limited to communication surveillance.
[68] PEGA Study, cited above, § 4.5.
[69] The tool employed is potentially capable of intercepting communications between computers and telematic systems (emails, WhatsApp messages, Skype conversations, etc.), activating microphones and/or cameras and GPS, recording everything typed on the keyboard (so-called keylogging function) and everything that appears on the screen (so-called screenshots function). It can also infiltrate the memory of devices where data is stored, thus capturing all data and information contained in or passing through the infected device, as well as modifying any information stored or transmitted.
[70] Article 8 § 1(c) of the Loi SRE.
[71] These methods include: (i) determining the characteristics of the automated work or the user, such as identity or location; (ii) executing the special investigative power of targeted interception. It is possible to intercept communications, such as email or spoken word, using a technical device (including software). This is further detailed in the explanatory report of the Computer Crime Act III (e.g., Parliamentary Series II 2015-2016, 34372, no. 3, p. 9); (iii) executing the special investigative power of systematic observation, for example, to determine the location of the device used (e.g., Parliamentary Series II 2015-2016, 34372, no. 3, p. 14); (iv) recording data stored in the automated work; (v) making data inaccessible, such as child abuse materials (Parliamentary Series II 2015-2016, 34372, no. 3, p. 29), cfr. Article 126nba(1)(a) of the Dutch Code of Criminal Procedure.

authority also includes the power to decrypt conversations, telecommunications, or data transmissions.[72] In **Norway** the reading may include communications, electronically stored data and other information about use of the computer system or the user account.[73] In **Spain** Article 588 *septies*(a) of the Code of Criminal Procedure provides that a software can be installed to examine the content of a computer, electronic device, computer system, computer mass data storage instrument or database, without the knowledge of the owner or user. In **Sweden**, spyware can be used not only to intercept data or to monitor communication and location information, but to carry out audio and camera surveillance.[74] In **Switzerland**, the use of spyware in criminal proceedings is unequivocally restricted to intercept and recover the content of communications and telecommunications metadata in unencrypted form.[75] There are no apparent limitations insofar as data collected in intelligence proceedings are concerned; however, Article 26 § d of the Swiss Federal Act of 25 September 2015 on the Intelligence Service ("IntelSA") provides that the intrusion into computer systems and computer networks can be performed not only to gather information available there or transmitted from there but also to disrupt, prevent or slow down access to information where the computer systems and computer networks are being used for attacks on critical infrastructures. In the **United Kingdom** Section 99 § 2 of the Investigatory Powers Act 2016 provides communications, equipment data or any other information can be obtained through a targeted equipment interference warrant.

42. In several of the countries which use spyware, data protected by professional secrecy of a lawyer or doctor, or by the secrecy of sources of a journalist cannot be collected or analysed, or specific procedures are in place.[76]

---

[72] Articles 47(1) and 45(2)(b)(d) of the Act on Security and Intelligence Services,

[73] Article 216 o § 4. Noteworthy is the provision according to which the data reading must be arranged so that no information is unnecessarily captured about the use of the computer system by anyone other than the suspect. The reading must be carried out in such a way that there is no unnecessary risk of operational disruption or damage to equipment or data. The police shall, as far as possible, prevent the risk that, as a result of the implementation, someone is enabled to gain unauthorised access to the computer system or protected information or to commit other criminal acts.

[74] Cfr. Section 2 of Act (2020:62) on Secret data reading. Statistics published by the Prosecutor General however show that authorisation to remotely activate *video* surveillance on a device was given only four times in 2023. Authorisation to remotely activate audio surveillance on a device was also given only four times in 2023.

[75] Article 269ter of the Code of Criminal Procedure.

[76] See for example in Belgium Article 18/9 § 4 of the L. R&S stipulates that an exceptional method may only be used against a lawyer, doctor or journalist, or the means of communication they use for professional purposes, if the intelligence and security service has serious prior evidence that the lawyer, doctor or journalist is or was personally and actively involved in the creation or development of a serious potential threat. Article 2 § 2 of the law, however, prohibits intelligence and security services from obtaining, analysing or exploiting data protected by the professional secrecy of a lawyer or doctor, or by the secrecy of sources of a journalist; in Finland Section 82 of the Act on Military Intelligence provides that telecommunications interception, collecting data other than through telecommunications interception, on-site interception, technical observation, radio signals intelligence or network traffic intelligence shall not be targeted at communications or information in respect of which a party may not testify or has the right to refuse to testify (professional secrecy in the relationship between a lawyer and his client, clergy privilege and doctor-client privilege). Similar provisions can be found in the Coercive Measures Act and the Police Act. In Luxembourg, Article 88-2 § 6(3), provides that the installation of the technical device mentioned in paragraphs 2 and 3 of article 88-1 may not, on pain of nullity, be carried out in premises used for professional purposes, the home or its outbuildings within the meaning of articles 479, 480 and 481 of the Criminal Code, or the vehicle of a lawyer, doctor, professional journalist or publisher. In the Netherlands a special procedure is foreseen if the intelligence measure is carried out against a journalist or a lawyer (Art. 30 of the Intelligence and Security Services Act 2017). If the surveillance measure is used against a journalist and this may lead to the identity of a source of the journalist being revealed to the intelligence and security service, authorisation for the exercise of this power must be granted by the district court in The Hague, rather than from the minister. The court will apply the same criteria that the minister would otherwise apply, including compliance with the principles of necessity, proportionality and subsidiarity. The court may authorise the exercise of the power for a period of no more than four weeks, rather than the regular limit of three months. In Sweden, Act 2020:62 on secret data reading (§ 11) prohibits the use of targeted surveillance by means of spyware on the computers or phones of journalists, advocates, doctors or priests; in Switzerland, Article 271 of the Code of Criminal Procedure provides that In the case of surveillance of a person belonging to one of the professional categories listed in Art. 170 to 173, the sorting of information which is not relevant to the subject of the investigation or to the reason for which the person concerned is subject to surveillance must be carried out under the direction of a court. This sorting is carried out in such a way that the prosecuting authorities are not privy to any professional secrets. Discarded data must be

C. Specific rules *ratione materiae, personae and temporis* in States which regulate the use of spyware

43. As mentioned above, certain States have developed specific rules for the use of intrusive surveillance tools such as spyware and have accordingly tailored the requirements for law enforcement and intelligence agencies to make use of these tools, in particular insofar as the applicability *ratione materiae* and *temporis* of the surveillance measure is concerned. This section provides an overview of these specific rules in the countries which reported the use of spyware.

1. *Ratione materiae*

44. In **Denmark**, the investigation should concern an offence punishable by law with imprisonment for six years or more or an intentional violation of Chapter 12 or 13 of the Penal Code.[77]

45. In **Germany**, the narrower list of crimes provided in Section 100b of the Code of Criminal Procedure applies (rather than that foreseen at Section 100a). In the framework of intelligence investigations, the Federal Criminal Police Office can only access IT systems if certain facts justify the assumption that there is a danger to the (i) body, life or liberty of a person or (ii) such public goods, the threat to which affects the foundations or the existence of the federation or a country or the foundations of human existence.[78]

46. In **Italy**, spyware in the framework of criminal proceedings can only be used in the framework of particularly serious offences (such as, for example, mafia-type criminal association)[79] or, provided that the places and times in relation to which the spyware may be activated are determined, even indirectly, also for offences committed by public officials against the public administration for which a maximum penalty of at least five years' imprisonment is provided.[80]

47. In **Luxembourg** spyware can be used in the framework of criminal proceedings only when dealing with serious crimes, including offences against State security[81] and acts of terrorism and terrorist financing;[82] in the framework of intelligence investigations spyware could only be used in the presence of a threat or risk of threat to national security.[83]

48. In the **Netherlands** the legislator has provided for different requirements having regard to the degree of intrusiveness of the measure sought, in relation to the seriousness of the offences. For

---

destroyed immediately; they may not be used. The preliminary sorting of information referred to in para. 1 must not be carried out if: a. there are serious grounds for suspicion against the holder of the professional secrecy, and b. there are special reasons for doing so. Similar provisions are contained in Article 58 of the of the Swiss Federal Act of 25 September 2015 on the Intelligence Service ("IntelSA") for targeted surveillance carried out by security services.

[77] Section 791(b) of the Administration of Justice Act.

[78] Section 49 § 1 of the Federal Criminal Police Office Act.

[79] Article 51 § 3-*bis* and 3-*quater* of the Code of Criminal Procedure.

[80] In the first phase of application, spyware had been introduced only with reference to the most serious crimes of organised crime and terrorism; the extension in 2019 to offences against public administration has been the subject of various criticisms, in terms of the principle of necessary proportionality, *see* Senato della Repubblica, *Documento approvato dalla 2ª Commissione permanente (Giustizia) nella seduta del 20 settembre 2023 a conclusione dell'indagine conoscitiva sul tema delle intercettazioni*, cited above, p. 43.

[81] As provided in articles 101 to 123 of the Criminal Code.

[82] As provided in Articles 135-1 to 135-6, 135-9 and 135-11 to 135-16 of the Criminal Code.

[83] The law specifies at Article 8 § 1(c) the nature of potential threats to national security: (i) espionage and interference; (ii) violent extremism; (iii) terrorism; (iv) proliferation of weapons of mass destruction or defense-related products and technologies; (v) organised crime and cyber-threats, insofar as they are linked to any of the above threats. The law explicitly excludes internal political surveillance from the security service's remit. The scope of this mission also extends to the security of foreign states and international and supranational organisations with which Luxembourg has signed agreements.

three categories of methods through which data can be collected or altered,[84] the measure can be requested in cases of suspicion of a serious offence where pre-trial detention is permitted (mainly offences carrying a penalty of at least four years). Two other more intrusive methods may be used[85] only for offences punishable by a penalty of at least eight years or designated as an offence under the law in the Investigation in a Computer System Decree[86] are considered. Intelligence services can employ spyware when targets (individuals or organisations) pose a threat to the national security or democratic order of the Netherlands.[87]

49. In **Norway**, the possibility of spyware use is limited to very serious crimes, i.e. crimes which carry a penalty of more than 10 years in prison.[88]

50. In **Spain** this type of measure is only authorised for specific offences (committed by criminal organisations, terrorism, offences against minors or persons with disabilities, offences against the constitution, treason or affecting national defence, offences committed through computer tools).[89]

51. In **Sweden**, there is a distinction between data reading not involving and involving activating a device's microphone to record sound. In the former case a rather wide list of offences for which communication interception is permitted applies.[90] For secret data reading which involves activation of the device's microphone to record sound, the list of permitted offences is much shorter: only those punishable by a minimum sentence of four years of imprisonment, as well as a small number of security offences (espionage etc.) punishable by a lower minimum sentence.[91]

52. In **Switzerland**, spyware can be used in criminal proceedings only for the narrow list of offences for covert investigations pursuant to Article 286 paragraph 2 CPC (for other targeted surveillance measures the broader list of Article 269 applies). In intelligence investigations, Article 27 of the IntelSA limits the possibility of gathering information to the specific cases mentioned in Article 19 § 2 (a-d) or the safeguard to other important national interests.

53. In the **United Kingdom** a targeted thematic equipment interference warrant can only be issued: (i) in the interests of national security, (ii) for the purpose of preventing or detecting serious crimes or (iii) in the interests of the economic well-being of the UK, so far as those interests are also relevant to the interests of national security.[92]

54. Lastly it is noted that a standard test of least intrusiveness/respect of proportionality is present in most of the countries on which information has been collected. This requires the requesting authority to demonstrate among others that there were no other less intrusive means to obtain

[84] Pursuant to Article 126nba § 1(a): (i) identifying and recording certain characteristics of the computer system or of the person using it, such as the identity and location of the computer system; (ii) an order to record communications following penetration; (iii) systematic surveillance order.
[85] (iv) capture of data stored in the computer system; and (v) data can be made inaccessible, including their (temporary) deletion.
[86] Available here.
[87] Article 8(2)(a) and 10(2)(a) of the Act on intelligence and security services
[88] Article 216 o and p; or other crimes of illegal intelligence activities against state secrets, revelation of state secrets, other illegal intelligence activities, participation in violent associations, influence by foreign intelligence services, incitement and recruitment to terror, travels with the intent of terror, participation in and recruitment to illegal military activity abroad, deprivation of liberty offences, human trafficking, production and dissemination of materials sexualizing children, receiving of stolen goods, money laundering, violations of the law on export control of strategic products, technology etc., and certain violations of the law on immigration.
[89] Article 588 *septies* of the Code of Criminal Procedure.
[90] Cfr. Section 4 of Act (2020:62) on Secret data reading which refers to Chapter 27 section 18a of the Code of Judicial Procedure.
[91] Cfr. Section 6 of Act (2020:62) on Secret data reading which refers to Chapter 27 section 2 d of the Code of Judicial Procedure.
[92] Section 102(5) of the Investigatory Powers Act 2016.

the information sought, and the authorisation body to find that the conduct authorised is proportionate to what is sought.[93]

2. *Ratione personae*

55. **Denmark**,[94] **Finland**,[95] **Italy**, the **Netherlands**, **Norway**,[96] **Spain**[97] limit the possibility to use spyware only to devices owned by the suspects of the offences provided for by law or by those who pose national security/equivalent threats, as established in the relevant domestic legal framework. In **Belgium**,[98] **Germany**,[99] **Sweden**,[100] **Switzerland**,[101] and the **United Kingdom**,[102] third parties who are sufficiently linked to the main target can also be the object of spyware surveillance.

3. *Ratione temporis*

56. From the comparative analysis it emerges that time limits for the authorisation of use of spyware as a tool of targeted surveillance are in most of the cases examined shorter when the authorisations are given in the framework of criminal proceedings compared to the authorisations in intelligence investigations.

[93] For example, in Belgium (Article 90*ter* § 1 of the Code of the Criminal Procedure); Canada (Section 21 § 2(b) of the Canadian Security Intelligence Service Act); Sweden (Section 3 of Act (2020:62) on Secret data reading); Switzerland (Article 27 IntelSA); the United Kingdom (Section 102(1)(b) of the Investigatory Powers Act 2016).
[94] Section 791(b) of the Administration of Justice Act.
[95] Article 23 § 3 of the Coercive Measures Act.
[96] Article 216 o § 4 of the Criminal Procedure Act. Insofar as intelligence investigations are concerned, it needs to be specified that the Intelligence Service cannot use targeted surveillance, or other surveillance, of persons in Norway. There is an explicit ban in Article 4 § 1 of the 2020 Intelligence Service Act.
[97] Article 588 *septies*(c) of the Code of Criminal Procedure.
[98] Article 90-*ter* § 1 of the Code of Criminal Procedure: surveillance can be ordered against persons presumed, on the basis of specific facts, to be in regular communication with a suspect.
[99] Pursuant to Section 100b § 3 of the Code of Criminal Procedure, where it is to be assumed, on the basis of certain facts, that: (i) the accused uses the other person's information technology systems; and (ii) the interference with the accused's information technology systems alone will not lead to the establishment of the facts or to the determination of the whereabouts of a co-accused. See also Section 49 § 3 of the Federal Criminal Police Office Act (when unavoidable).
[100] Section 4a of Act (2020:62) on Secret data reading.
[101] In criminal proceedings, Article 270 of the Code of Criminal Procedure provides that, in addition to the accused, third parties can be monitored if there is specific information that: (i) the accused uses the postal address or the telecommunications service of the third party, or (ii) the third party receives certain communications on behalf of the accused or passes on communications from the accused to another person. Likewise, the Federal Intelligence Service may order an information gathering measure requiring authorisation in relation to a third party if there is reason to believe that the person from whom it is intended to gather the information is using premises, vehicles or storage facilities belonging to the third party or the latter's postal addresses, telecommunication connection points, computer systems or computer networks in order to transmit, receive or store information.(Article 28 of the Swiss Federal Act of 25 September 2015 on the Intelligence Service ("IntelSA"). The measure may not be ordered if the third party belongs to one of the professional groups mentioned in Articles 171–173 of the Code of Criminal Procedure.
[102] Section 101 of the IPA 2016.

57. In criminal proceedings, in countries which use spyware the time limits span from 15 days[103] to six months,[104] with time-limits of four weeks,[105] one month[106] or three months[107] also being reported.

58. In intelligence investigations, this goes from four weeks,[108] to six months,[109] with other countries providing for time-limits of one month,[110] 40 days,[111] two months,[112] or three months.[113]

D. Authorisation of targeted surveillance measures

59. Insofar as the authorisation of targeted surveillance measures in the framework of criminal investigations/proceedings is entrusted to the judiciary in the overwhelming majority of the States on which data is available,[114] the approach differs as to the authorisation of targeted surveillance measures in intelligence investigations. In **France**,[115] **Germany**,[116] **Luxembourg**,[117] the **Netherlands**,[118] such authorisation is entrusted to the executive backed up by an independent authorisation body. In **Belgium**, a reasoned decision by the head of the security

[103] Italy (Article 267 § 3 of the Code of Criminal Procedure), Norway (Article 216 o § 5 of the Code of Criminal Procedure).
[104] United Kingdom, Article 116 § 2 (b) of the Investigatory Powers Act.
[105] Denmark (Section 783 of the Administration of Justice Act), the Netherlands (Article 126nba § 3 of the Code of Criminal Procedure).
[106] Belgium (Article 90-*quater* of the Code of Criminal Procedure); Finland (Article 24 of the Coercive Measures Act); Germany (Section 100e § 2 of the Code of Criminal Procedure - after a total period of six months it is the higher regional court which decides on any further extension orders); Luxembourg (Article 88-2 § 4 - renewable for a maximum total period of one year); Spain (Article 588 *septies* (c) of the Code of Criminal Procedure - renewable for a maximum total period of three months); Sweden (Section 18 of Act (2020:62) on Secret data reading – renewable; the Act also provides that if the conditions for the authorisation have changed, the surveillance is to cease immediately. Figures from 2023 show that the average period of authorisation was 21 days, with the median period being 13 days).
[107] Switzerland (Article 274 of the Code of Criminal Procedure).
[108] Denmark (Section 783 of the Administration of Justice Act).
[109] Finland (Article 24 of the Police Act and Article 33 of the Act on Military Intelligence); United Kingdom (Article 116 § 2 (b) of the Investigatory Powers Act).
[110] Sweden (Section 18 of Act (2020:62) on Secret data reading – renewable; the Act also provides that if the conditions for the authorisation have changed, the surveillance is to cease immediately. Figures from 2023 show that the average period of authorisation was 21 days, with the median period being 13 days).
[111] Italy (Article 4-*bis* § 1 of Law no, 144/2005).
[112] Belgium (Article 18/10 § 1).
[113] Germany (Section 49 § 6(3) of the Federal Criminal Police Office Act); Luxembourg (Article 7 § 1 Loi SRE), the Netherlands (Article 49 § 4 of the Act on Intelligence and Security Services 2017), Spain (Unique Article, Law 2/2002 Regulating The Prior Judicial Control Of The National Intelligence Center); Switzerland (Article 26 § 6 IntelSA).
[114] Notable exceptions are Ireland, Malta and the United Kingdom, *see* respectively at footnotes 120, 146 and 121 below.
[115] If the Prime Minister decides not to consider a negative opinion delivered by the National Commission for Control of Intelligence Techniques (*Commission nationale de contrôle des techniques de renseignement,* CNCTR), the CNCTR must immediately refer the case to the Council of State. The Council takes the final decision.
[116] In Germany the federal intelligence services are not permitted to carry out telecommunications interceptions at source until they have received orders from the Federal Ministry of the Interior and Community and the operation has been cleared by the G10 Commission (a commission composed of five members, at least three of whom must be qualified to hold judicial office appointed by the Parliamentary Oversight Panel), while the Federal Intelligence Service (BND) requires clearance from the Independent Oversight Council (Unabhängiger Kontrollrat) before it can undertake computer network exploitation measures. According to Section 23 § 7 of the Federal Intelligence Service Act, the Council must authorise data searches before their use. In case of urgency, one member of the Council can authorise such measures, but they have to be reviewed by the Council as soon as possible.
[117] Ordered by the Ministerial Intelligence Committee at the written request of the Director of the National Intelligence Agency and after approval by a Special Commission composed of senior magistrates, namely the President of the Superior Court of Justice, the President of the Administrative Court and the President of the District Court of Luxembourg (Article 7 § 4 of the Loi SRE)
[118] The head of service of the General Intelligence and Security Service (AIVD) or the Military Intelligence and Security Service (MIVD). A minister must authorise the use of this investigative power in Article 45 Act on intelligence and security services. The Investigatory Powers Commission (TIB) further conducts a review of the lawfulness of using this power prior to its use.

services department is required, following the assent of a specialised administrative commission.[119] In **Ireland**[120] and the **United Kingdom**,[121] both the executive and the judiciary have roles to play in the procedure authorising targeted surveillance measures. In **Bulgaria**, **Bosnia and Herzegovina**,[122] **Canada**, **Croatia**,[123] **Denmark**, **Estonia**,[124] **Finland**,[125] **Greece**,[126] **Iceland**, **Italy**,[127] **Kosovo**,[128] **Kyrgyzstan**, **Lithuania**,[129] the **Republic of**

[119] The Commission responsible for overseeing specific and exceptional data collection methods intelligence and security services (BIM Commission), composed of three magistrates and chaired by an examining magistrate.

[120] Judicial authorisation is required in relation to certain types of surveillance devices (such as the planting of audio bugs or covert video cameras) under the Criminal Justice (Surveillance) Act 2009 whereas authorisation from the executive (the Minister of Justice) is required in relation to interception of telephone communications under the Interception of Postal Packets and Telecommunications Act 1993. The Communication (Retention of Data) Act 2011, as amended by the 2022 Act entrusts the High Court with the power to retain Schedule 2 data (location and communications traffic data). Access to internet source data and Schedule 2 data is granted by a District Court judge. Insofar as user data is concerned, there is no requirement for authorisation by a judge or an independent body.

[121] Section 108 of the Investigatory Powers Act: both in the context of criminal and intelligence investigation, the Investigatory Powers Commissioner (IPC) approves the warrants for equipment interference at the request of public authorities, such as the Secretary of State, intelligence agencies, police and local authorities. The IPC is supported by a team of Judicial Commissioners. They are appointed by the Prime Minister but must hold or have held high judicial office.

[122] The President of the Court of Bosnia and Herzegovina or a judge delegated by him/her. A decision of the Constitutional Court of Bosnia and Herzegovina (U-21/16 of 1 June 2017) declared unconstitutional the provision (Article 78, paras 3, 4 and 5 of the Law on the Intelligence and Security Agency of Bosnia and Herzegovina) that previously granted the Director General of the Security Services Agency the possibility to approve the intelligence measure with the consent of the Chairman of the Council of Ministers of Bosnia and Herzegovina if the delay would cause irreparable damage to the security of Bosnia and Herzegovina. Relying on the ECtHR jurisprudence, the Court found that the law did not request the Director General to send a written request to the judge nor did it prescribe within which period the judge must either approve or suspend the application of these measures.

[123] Judicial warrant of the highest court (the Supreme Court of the Republic of Croatia) is needed for the following more intrusive measures: secret surveillance of the communication content, postal censorship (secret surveillance of mail and other postage), secret surveillance and technical recording of the interior of facilities, closed spaces and objects, as well as the secret surveillance and monitoring, with audio recording of the content of communication between persons in open and public spaces (Article 36 of the 2006 Security and Intelligence System Act). Other less intrusive measures such as: secret surveillance of the telecommunications traffic data, location of the user and international telecommunications; secret surveillance and monitoring, with recording of images and photos of persons in open and public spaces; secret purchase of documents and objects can be taken if approved by one of the Directors of security and intelligence agencies within their respective scope of activities (Article 38).

[124] The President of an administrative court or an administrative judge appointed by him/her.

[125] But the mere installation and removal of a device or software does not need authorisation by a court, see Section 42 of the Act on Military Intelligence and Section 26 of the Coercive Measures Act.

[126] Pursuant to Article 4 of law 5002/2022, the relevant order (διάταξη) is issued by the competent prosecutor following a request by the Greek National Intelligence Agency (EYP). However, the competent prosecutor is detached (αποσπασμένος) on a full-time assignment to EYP (under Article 5§3 of law 3649/2008) and his independence is thereof often contested. The EYP's prosecutor's order must be confirmed by a second (high-ranked) prosecutor who serves either at the Court of Appeals or at the Supreme Court (Areios Pagos).

[127] Article 4 of Decree-Law No. 144 of 27 July 2005 assigns to the President of the Council of Ministers the power to authorise the Directors of the Security Intelligence Services referred to in Article 2 § 2 of Law No. 124 of 3 August 2007 to request authorisation for the interception of communications or conversations, including by telematic means, as well as for the interception of communications or conversations, even in the places referred to in article 614 of the Penal Code, if this is deemed necessary for the performance of the tasks entrusted to them by articles 6 and 7 of law no. 124 of 3 August 2007. The authorisation shall be requested from the Public Prosecutor's Office at the Court of Appeal in Rome, that shall grant the authorisation if the conditions laid down in Article 4-bis are fulfilled.

[128] A Supreme Court Judge upon a request from the Director or Deputy Director of the Kosovo Intelligence Agency (KIA), *see* Law No. 03/L-063 on the Kosovo Intelligence Agency.

[129] Article 10 of the Law on Criminal Intelligence.

Moldova,[130] **Monaco**, **North Macedonia**,[131] **Norway**,[132] **Portugal**,[133] **Romania**, **Serbia**,[134] the **Slovak Republic**,[135] **Spain**,[136] **Sweden**,[137] **Ukraine**,[138] the **United States**[139] the authorisation power is entrusted to the judiciary. In **Korea** targeted surveillance measures in the framework of intelligence investigations require either permission from the chief presiding judge of the high court or approval from the President of the Republic.[140] In **Poland** authorisation power is normally entrusted to the judiciary,[141] but with regard to secret surveillance of foreign nationals, a special regime allows the authorities to conduct secret surveillance for three months without prior judicial authorisation.[142] In **Switzerland** the situation is different depending on whether the target is in Switzerland or abroad. In the first case, both the judiciary and the executive are involved.[143] In the second case, no judicial authorisation is required.[144] In **Hungary**[145] and **Malta**[146] the power

[130] With the *caveat* that the search of objects and documents, visual surveillance and gathering information can be ordered with the authorisation of the head of the specialised subdivision of the security services, cfr. Article 27 in conjunction with article 20 of Law no. 59/2012 on the special investigation activity.
[131] A Supreme Court judge at the demand of the Public Prosecutor of the Republic of North Macedonia on initiative of the Minister of Interior or Minister of Defence (Art. 20 of the Law on Communications Surveillance).
[132] Decisions on information gathering on cross boundary electronic information (internet traffic) requires approval by a court, see Article 8-1 of the 2020 Intelligence Act.
[133] A formation of three judges of the criminal chambers of the Supreme Court of Justice.
[134] According to the Law on Security Information Agency (Article 15), the decision on substantiated proposal of the Director of the Agency shall be made by the President of the Higher Court in Belgrade, i.e. a judge whom s/he shall delegate among judges from the Special department of that Court, which, according to the law, processes cases dealing with criminal offences relating to organised crime, corruption and other particularly severe criminal offences.
[135] Under Section 4a of the Protection Against Interception Act (PAIA), the jurisdiction lies with the regional court in whose district the requesting state authority is located. The only exception concerns crimes within the competence of the Specialised Criminal Court.
[136] The General Council of the Judiciary appoints a Supreme Court magistrate (from the administrative or criminal chamber) and a substitute to authorise interceptions of communications by intelligence services. Both must have at least three years' seniority in the Supreme Court. Their term of office shall be five years. This judge may authorise the interception of communications at the proposal of the Director of the CNI. On 8 September 2023, the Parliamentary Group of the Basque Nationalist Party presented a bill to amend Law 11/2002 and Organic Law 2/2002. The bill proposes a strengthening of prior judicial control by replacing the figure of the single Supreme Court magistrate in charge of these matters with a three-member chamber of Supreme Court magistrates. The bill has been adopted as a full initiative by the Congress on 27 February 2024 but has not yet been adopted by the Senate.
[137] Section 14 of the Act (2020:62) on Secret data reading.
[138] Article 15 § 2of Law no. 912-IX “on intelligence” provides that an intelligence agency may start conducting intelligence activities solely on the basis of a court decision. Under the decision of the head of the intelligence agency, an intelligence measure, can be extended for a period until a court decision is obtained, but not more than 72 hours from the moment of identification of the person.
[139] A specialised court (the United States Foreign Intelligence Surveillance Court), serve as an approval body for the use of surveillance tools. Collection of electronic communications of non-Americans located outside of the United States do not necessitate a warrant.
[140] Presidential approval is required only in special circumstances, while judicial permission is the standard procedure.
[141] The application for operational control is submitted to the competent district (*sąd okręgowy*) court along with the materials justifying the need for its implementation. Applications for the authorisation of surveillance are considered by single judges, and in accordance with Article 47a of the Law on the System of Common Courts (*Ustawa o ustroju sądów powszechnych*), they are assigned to a judge on duty. At the meeting, a prosecutor and a representative of the authority requesting operational control may participate.
[142] Article 9 § 1 of the Anti-Terrorism Act; *see Pietrzak and Bychawska-Siniarska and Others v. Poland*, cited above, §§ 53-54.
[143] The intelligence measure must be authorised by the president of a special section of the Federal Administrative Court (Article 29 IntelSA). Furthermore, the measure must be cleared by the Minister of Defence after consultation with the Minister of Foreign Affairs and the Minister of Justice. The Federal Council must be informed of cases of particular importance (Article 30 IntelSA).
[144] Only the Federal Council has the authority to decide on attacks on computer networks (Article 37 § 1, IntelSA). In the case of computer network exploitation (§ 2), it is the Minister of Defence, after consulting the Ministers of Foreign Affairs and Justice.
[145] According to the National Security Act, it is the Minister of Justice who is responsible for providing such authorisation.
[146] Under Chapter 391 of the Security Service Act, the Security Service of Malta can obtain authorisation for interception or interference with communications by means of a warrant issued by the Minister responsible for the Security Service, that is, as a norm, the Minister for Home Affairs. The law also applies to criminal proceedings.

to authorise targeted surveillance measures in the framework of intelligence investigations is entrusted to the executive.

60. In many States there is the possibility for law enforcement agencies or intelligence services, in exceptional and urgent cases (for example a danger to human life, health, public or state security) to carry out targeted surveillance in the absence of a prior authorisation, provided that such authorisation is granted by the relevant authorising body within a deadline that varies between 24 hours,[147] two days, [148] three days[149] and five days.[150]

E. Oversight mechanisms

61. The data available to the Venice Commission shows that national systems of oversight are diverse in terms of their legal frameworks, organisation, composition, mandate, functions and powers. A wide range of various actors appear to be involved in the national systems of oversight, including the judiciary (courts or tribunals or similar judicial bodies), parliaments (specialised parliamentary (sub-)committees), independent national institutions (e.g. ombudsmen) and specialised oversight agencies (with a special oversight mandate) that are not part of Parliament, the executive or the agencies they oversee.[151]

62. Oversight of targeted surveillance measures ordered in the context of criminal proceedings is normally entrusted to the judiciary in the framework of the general oversight of the ongoing proceedings.[152]

---

[147] Croatia (Article 36 § 2 of the Security and Intelligence System Act of the Republic of Croatia); Denmark (Article 783 of the Administration of Justice Act); Estonia (Article 126^4 § 2 and § 3 of the Code of Criminal Procedure); Finland (Article 24 of the Coercive Measures Act, Article 24 of the Police Act and Article 33 of the Act on Military Intelligence); the Slovak Republic, Section 114 § 2 of the PAIA.

[148] Italy (Article 267 of the Code of Criminal Procedure); Kosovo (Law No. 03/L-063 on the Kosovo Intelligence Agency), Romania (Article 141 § 1 of the Code of Criminal Procedure), San Marino (Article 4 of Law no. 98 of 21 July 2009 ("Law on Interceptions")).

[149] Kosovo (in the framework of criminal proceedings – Article 90 § 2 of the Code of Criminal Procedure); Ukraine (Article 15 of the Law "on intelligence"); the United Kingdom (Section 109 § 3 of the IPA 2016).

[150] Poland, Article 19 § 3 of the Police Act.

[151] A comprehensive overview of the oversight mechanisms in place in the EU countries in the context of surveillance by intelligence services is found in the FRA Report, cited above. *See also* Council of Europe, Commissioner for Human Rights, *Democratic and effective oversight of national security services*, May 2015.

[152] Some notable exceptions: in the Netherlands, in addition to the judiciary oversight during trial, the Inspection Authority of the Ministry of Justice and Security has a special mandate to check (mostly procedures) the use of hacking as an investigative power. They report annually but have no binding remedial powers. In Norway Article 216 h of the 1981 Criminal Procedure Act requires the establishment of an independent body tasked with controlling the legality of the use and storage of communication control measures (wire taps, surveillance, data taps). This body of at least 3 members (currently 6 members) is appointed by the Government. The leader must fulfil the requirements to qualify as a Supreme Court judge. The body can address any issue raised by individuals or organisation concerning police surveillance. The body may also by its own initiative address any issue and shall prioritise issues that have raised public debate or criticism. The body has access to all information related to communication control measures, including the actual wire taps, videos, data taps etc. In Sweden, in addition to judicial control, the Commission on Security and Integrity Protection (see the Act on Supervision of Certain Crime-Fighting Activities 2007:980) has the mandate to ensure that: the surveillance activities by the police, including the Security Police, and the latter's filing of personal data, are conducted in accordance with laws and other regulations. It is a 10-member body appointed by the government for a renewable period of no more than four years. All the parties in the Riksdag can propose a member of the Commission. Most of the parties have appointed experienced politicians, some of whom are active MPs. The Chair and Vice Chair shall be, or have been, a tenured judge or have other equivalent legal experience. Section 2 of the Supervision Act provides that SIN exercises its supervision through inspections and other investigations. It takes up a number of cases of its own motion every year. SIN reports annually to the government. An important provision is that according to which, unlike for other secret investigative measures, such as telecommunications interception, in cases of secret data reading there is a duty on an authorising court to inform SIN when an authorisation has been granted (section 21 of the Act on Secret data reading). This proactive duty gives SIN a better overview of how the Act is being applied, and to decide whether or not to initiate an oversight investigation. In the United Kingdom the Investigatory Powers Tribunal (IPT) is an entirely independent Tribunal established to hear complaints about the misuse of investigatory powers. It is comprised of individuals who have held high judicial office (and the President must be such a person) and senior lawyers. The

63. Insofar as the oversight over surveillance measures carried out by intelligence agencies is concerned, the Venice Commission observed that independent expert bodies carry out oversight in a number of countries, notably in **Austria**,[153] **Belgium**,[154] **Bulgaria**,[155] **Canada**,[156] **Croatia**,[157]

Tribunal also has power to award compensation and may make orders for the destruction of information and records of information and for the cancellation of warrants.

[153] The legal protection officer is responsible for monitoring data processing covered by Section 12 paras 1 and 1a of the Law on State Security and Intelligence and for legal protection under Section 6 §§ 1 and 2 of the Law. Competent organisational units shall obtain his/her authorisation in advance before carrying out tasks under Section 6 §§ 1 and 2 of the Law. S/he shall have insight into all necessary documents, records and processed data as well as grant him or her access to all premises under the conditions stipulated in the law. S/he can also lodge a complaint with the data protection authority on behalf of the affected persons. Each year, the legal protection officer reports to the Minister of the Interior on his/her activities and perceptions in the context of the fulfilment of his/her duties (Section 15 § 4 of the Law). The Directorate also reports to the Minister of the Interior and publishes a yearly report about current and possible developments relevant to the protection of the constitution in order to inform the public. The Independent Control Commission for the Protection of the Constitution shall be responsible for monitoring the activities of the organisational units and shall investigate allegations against activities of the organisational units. The Commission shall have access to all premises and be able to inspect documents and records. They submit an annual report to the Federal Minister of the Interior and the Standing Subcommittee of the Committee of Internal Affairs (of the National Council) as well as prepare an annual report informing the public about its activities. It may make recommendations to the Federal Minister of the Interior at any time.

[154] The Standing Committee R is responsible for overseeing the general operation of the intelligence and security services. It is a collegiate body: it comprises three members including a chairman, who must be a magistrate. It monitors the legality of decisions relating to specific and exceptional methods, as well as compliance with the principles of proportionality and subsidiarity. Where the Standing Committee R finds that a method is illegal, or that the principle of proportionality or subsidiarity has not been respected, it may terminate the method. All information gathered using the method must then be destroyed.

[155] The National Bureau for Control over Special Intelligence Means.

[156] The National Security and Intelligence Review Agency (NSIRA) is an independent and external review body that reports to Parliament. NSIRA is empowered to review Government of Canada national security and intelligence activities to ensure that they are lawful, reasonable and necessary. Following a review, NSIRA may make findings or recommendations that is considers appropriate. NSIRA also investigates public complaints regarding key national security agencies and activities, as well as complaints related to security clearances. Following an investigation, NSIRA must provide a report containing findings of the investigation and any recommendations that it considers appropriate. Findings and recommendations made by NSIRA are non-binding.

[157] The Council for Civic Oversight of Security Intelligence Agencies conducts a regular ex-post oversight of agencies, focused on the legality of work and implementation of special data gathering measures. It acts on the basis of requests sent by citizens and legal persons about potential irregularities and human rights violations. The Council is composed of seven citizens appointed by the Parliament on the basis of a public call for four-year mandates but with specific expertise and full security clearances. Where, in the conducted oversight, it is established that there have been some unlawful acts, the Chairperson of the Council shall notify the President of the Republic, the President of the Parliament, the President of the Government and the Chief State Attorney.

Denmark,[158] **Finland**,[159] **France**,[160] **Germany**,[161] **Greece**,[162] **Lithuania**,[163] the **Netherlands**,[164] **North Macedonia**,[165] **Portugal**,[166] **Sweden**.[167] In **Switzerland**, in addition to oversight by an expert body,[168] self-oversight and control and supervision by the executive[169] also exist. In the **United Kingdom** the oversight regime includes both expert bodies and the judiciary.[170] In the

[158] The Danish Intelligence Oversight Board has the power to fully access data collected by security services.
[159] The Intelligence Ombudsman oversees both the civilian intelligence and military intelligence authorities: the Finnish Security and Intelligence Service, the Intelligence Division of the Defence Command and the Finnish Defence Intelligence Agency. According to Section 15 of the Act on the Oversight of Intelligence Gathering, the Intelligence Ombudsman has competence to order the use of the intelligence method to be suspended or stopped if the Ombudsman considers that the intelligence authority has acted unlawfully in intelligence gathering.
[160] The CNCTR ensures that intelligence gathering is undertaken in compliance with the Code of Internal Security (Code de la Sécurité Intérieure). According to Article L831-1 of the Code, the CNCTR is composed of four parliamentarians (two members of the National Assembly and two senators), two members of the Council of State, two magistrates, one expert in electronic communication techniques. The Commission can deliver opinions on the use of intelligence gathering techniques, but these are not binding.
[161] The G10 Commission and the Independent Oversight Council. The former is constituted by Parliament according to Aricle. 10 § 2 of the German Grundgesetz and is limited to measures concerning telecommunications. It substitutes a control by the judicial branch. The latter acts as an administrative oversight body. Its members are six judges of the Federal Supreme Court and/or the Federal Administrative Court, who are elected by the Parliamentary Oversight Panel for 12 years.
[162] The Hellenic Authority for Communication Security and Privacy (ADAE). In accordance with article 6 of Law no. 3115/2003, ADAE has the power to conduct audits of installations, equipment, archives, data bases and documents of the EYP.
[163] The Intelligence Ombudsperson, established in 2022 is authorised to investigate cases where there are signs that intelligence institutions or officers are abusing their powers, infringing upon human rights and freedoms, compromising legitimate interests, or breaching regulations related to the processing of personal data for national security or defense purposes.
[164] The Dutch Review Committee on Intelligence and Security Services (CTIVD) is the oversight body for intelligence and security services. The CTIVD conducts oversight during the application of hacking as an investigative power, i.e., to test the technical risks involved and which devices are targeted. It also publishes reports about the lawfulness of hacking as an investigative power. However, as part of new legislation relating to 'State actors with cyber programs' in 2024, the CTIVD has limited binding powers in its oversight relating to hacking powers. Under this new legislation, intelligence and security services can appeal a decision of the TIB and CTIVD, and a judge can decide on this. There is no judgment available yet. Individuals who believe they have been treated unlawfully or unfairly by the intelligence and security services can file a complaint with the Minister of the Interior and Kingdom Relations or the Minister of Defence. If they are dissatisfied with how their complaint was handled, they can file a complaint with the CTIVD. The complaints department can issue binding decisions after unlawful conduct by the intelligence and security services.
[165] The Council for Civil Control is established to ensure civilian oversight of communication surveillance measures. Appointed by the Assembly of the Republic of North Macedonia, the Council comprises a president and six members, serving a three-year term without the possibility of reappointment. The members include three experts and three representatives from non-governmental organisations focused on human rights, security, and defense. The Council submits an annual report on its activities to the Assembly by the end of February each year. The Council can act on its own initiative or in response to citizen complaints.
[166] Council for the Oversight of the Intelligence System of the Portuguese Republic monitors and supervises the activity of the Secretary-General of the Intelligence System and the intelligence services, ensuring compliance with the Constitution and the law, with particular focus on the preservation of rights, freedoms and guarantees. It is composed of three eminent citizens, independent, elected by the Assembly of the Republic, by a majority of 2/3, for a four-year mandate; this body, among several powers, oversees the procedure for accessing telecommunications and internet data and the so obtained data by the intelligence services. The law of the Information System of the Portuguese Republic also establishes a Data Supervision Commission, composed of three magistrates from the Attorney General Office, appointed and empowered by the Attorney General of the Republic. The Data Supervision Commission is the competent public authority for monitoring compliance with the principles and compliance with the rules relating to quality and safeguarding the confidentiality and security of data obtained in accordance with the mandatory and legally bound procedure provided for in organic law nº 4/2017.
[167] *See* footnote 152 above.
[168] The Independent supervisory authority supervises the intelligence activities of the FIS, the cantonal enforcement agencies and other entities and third parties commissioned by the FIS, and monitors these activities with regard to their legality, appropriateness and effectiveness. It has access to all relevant information and documents, and to all premises used by entities subject to supervision. Cfr Articles 76-78 of the IntelSA.
[169] Cfr. Article 80 of the IntelSA.
[170] The IPC carries out a detailed auditing and reporting of the use of investigatory powers while the IPT hears complaints about the misuse of investigatory powers (*see* footnote 152 above).

United States, both the executive and the judiciary are involved.[171] In **Ireland**,[172] independent judicial oversight of the operation of the relevant acts is carried out by a serving High Court judge who is designated for this purpose.[173] In **Kyrgyzstan**[174] and in the **Republic of Moldova**,[175] the oversight over the implementation of the laws by bodies carrying out intelligence activities is entrusted to the prosecution. In **Malta**,[176] **Poland**[177] and **Serbia**,[178] it is the executive which is involved in the oversight of the activities of the intelligence agencies.

64. A system of parliamentary oversight of the activities of the intelligence agencies through specialised parliamentary committees exists in **Austria**, **Belgium**, **Bosnia and Herzegovina**, **Bulgaria**, **Canada**,[179] **Croatia**,[180] **Denmark**, **Estonia**, **Finland**,[181] **France**, **Germany**, **Greece**,

[171] The Privacy and Civil Liberties Oversight Board (PCLOB) is responsible for reviewing new policies and procedures implemented by intelligence agencies and conducts an annual review of the Data Protection Review Court's redress process whereas the FISC and the Data Protection Review Court (DPRC) are mandated to provide oversight. The DPRC provides a mechanism for redress through independent and impartial review of specific complaints from individuals who allege violations of U.S. law in the conduct of U.S. intelligence activities. Its decisions are binding.

[172] Ireland does not have a distinct intelligence agency. Intelligence and state security functions are the responsibility of An Garda Síochána and the Defence Forces.

[173] The Designated Judge is tasked with keeping the operation of the legislation under review and publishing annual reports under Section 8 of the 1993 Act, Section 12 of the 2009 Act and Section 12 of the 2011 Act. In practice, this consists of annual meetings with officials from the Department of Justice, the police, and other Irish agencies who use interception and data retention powers, and some inspection of their files. The oversight role is a part-time function of a judge. The role has no specialist legal or technical support, meaning that there is no institutional memory and is dependent on the support of the entities being monitored. When the Policing, Security and Community Safety Act 2024 enters into force, primary oversight will be assigned to an Independent Examiner.

[174] At the request of the authorised prosecutor in connection with materials, information and appeals from citizens received by the prosecutor's office regarding violations of laws during the conduct of operational-search activities, as well as during the verification of the established procedure for conducting operational-search activities and the legality of the decisions taken in this regard, the heads of the body carrying out operational-search activities shall submit to the said prosecutor operational-service documents that served as the basis for conducting these activities.

[175] Article 39 of Law 59/2012: the control over the execution of the Law shall be carried out by the hierarchically superior public prosecutors on the basis of complaints lodged by persons whose rights and legitimate interests are alleged to have been violated as a result of the special investigative activity or ex officio. The hierarchically superior public prosecutors carrying out the control shall have the right of access to the information constituting state secret in the manner established by law.

[176] The Commissioner for the Security Services.

[177] The Minister of the Interior and Administration oversees the activities not only of the Police but also of some special forces, such as the Internal Security Agency (ABW). This executive oversight includes setting strategic directions and ensuring that security services operate within the bounds of the law. However, the Minister's role is more administrative and less focused on day-to-day operational control. The Minister of Justice plays a role in overseeing surveillance activities, especially those related to significant criminal investigations.

[178] The Ministry of the Interior and the Ministry of Defence, oversees various security services. These ministries have administrative and operational oversight responsibilities.

[179] The National Security and Intelligence Committee of Parliamentarians (NSICOP) is a committee of Parliamentarians that has a broad mandate, including to review any activity carried out by a department that relates to national security or intelligence, unless the activity is an ongoing operation and the appropriate Minister determines that the review would be injuries to national security. NSICOP submits an annual report to the Prime Minister (which is then tabled in Parliament), which includes the findings and recommendations (non-binding) that were made during the previous year.

[180] The Committee for Internal Affairs and National Security has the authority to perform direct on-site oversight of the Security and Intelligence Agency and the Military Security and Intelligence Agency. Otherwise, their work is based on receiving, reviewing and discussing reports from agencies (annual reports and reports concerning specific cases or themes). The Chair of the Committee has to be from the benches of the largest opposition party. The Committee issues non-binding decisions, conclusions and recommendations.

[181] The Intelligence Oversight Committee oversees the proper implementation and appropriateness of intelligence operations, monitors and evaluates the focus areas of intelligence operations, monitors and promotes the effective exercise of fundamental and human rights in intelligence operations, prepares reports by the Intelligence Ombudsman and processes the supervisory findings of the Intelligence Ombudsman.

Italy,[182] **Kosovo**,[183] **Kyrgyzstan**, **Lithuania**, **Luxembourg**,[184] the **Republic of Moldova**, the **Netherlands**, **North Macedonia**,[185] **Norway**,[186] **Poland**,[187] **Romania**, **Serbia**,[188] the **Slovak Republic**,[189] **Spain**,[190] **Sweden**, **Switzerland**,[191] **Ukraine**,[192] the **United Kingdom**, the **United States**.[193] The boundary line between parliamentary and independent/expert oversight bodies is not rigid, as "hybrid" bodies exist (see also paragraph 117 below).

65. In **Cyprus** and **Portugal** non-specialised parliamentary committees participate in the oversight of the activities of the intelligence agencies.

---

[182] Article 31 of the law n. 124/2007: the Parliamentary Committee may obtain, even in derogation of the prohibition established by Article 329 of the Code of Criminal Procedure, copies of acts and documents relating to proceedings and investigations under way at the judicial authority or other investigative bodies, as well as copies of acts and documents relating to parliamentary investigations and inquiries.

[183] Its responsibilities include, inter alia, overseeing the legality of the work of the Intelligence Agency, reviewing reports from the Director of the Intelligence Agency regarding the operations of the Agency and the reports from the Inspector General, as well as conducting inquiries regarding the work of the Agency.

[184] Chapter 6 of the Loi SRE. The Parliamentary Control Committee is informed *ex officio* every six months of surveillance and communications monitoring measures ordered by the Ministerial Intelligence Committee at the request of the State Intelligence Agency. The Parliamentary Control Committee may also carry out checks on specific cases.

[185] The Commission for Oversight of Communication Monitoring Measures, chaired by a representative of the major opposition party, also engages national and international technical experts, two of which are appointed permanently. The Commission's primary goal is to verify that communication monitoring measures are implemented legally and effectively. The Commission also reviews the annual report from the Public Prosecutor on special investigative measures to gauge the effectiveness of these measures. Oversight is conducted at least every three months, often without prior notice. After each oversight session, the Commission prepares a detailed report indicating whether the conduct observed was legal or if any abuses were detected. In cases of irregularities or abuses, the Commission is required to notify the public prosecutor and relevant authorities promptly. Finally, the Commission submits an annual report to the Assembly by the end of February each year.

[186] The Norwegian Parliamentary Oversight Committee on Intelligence and Security Services (the EOS Committee has complete access to all information held by the intelligence services regardless of classification. The EOS Committee can address complaints by individuals and whistle blowers but also investigate issues by its own initiative. If the EOS Committee during a control finds that surveillance is illegal, it can demand a cease of the surveillance and deletion of all information by a motion to the Oslo city court, see Article 7-12 of the 2020 Intelligence Act. It reports annually to the Parliament.

[187] The Committee on Special Services, which monitors and reviews the operations carried out by the Internal Security Agency (ABW) and the Intelligence Agency (AW). This committee holds hearings, examines reports, and ensures that the activities of security services are conducted in compliance with the law and democratic principles.

[188] The Special Security Services Control Committee, among other things, supervises the constitutionality and legality of the work of security services and the legality of the application of special procedures and measures for secret collection of data.

[189] The Special commission for the monitoring of the use of information-technical devices (the Commission has still not been established in practice, mostly due to political disagreements) has eight members, with the president who must belong to the opposition. It carries out inspection at least on an annual basis but may do so at any time of its own motion and upon complaint by anyone who claims they have been subjected to unlawful surveillance. The Commission's powers are mostly of monitoring nature. Its members have the right to enter premises, access registers and obtain information, even if classified, from the relevant state authorities. The protocols of inspections carried out are then submitted to the relevant parliamentary committees. Should the respective parliamentary committees suspect that surveillance has been carried out in violation of the law, they must inform the Speaker of Parliament, who then informs the Prosecutor General. The parliament must discuss in plenary twice a year the reports of the committees on the state of use of surveillance measures.

[190] The "Official Secrets Committee" meets "in camera" and its members are bound by an obligation of Confidentiality.

[191] The "oversight delegation" and the "finance delegation" have complete and unhindered access to all information they require to fulfil their oversight responsibilities.

[192] Cfr. Article 53 of the Law of Ukraine "on intelligence".

[193] The House Permanent Select Committee on Intelligence (HPSCI) and the Senate Select Committee on Intelligence (SSCI) provide congressional oversight of intelligence activities, including surveillance practices. The HPSCI has legislative and oversight responsibilities over Intelligence Community programs, policies, budgets, operations, all covert actions, and the collection, exploitation, and dissemination of human intelligence. The SSCI provides legislative oversight concerning the intelligence activities of the US government. They do this by inter alia conducting hearings with high-ranking intelligence agency officials; conducting investigations and review of intelligence programs; and reviewing and collecting intelligence activities/analysis.

F. Notification of targeted surveillance measures

66. Lastly, the Venice Commission has analysed the availability of a post-surveillance notification mechanism in the framework of the execution of measures of targeted surveillance. In the framework of criminal proceedings, the existence of a notification mechanism of targeted surveillance measures has been reported by **Bosnia and Herzegovina**,[194] **Canada**,[195] **Denmark**,[196] **Estonia**,[197] **Finland**,[198] **Germany**,[199] **Greece**,[200] **Italy**,[201] **Korea**,[202] **Kyrgyzstan**, **Liechtenstein**,[203] **Lithuania**,[204] **Luxembourg**,[205] the **Republic of Moldova**,[206] the **Netherlands**,[207] **North Macedonia**,[208] **San Marino**,[209] **Serbia**,[210] the **Slovak Republic**,[211] **Switzerland**,[212] **Ukraine**[213]. In the absence of notification requirements, complaints for measures ordered or carried out in violation of legal provisions can be filed in **Austria**,[214] **Ireland**.[215] The

[194] Article 119 of the Code of Criminal Procedure, with the possibility to request the court the examination of the legality of the order and the manner in which the measure was implemented.
[195] Sections 196 and 196.1 of the Criminal Code provide requirements for after-the-fact written notice to be provided to persons whose private communications have been intercepted pursuant to an authorisation or in warrantless situations of urgency where there is imminent risk of harm.
[196] Article 788 of the Administration of Justice Act: notification shall be given as soon as possible if the police have not, within 14 days after the expiry of the period for which the interference has been permitted. Exceptions are cases in which it would be detrimental to the investigation or to the investigation in another pending case concerning an offense which, according to law, may form the basis for an interference with the secrecy of communications, or if the protection of confidential information about the police's investigative methods or the circumstances otherwise speak against notification. In these cases the court may, upon application by the police, decide that notification shall be omitted or postponed for a specified period of time, which may be extended by subsequent decision.
[197] Article 126 § 13 of the Criminal Procedure Code.
[198] Section 60 of the Coercive Measures Act provides on giving notice of the use of covert coercive measures.
[199] Section 101 of the Code of Criminal Procedure.
[200] In criminal matters, after the expiration of the measure and upon submission of a relevant request by the affected party, the ADAE notifies the affected party of the imposition of this measure within a period of sixty (60) days, with the consent of the Supreme Court Prosecutor and under the condition that the purpose for which the measure was ordered is not compromised (Article 6 of Law no. 5002/2022).
[201] Articles 268 and 269 of the Code of Criminal Procedure.
[202] Within 30 days from the date of termination of the measures.
[203] Article 104 § 2 of the Criminal Procedure Code (StPO). Art. 104 § 4 StPO further provides that an appeal can be filed with the Superior Court within fourteen days of notification by the investigating judge. Against this decision an individual complaint to the Constitutional Court may be lodged.
[204] Article 161 of the Code of Criminal Procedure.
[205] Article 88-4 § 6 of the Code of Criminal Procedure; they are further informed that they can lodge an appeal for annulment on the basis and under the conditions of Article 126.
[206] Notification can be postponed until the end of the criminal investigation. Article 313 of the Criminal procedure code provides a judicial remedy against unlawful actions and acts of the prosecution and special investigative bodies.
[207] Article 126bb of the Code of Criminal Procedure. Notification must take place as soon as possible but does not occur when this is 'reasonably not possible' or when individuals are automatically notified in pending criminal procedures.
[208] Article 262 of the Criminal Procedure Code.
[209] Law no. 98 of 21 July 2009.
[210] Article 163 of Code of Criminal Procedure
[211] Sections 114 and 115 of the Code of Criminal Procedure: the persons concerned who do not have access to the file must be, within three years from the final decision in the criminal case, notified that they had been subjected to surveillance and that any recordings have been destroyed. They must be informed of the possibility to file with the Supreme Court a motion for review of the court warrant authorising the surveillance.
[212] Article 279 of the Code of Criminal Procedure: reason, type and duration of the surveillance at the latest when the preliminary proceedings conclude. Compulsory measures court may postpone or waive the notification if the findings are not used as evidence in court proceedings and the postponement or omission is necessary to protect overriding public or private interests.
[213] Article 253 of the Criminal Code.
[214] Section 106 § 1 of the Code of Criminal Procedure.
[215] Section 9 of the 1993 Act, Section 11 of the 2009 Act and Section 10 of the 2011 Act allow an individual to apply to a Complaints Referee to investigate whether a ministerial authorisation for interception was made and if so, whether the requirements of the relevant Act were followed in respect of the request. The Referee can examine the lawfulness of the relevant measures. The Referee is appointed by the Taoiseach for a five-year term. All holders of the office to date have been sitting judges of the Circuit Court. The Referee has the power to access any official documents relating to measures taken. If the Referee concludes that the law has been contravened, they must

meaningfulness of notification as a remedy depends upon how the exceptions to this are interpreted in practice (see paragraphs 120-122 below).

67. The following countries reported a system of notification in cases of targeted surveillance carried out by security services: **Belgium**,[216] **Bosnia and Herzegovina**,[217] **Denmark**,[218] **Estonia**,[219] **Finland**,[220] **Germany**,[221] **Korea**,[222] the **Republic of Moldova**,[223] the **Netherlands**,[224] **North Macedonia**,[225] **Romania**,[226] **Switzerland**,[227] **Ukraine**.[228]

notify the applicant in writing and make a report to the Taoiseach. The Referee may also quash a ministerial authorisation, direct the relevant agency to destroy the information obtained and recommend compensation. The redress system is limited to investigating whether a warrant was issued properly and does not provide a remedy in relation to other situations such as improper data retention or disclosure by the telecommunications data or misuse of data by the Gardaí.

[216] As provided in Article 2 § 3 of the L. R&S. Conditions are that, *inter alia*, a period of more than ten years has elapsed since the end of the method, the notification cannot prejudice an intelligence investigation and may not prejudice relations between Belgium and foreign international or supranational institutions.

[217] Article 77 of the Law on Intelligence and Security Agency, after the end of the monitoring, unless such information could endanger the completion of the Agency's tasks or the completion of the proceedings before the competent authorities.

[218] See footnote 196 above.

[219] Article 29 of the Security Authorities Act: exceptions are 1) significantly harm another person's rights and freedoms guaranteed by law or put another person at risk; 2) endanger the confidentiality of the security authority's means, methods or tactics; 3) endanger the source of information or a person recruited to secret co-operation; 4) harm exchange of information between security authorities or co-operation with a foreign state or an international organisation.

[220] Section 20 of the Act on the Use of Network Traffic Intelligence in Civilian Intelligence and Section 89 of the Act on Military Intelligence.

[221] Section 59 of the Federal Intelligence Service Act and section 12 of the Article 10 Act.

[222] See footnote 205 above.

[223] Article 22 of Law no. 59/2012, with the following exceptions: (a) the information constitutes an increased risk to the life and health of the person; b) it is necessary to carry out another special investigation measure within the same special file; c) the results of the special investigative measure necessitate criminal proceedings. Article 26 of the Law no. 59/2012 provides for a redress mechanism.

[224] Article 59(1) of the Act on Intelligence and Security Services. In principle, individuals involved in the application of an investigative power must be informed five years after the termination of the investigative power. Notification is not required when (a) sources of a service, including intelligence and security services of other countries, are disclosed; (b) relations with other countries and with international organisations are seriously harmed; or (c) a specific application of a method (modus operandi) or the identity of the person who assisted the service in applying the method is disclosed.

[225] Article 51(6) of the Law on Communications Surveillance requires the Council for Civil Control to notify the citizen promptly if abuse is detected during the oversight. If no abuse is found, the citizen is still informed but with limited details to preserve confidentiality.

[226] Article 21 § 2 of Law no. 51/91 on the National Security of Romania. Notification is excluded if: (a) it could lead to jeopardising the performance of the official duties of State bodies responsible for national security by disclosing their sources, including those of the security and intelligence services of other States; (b) could affect the defence of national security; (c) could prejudice the rights and freedoms of third persons; (d) could lead to the disclosure of the methods and means, including specific investigative techniques, used in the case in question by State bodies responsible for national security.

[227] If the target is located in Switzerland Article 33 IntelSA provides that the person monitored must be notified within one month after concluding the operation. Exceptions are: a. the postponement is necessary in order not to jeopardise an ongoing search or to legal proceedings; b. the postponement is necessary because of another overriding public interest in preserving internal or or external security, or because of Switzerland's relations with foreign countries; c. the information could endanger third parties; d. the person concerned cannot be reached. If the target is located abroad, the individual is not informed of the intelligence measure.

[228] Article 25 of the Law of Ukraine "On Intelligence" on the condition that the provision of this information will not pose a threat to the national security of Ukraine.

68. In **Canada**, **Greece**,[229] **Ireland**,[230] **Kosovo**,[231] **Kyrgyzstan**, the **Slovak Republic**,[232] the **United States**,[233] while no notification requirements exist in the context of intelligence operations, complaints can be filed with relevant oversight bodies/courts.

G. Overview of certain States' law and practice aiming to prevent abuse of spyware

69. It is noteworthy that in some States specific legislative measures have been undertaken to limit the development of spyware or to react to misuse allegations.

70. In **Austria**, the Constitutional Court held on 11 December 2019[234] that covertly monitoring the use of computer systems constituted a serious interference with the right to privacy protected by Article 8 of the European Convention on Human Rights (ECHR) and was only permitted within extremely narrow limits in order to protect equally important legal interests.[235] It therefore declared uncostitutional Section 135a of the Code of Criminal Procedure that had been enacted in 2018, permitting the use of spyware to read encrypted messages. Section 135a in conjunction with Section 134 § 3a of the Code of Criminal Procedure provided (in specified cases and under certain conditions) for an authorisation to covertly monitor encrypted messages by installing spy software – a so-called "Federal Trojan" *(Bundestrojaner)* – on a computer system. However, these provisions eventually never entered into force because on 11 December 2019, the Austrian Constitutional Court quashed them.

---

[229] In April 2024, the Greek Council of State declared unconstitutional a 2021 legislative amendment which barred the ADAE from informing citizens of state surveillance on "national security" grounds. The Council of State found the blanket prohibition on informing individuals about the fact that they had been subjected to surveillance an "excessive restriction" on the right to privacy and a threat to the rule of law. Through the 2022 legislative changes, pursuant to Article 4 § 3 of Law no. 5002/2022, interested individuals, should they suspect that they have been targeted, must submit a request thereof to ADAE, which, thereafter, submits it to EYP. The law provides however that such requests are admissible only after the elapse time-period of three years from the termination of the surveillance. Neither ADAE nor EYP can decide thereof, but a three-member committee, composed by EYP's prosecutor, the high ranked second prosecutor in charge with the file and the president of ADAE. That committee may satisfy the demand only if it considers that the disclosure does not jeopardise the scope for which the specific surveillance had been imposed. What is even more important, should that committee decide to notify the interested person, the law provides that no other information is notified to him but that his communications had indeed been intercepted for the disclosed period of time. Nevertheless, all information concerning the reasons why the surveillance was imposed are to be withheld.

[230] See footnote 215 above.

[231] Article 39 § 2 of the Law on the Kosovo Intelligence Agency provides that Individuals, institutions and third parties have the right of complaint against the Kosovo Intelligence Agency to the Ombudsperson Institution.

[232] The affected persons may also file a constitutional complaint under Art. 127 of the Constitution. The constitutional complaint mechanism has recently proven essential in filling in a lacuna in the PAIA consisting in the fact that the regional courts exercising judicial review under PAIA have no power to specifically order the destruction of recordings obtained through illegal surveillance. This legislative omission was criticised by the ECtHR in its 2021 judgment in *Zoltán Varga v. Slovakia*, nos. 58361/12 and 2 others, 20 July 2021. In the recent 15 May 2024 judgment (III. ÚS 97/2012), the Constitutional Court specifically ordered – in this case – the Slovak Information Service to destroy any still existing recordings and other documents obtained through the illegal surveillance carried out in that case and to inform the complainant of their destruction.

[233] FISA provides for individual remedies for the unlawful acts of individual government officers against data subjects. Under the ECPA a suppression remedy is available when there is an interception of wire and oral communications. Lastly, before the Data Protection Review Court, individuals can submit complaints of alleged violations of the US government's surveillance activity in collecting or handling an individual's data.

[234] Constitutional Court, Collection of the decisions 20356/2019 (11 December 2019).

[235] The Constitutional Court found that the "Federal Trojan" was a particularly intrusive form of surveillance measure, especially because an overview of the data obtained by monitoring a computer system enabled conclusions to be drawn about, among others, individual users' personal preferences and lifestyles. Moreover, among others, it: (a) affected a large number of people; (ii) there was no guarantee that the surveillance measure would only take place if it was used to prosecute and solve sufficiently serious offences; (iii) the measure did not adequately secure the protection of the privacy of those affected by the Trojan; and (iv) there was no guarantee that after the *ex-ante* judicial approval of the measure, the legal protection officer would actually be able to effectively and independently monitor any ongoing covert surveillance.

71. Various forms of evaluation of the use of spyware, including through commissions of inquiry, have taken place in **Belgium**,[236] **Canada**,[237] **Greece**,[238] **Italy**,[239] the **Netherlands**,[240] **Poland**,[241] **Spain**,[242] **Sweden**,[243] **Switzerland**,[244] the **United States**.[245]

[236] *Enquête de contrôle à la suite des révélations sur l'utilisation du logiciel PEGASUS*, cited above.
[237] The House of Common's Standing Committee on Access to Information, Privacy and Ethics prepared a report about the Device investigative tools used by the Royal Canadian Mounted Police (RCMP) and related issues, cited above. The report examines the benefits and risks of the use of on-device investigative tools and examines legislative and non-legislative measures that could be considered to better regulate these types of tools in Canada. The report found that that there is a legislative gap regarding the use of new technological investigative tools. It therefore concluded that a better legislative framework for the use of on-device investigative tools by the RCMP is needed to ensure the appropriate use of these tools and the protection of Canadians' privacy rights.
[238] Following the incidents reported in 2022 (see PACE Report, cited above, Explanatory memorandum §§ 31-35), an official Parliamentary Inquiry took place to examine any allegation of use of illegal spyware for official purposes. The Committee examined how the national intelligence services, in their role, might be conducting legally authorised surveillance operations, through proportionate and conventional means. The findings of the Committee were made available, under confidentiality, to all Members of the Greek Parliament.
[239] *Documento approvato dalla 2ª Commissione permanente (Giustizia) nella seduta del 20 settembre 2023 a conclusione dell'indagine conoscitiva sul tema delle intercettazioni*, cited above, p. 41 et ff.
[240] In 2022, the Research and Data Centre of the Dutch Ministry of Justice and Security published an evaluation report on the Dutch use of spyware by law enforcement authorities. It is an empirical study into the implementation of this power. The study revealed that between March 2019 and March 2021, the power was issued in 26 criminal investigations. It has been used in criminal investigations into more serious forms of traditional crime such as (attempted) murder, cases involving narcotics, falsification of documents, money laundering, sexual offences, terrorism offences, and membership of a criminal organisation. The report clarified that the Dutch police used of a commercial tool in the 'vast majority' of cases. In the context of intelligence and security services, the entire Act on intelligence and security services was evaluated in 2020, including the use of spyware in Article 45. However, its focus was not on 'targeted surveillance' but rather on the use of spyware directed at organisations and the acquisition of bulk datasets. The name of the commercial tool(s) used is not public.
[241] In February 2024, a special parliamentary committee was established to investigate the use of spyware, which, according to Poland's justice minister, was used on almost 600 people between 2017 and 2022. On 10 September 2024, Poland's Constitutional Tribunal ruled that the commission is unconstitutional in the scope of its activity.
[242] Following revelations that 65 people have been targeted (in the so-called "CatalanGate") by spyware, (PACE Report, cited above, Explanatory memorandum, §§ 36-42) a special commission of inquiry has been set up: the Parliamentary Committee of Inquiry into the spying and intrusion into privacy and intimacy, through the Pegasus and Candiru malware, of political leaders, activists, lawyers, journalists, institutions and their families and relatives. *Comisión de Investigación sobre el espionaje e intromisión a la privacidad e intimidad, a través de los malware Pegasus y Candiru, a líderes políticos, activistas, abogados, periodistas, instituciones y sus familiares y allegados.* The Committee is competent to: a) explore in detail the involvement of state institutions in alleged unlawful interference against political leaders, institutions and other individuals; b) investigate the alleged responsibility and misuse of technical bodies in all ministerial departments and the linking of these bodies to espionage; c) explore in detail all the Foreign Ministry's activities in relation to the investigations carried out in an allegedly illegal manner, without being sub judice, of the Generalitat's delegations abroad; d) know the contracts, costs and contracting processes for the alleged development and/or purchase of Pegasus software or other tools used for espionage by official bodies; e) investigate all initiatives carried out by state authorities in order to persecute political dissidence; f) propose and raise redress measures for all those affected by illegal investigations, as well as accountability for misuse of government machinery; and g) propose appropriate control, investigation and prevention measures to shield democracy from abuses of state power and prevent its use against civil and political rights. A second Committee, the Parliamentary Committee of Inquiry "*into the so-called "Operation Catalonia" and the actions of the Ministry of the Interior during the governments of the Popular Party in relation to the alleged irregularities linking high-ranking officials and police commanders to the existence of a vigilante plot*" has the competence, among others to "know the contracts, expenses and contracting procedures for the alleged development and/or purchase of software called "Pegasus", or other tools allegedly used for spying by official bodies.
[243] The initial authority to use spyware was preceded by a commission of inquiry (as is the norm for any new legislation in Sweden) - *Hemlig dataavläsning – ett viktigt verktyg i kampen mot allvarlig brottslighet*, SOU 2017:89. The Act introduced in 2020 was to apply for a limited period of time (until March 2025). During 2023, the operation of the Act was reviewed by another commission of inquiry, *Hemlig dataavläsning – utvärdering och permanent lagstiftning*, SOU 2023:78. The general conclusion of this second commission of inquiry was that the Act, even though only a short period of time had elapsed, had been used more than expected, and that it was an essential tool of investigation which should be made permanent.
[244] The competent parliamentary committee has requested an annual performance report from the FIS in accordance with Article 26 IntelSA and the measures against foreign computer systems in accordance with Article 37 IntelSA since 2019. In its report, the FIS provides a comprehensive assessment of the benefits of the measures and addresses technical aspects and resource issues. Statistics show that 9 operations used special computer software in 2023, compared to 7 in the previous year.

72. The **United States** has enacted Laws imposing restrictions on Pegasus and related categories of commercial spyware. Public Law 117-263 (50 USC §3232a) (2022)[246] requires U.S. intelligence agencies to provide annual reports assessing counter-intelligence threats "and other risks to national security" that "foreign commercial spyware" poses to the United States. It further authorises the Director of National Intelligence to prohibit intelligence agencies from "entering into any contract or other agreement for any purpose with a company that has acquired, in whole or in part, any foreign commercial spyware." Public Law 117-81 (22 USC §2679e) (2021)[247] requires the Secretary of State to prepare a list of contractors that have "knowingly assisted or facilitated a cyberattack or conducted surveillance" against the United States or against: "*[i]ndividuals, including activists, journalists, opposition politicians, or other individuals for the purposes of suppressing dissent or intimidating critics, on behalf of a country included in the annual country reports on human rights practices of the Department for systematic acts of political repression, including arbitrary arrest or detention, torture, extrajudicial or politically motivated killing, or other gross violations of human rights*". Executive Order 14093,[248] promulgated under such authorisation, prohibits any federal agency or department from making operational use of commercial spyware when they determine *inter alia* "that the commercial spyware poses significant risks of improper use by a foreign government or foreign person." The order further articulates the bases upon which an agency could make such a determination, including uses in violation of international human rights law.

73. It is noted that the governments of Australia, Austria, Canada, Costa Rica, Denmark, Estonia, Finland, France, Germany, Japan, Lithuania, the Netherlands, New Zealand, Norway, Poland, the Republic of Ireland, the Republic of Korea, Sweden, Switzerland, the United Kingdom, and the United States have endorsed a joint statement which commits the signatories to work collectively to counter the proliferation and misuse of commercial spyware.[249] In particular, the parties commit to partner to counter the misuse of spyware and to: (i) working to establish robust guardrails and procedures to ensure that any commercial spyware use is consistent with respect for universal human rights, the rule of law, and civil rights and civil liberties; (ii) preventing the export of software technology, and equipment to end-users who are likely to use them for malicious cyber activity; (iii) sharing information on commercial spyware proliferation and misuse; (iv) working closely with industry partners and civil society groups to inform their approach, help raise awareness, and set appropriate standards, while also continuing to support innovation; (v) engaging additional partner governments around the world to better align policies and export control authorities to mitigate collectively the misuse of commercial spyware and drive reform in this industry.

V. Minimum safeguards against abuses of power

74. As observed above, it is crucial to ensure that the use of spyware does not provide States with arbitrary and unlawful power to interfere with the private life of individuals.[250] States are

[245] The United States has evaluated commercial spyware and concluded, in the 27 March 2023 Executive Order (The White House, *Executive Order on Prohibition on Use by the United States Government of Commercial Spyware that Poses Risks to National Security*, 27 March 2023), that "*[t]he growing exploitation of Americans' sensitive data and improper use of surveillance technology, including commercial spyware, threatens the development*" of an international technology "*ecosystem […]*". As to the national security and foreign policy interests, the Executive Order noted that there is value in "*ensuring that technology is developed, deployed, and governed in accordance with universal human rights; the rule of law; and appropriate legal authorisation, safeguards, and oversight, such that it supports, and does not undermine, democracy, civil liberties, and public safety*."

[246] Available here.

[247] Available here.

[248] *Executive Order on Prohibition on Use by the United States Government of Commercial Spyware that Poses Risks to National Security*, cited above.

[249] The White House, *Joint Statement on Efforts to Counter the Proliferation and Misuse of Commercial Spyware*, 18 March 2024. List of States as most recently amended on 22 September 2024.

[250] Venice Commission, CDL-AD(2016)007, cited above, § 118.

bound by obligations under customary international law as well as obligations they have undertaken by acceding to international human rights treaties, such as the ECHR (and the ICCPR), aimed at protecting human rights and upholding the rule of law. In order for surveillance through the use of spyware to be compatible with Article 8 ECHR and Article 17 ICCPR, the legal framework allowing for it needs to meet very strict requirements. Drawing on the jurisprudence of the ECtHR on targeted surveillance, the Venice Commission's previous reports, other European and international standards such as Convention 108+ as well as on the comparative analysis of relevant legislation in the Venice Commission's member states, this section provides a non-exhaustive overview of major principles that would need to be upheld when using spyware in order to comply with rule of law and human rights standards.

A. Primary legislation that is accessible and foreseeable

75. Since the use of spyware constitutes an interference with the right to respect for one's private life, as illustrated above, Article 8(2) of the ECHR and Article 17 ICCPR require that it may only be authorised if it is adequately regulated by law, i.e. that it is "in accordance with the law". According to the ECtHR, this "not only requires that the impugned measure should have some basis in domestic law, but also refers to the quality of the law in question, requiring that it should be accessible to the person concerned and foreseeable as to its effects".[251]

76. The ECtHR has stated that in view of the risk of abuse intrinsic to any system of secret surveillance, such measures must be based on a law that is particularly precise, especially as the technology available for use is continually becoming more sophisticated.[252] Thus, the use of a special investigative tool such as spyware is to be regulated by *primary* legislation, i.e. a statute.[253] Such a requirement has the benefit of democratic legitimacy, as it allows a democratically elected legislature to determine the exact balances which should be drawn between competing interests, and enhances legal certainty.[254]The law must moreover meet quality requirements: it must be accessible to the persons concerned and foreseeable as to its effects.

77. In view of the above, the quality of the domestic law governing the use of spyware is an essential precondition for reducing the interference of spyware with privacy and data protection rights (and other human rights), as well as for limiting the risk for abuse of power. Should States decide to employ such a surveillance technique, a positive obligation would be imposed on them to provide that the legislative framework is in accordance with the "quality" of law requirements provided for notably in Article 8 of the ECHR.

1. Accessibility of legislation

78. In the countries on which the Commission has information, the law governing targeted surveillance would usually be a provision of the Code of Criminal Procedure or a specific piece of primary legislation devoted to surveillance/investigative powers.[255] These are officially published acts which are accessible to the public.

2. Foreseeability of legislation

79. According to the ECtHR, a rule is "foreseeable" if it is formulated with sufficient precision to enable any individual – if need be with appropriate advice – to regulate his conduct. This

[251] ECtHR, *Rotaru v. Romania* [GC], no. 28341/95, 4 May 2000, § 52.
[252] ECtHR, *Uzun v. Germany*, no. 35623/05, 2 September 2010, § 61.
[253] *See, mutatis mutandis*, ECtHR, *Bykov v. Russia* [GC], no. 4378/02, 10 March 2009, §76.
[254] In Sweden for example, it was found necessary to make a statutory requirement to document all decision-making in secret investigative measures. It was not regarded as sufficient that such matters be governed by internal instructions in the prosecutor's office or police/security police. *See* prop. 2022/23:126, p. 181.
[255] *See*, *among many others*, the Investigatory Powers Act 2016 in the United Kingdom.

requirement of precision constitutes an essential guarantee against arbitrariness in the imposition of restrictive measures, and such protection is even more important as regards secret surveillance measures, due to the heightened risks of arbitrariness in such circumstances.[256]

80. However, in the special context of surveillance, foreseeability does not mean that individuals should be able to foresee when the authorities are likely to intercept their communications so that they can adapt their conduct accordingly.[257] In the context of surveillance aimed at facing threats to national security, the vagueness of the national security concept creates special problems because effective regulation requires a high level of precision, and effective regulation is a precondition for effective oversight.

81. The ECtHR has however found that the requirement of "foreseeability" of the law does not go so far as to compel States to enact legal provisions listing in detail all conduct that may prompt a decision to subject an individual to secret surveillance on "national security" grounds. By their very nature, threats to national security may vary in character and may be unanticipated or difficult to define in advance.[258] At the same time, the ECtHR has also emphasised that in matters affecting fundamental rights it would be contrary to the rule of law, one of the basic principles of a democratic society enshrined in the Convention, for a discretion granted to the executive in the sphere of national security to be expressed in terms of unfettered power.[259] Furthermore, the ECtHR has found that the limits of the notion of national security cannot "be stretched beyond its natural meaning".[260] 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, having regard to the legitimate aim of the measure in question, to give the individual adequate protection against arbitrary interference.[261] The ECtHR found that States cannot make general assertions regarding the scope of national security which would make it impossible for an applicant to effectively challenge the claim.[262]

82. As observed above, few States specifically regulate spyware as a tool of targeted surveillance, while many of them include it as a "special technical means" of surveillance without providing for specific rules. While some domestic legal regimes are quite detailed and precise, some others tend to rely on relatively broad and open-ended formulations which do not necessarily provide the required degree of certainty and precision. The Venice Commission considers that having regard to the particularly high level of intrusiveness of spyware, in particular the fact that it can involve a combination of different intrusions into privacy, should they authorise the deployment of spyware, States should enact specific and tailored legislation with a stricter scope *ratione personae*, *materiae* and *temporis vis-à-vis* other targeted surveillance measures. This should be a precondition for State use of spyware.

3. Necessity to distinguish between different levels of intrusiveness of surveillance

83. As observed above, a variety of personal data can be potentially made available by the surveillance through spyware intruding into electronic devices. The comparative research has

[256] ECtHR, *Malone v. the United Kingdom*, no 8691/79, 2 August 1984, § 68: "*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 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, having regard to the legitimate aim of the measure in question, to give the individual adequate protection against arbitrary interference*"; *see also* *Segerstedt-Wiberg and Others v. Sweden*, no. 62332/00, 6 June 2006, § 76.
[257] ECtHR, *Weber and Saravia v. Germany* (dec.), no. 54934/00, 29 June 2006, § 93.
[258] ECtHR, *Kennedy v. the United Kingdom*, cited above, § 159.
[259] ECtHR, *Roman Zakharov v. Russia* [GC], cited above, § 247.
[260] ECtHR, *C.G. and others v. Bulgaria*, no. 1365/07, 24 April 2008, §43.
[261] ECtHR, *Liu v. Russia*, no. 42086/05, 6 December 2007, § 56, with further references.
[262] ECtHR, *Amie and Others v. Bulgaria*, no. 58149/09, 12 February 201, §§ 92 and 98.

shown that, in countries which specifically regulate the use of spyware, the kind of data that could be collected differs. Data on actual spyware usage is understandably scarce.[263]

84. A particular question arises in cases where live audio or video surveillance on a device is remotely activated. At least in some states, outside of the specific issue of spyware, real-time interception of communications (i.e. audio surveillance of a locality) is generally perceived as more intrusive of privacy than interception of the content of telecommunications. Activating a mobile phone to act as a real-time interception device is even more intrusive, as it will follow the target wherever they go, and whatever they do. In such states, it seems reasonable that where special limits apply in legislation to law enforcement or security use of real-time interception of communications, e.g. minimum thresholds of seriousness as regards offences, sufficiently proximate if not direct links to a real and serious threat to national security or limits or prohibitions on the use of real-time interception of communications in certain locations (places of worship, mass media, lawyers' offices etc.) then these must also apply when the police or security agency request that the audio surveillance function on a telephone or other device is activated. Where relevant laws provide that audio/video surveillance shall be limited to places where the suspect can be assumed to be staying, to be defined in the authorisation warrant, then such limits must also apply when spyware is used to activate audio surveillance.[264]

85. Spyware can present a particular challenge here because, for technical reasons, it may not be possible to limit the information so gathered. Given the extraordinary intrusiveness of spyware compared to other surveillance approaches, the screening of authorised and unauthorised (or relevant and irrelevant) information may be difficult as a technical matter. The Venice Commission strongly urges states considering the use of spyware to ensure that it has, as a required safeguard, specialised, vetted, professional teams capable of implementing effective information screening as is required with respect to other information-gathering practices. Destruction requirements should also be in place, backed up by strong, independent and well-resourced external oversight.[265] This external oversight must be robust and functional both in theory and in practice.

86. Turning to the question whether it is ever justified to use spyware to activate the video surveillance function of a mobile device, the Venice Commission notes that live video surveillance is arguably one of the most intrusive functions that a spyware can activate. Given its intrusiveness, if ever allowed, legislation should provide for a strict and clear framework for its activation, including imposing a duty on the requesting body (and in turn to the authorisation body) to specify the type of information sought, as well as the temporal and geographical limitations of the surveillance. The destruction requirements outlined above must also apply.

87. The Venice Commission believes that domestic legislation must make a clear distinction of the type of investigation in the context of which use of spyware may be authorised and the personal data of the target or others that may be sought. This distinction affects the assessment

[263] See as an example the Swedish practice, referred to in footnote 74 above, which indicates that spyware use in Sweden is almost exclusively for the interception of telecommunications and the collection of data contained in the device (i.e. not for audio or video surveillance).

[264] *See, for example*, SOU 2023:78, cited above, Section 3.2.8, p. 73.

[265] For example, the Swedish approach to this is to establish two or more "layers" of accessing the material within the investigating organisation. As noted above (paragraph 14) the use of spyware requires a specialised group of experts. This group will invariably be separate from the actual group investigating the specific offence or specific threat against national security (law enforcement or intelligence officers). The expert group will not need to know (and usually will not know) anything about the actual investigation. The expert group gathers the material, sifting out anything not covered by the time and place parameters set out in the authorisation, and destroying this surplus material (see further below paragraphs 126-129). Such a layered system can reduce the risks of gathering of too much information. However, for it to work, it obviously requires there first be a highly specific crime or a real and serious threat to national security being investigated and that there be clear temporal and spatial limits for the surveillance set out in the authorisation. Moreover, every accessing of material gathered must be subject to logs which cannot be tampered with. These logs must in turn be supervised by a layer or layers of internal review/control, *see* SOU 2023:78, cited above, p. 190.

of the necessity and proportionality of measures taken. Such an assessment should particularly take into account both the duration of the measures and the intensity of their intrusion into one's private and/or family life.[266]

B. Scope *ratione personae* of targeted surveillance measures

88. Another standard requirement stemming from the ECtHR's jurisprudence is that the law clearly provide that targeted surveillance measures be primarily available for communication devices only of a person who is personally suspected of a serious offence, or of posing a specific threat to national security.[267]

89. According to the ECtHR's jurisprudence, interception measures in respect of a person who is not suspected of an offence, or is posing a threat to national security can, exceptionally, be justified under Article 8 of the Convention.[268] However, this is possible only if certain strict requirements are fulfilled, that is, only if there are particularly strong reasons to believe that another person who is a suspect will contact the other person's device, or material contact information is likely to be found on this other person's device.[269] The Venice Commission considers that, if a State wishes to allow, exceptionally, surveillance for such purposes, then such a possibility should be combined with [judicial] pre-authorisation and stronger oversight, e.g. a specific requirement to notify the oversight body, combined with a procedural duty on the oversight body to pay particular attention to such cases.[270] Moreover, the circle of third parties who may be subject to interception measures should be specified in the decision in question, and the authority granting authorisation should give sufficient reasons for its decision on that point.[271]

90. Further limits can include only allowing the examination of (stored) historical metadata, not real-time data or communications and not permitting the activation of audio or video surveillance functions.[272]

91. Particular problems obviously arise where an organisation is made the subject of an investigation. This can happen both for organised crime and threats to national security. Organisations can also be "fluid" in practice. A "solid" organisation is an organisation featuring a – more or less – fixed structure and staff composition, while a "fluid" organisation is more informal in terms of composition and time. Considerable care must be taken in formulating the conditions for use of spyware in such circumstances, so as not to undermine safeguards for individuals.[273] Due to the more amorphous nature of national security, and its consequent greater potential for abuse, these safeguards are particularly important here.

92. It is to be noted that some countries prohibit the use of targeted surveillance by means of spyware on the computers or phones of a lawyer, a journalist or a doctor.[274] Where this is,

---

[266] Different requirements need to be established having regard to the degree of intrusiveness of the measure sought, for example having regard to the seriousness of the offence. As seen above (footnote 71 and paragraph 48) the Dutch Code of Criminal Procedure, as amended in 2019, provide for five different types of investigative acts that can be ordered to the investigating officer by means of accessing a device used by a suspect – with different criteria of applicability *ratione materiae*; in Sweden (paragraph 51 above), legislation makes a difference between the data reading involving and not involving activating a device's microphone to record sound – with different categories of offences that justify the authorisation of the measure.

[267] ECtHR, *Roman Zakharov v. Russia* [GC], cited above, § 231.

[268] ECtHR, *Greuter v. the Netherlands* (dec.), no. 40045/98, 19 March 2002.

[269] It should be stressed that these findings were made in the context of traditional surveillance rather than intrusive surveillance measures, where arguably a higher threshold should be used.

[270] In *Haščák v. Slovakia*, nos. 58359/12, 27787/16 and 67667/16, 23 June 2022, § 95, the ECtHR found that the applicable law provided no protection to persons randomly affected by covert surveillance measures.

[271] ECtHR, *Pietrzak and Bychawska-Siniarska and Others v. Poland*, cited above, § 201.

[272] See, for example, the Swedish legislation (paragraph 51 above) which imposes such limits in Section 5.

[273] *See for example* the recommendations made by the Dutch CTIVD in Review report 53 on the use of the investigatory power to hack by the AIVD and the MIVD in 2015, 8 March 2017, p. 17.

[274] See section IV.B above.

exceptionally, permitted, the ECtHR and the Venice Commission have previously concluded that, should surveillance be carried out against journalists and lawyers, higher standards throughout such operations must apply (higher thresholds before approving surveillance operations, more demanding internal and external oversight etc.).[275]

1. Use of spyware against journalists and other media actors

93. With particular regard to journalism, it is well-established that surveillance tools may be applied in only the most exceptional circumstances. European and international sources have widely recognised that journalism's watchdog role requires exceptional caution when considering interferences with their functions. The ECtHR has noted that "*authorities have only a limited margin of appreciation to decide whether a 'pressing social need' exists*" so as to satisfy the necessity of an interference with journalists' privacy and freedom of expression.[276] The protection extends to human rights defenders, non-governmental organisations researching and disseminating information in the public interest[277] as well as academics, writers, bloggers and others on the internet.[278] International experts have called for "comprehensive measures" to protect journalists from surveillance.[279] The Council of Europe has long considered that interception orders or actions, surveillance, and other forms of searches or seizures of journalistic data "*should not be applied if their purpose is to circumvent the right of journalists […] not to disclose information identifying a source*."[280]

94. These principles have special weight in the context of spyware, particularly since, as the European Data Protection Supervisor noted, "*Pegasus should not be equated to 'traditional' law enforcement interception tools*."[281] The Council of Europe Commissioner for Human Rights, assessing the extreme difficulty of limiting the reach of spyware in particular cases, noted that, even in the context of a framework of safeguards, "*it is virtually unimaginable that the use of Pegasus or equivalent spyware could ever be considered in accordance with the law and the necessary safeguards as outlined by the Court*."[282] The UN High Commissioner for Human Rights specifically warned that spyware's "chilling effects" on journalism could result in "eroding democratic governance."[283]

95. The European Media Freedom Act of the European Union, which entered into force in 2024 and will apply as of August 2025, sought to address this problem. Article 4 § 3 (c) of the Act provides, as a general rule, that spyware may not be deployed against media service providers or others that might result in disclosure of sources and communications. It provides for derogation from this standard protection only where: (i) authorities demonstrate the existence of an overriding reason of public interest; (ii) there is an ex ante authorisation by a judicial authority or an independent and impartial decision-making authority or, in exceptional and urgent cases, is subsequently authorised by such an authority; (iii) the investigation concerns particularly serious

[275] Venice Commission, CDL-AD(2015)011, cited above § 103; with regard to journalists *see* ECtHR, *Telegraaf Media Nederland Landelijke Media B.V. and Others v. the Netherlands*, no. 39315/06, 22 November 2012; with regard to lawyers *see Bersheda and Rybolovlev v. Monaco*, nos. 36559/19 and 36570/19, 6 June 2024, §§ 73-76. With particular regard to journalists and media outlets, see also European Media Freedom Act, cited above.
[276] ECtHR, *Stoll v Switzerland* [GC], no. 69698/01, 10 December 2007, § 105.
[277] ECtHR, *Animal Defenders International v. the United Kingdom*, no. 48876/08, 22 April 2013, §103.
[278] ECtHR, *Magyar Helsinki Bizottság v. Hungary*, no. 18030/11, 8 November 2016, § 168.
[279] *See for example* Joint Declaration on Media Freedom and Democracy, the United Nations (UN) Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, the Organisation for Security and Co-operation in Europe (OSCE) Representative on Freedom of the Media, the Organisation of American States (OAS) Special Rapporteur on Freedom of Expression and the African Commission on Human and Peoples' Rights (ACHPR) Special Rapporteur on Freedom of Expression and Access to Information in Africa, 2 May 2023.
[280] Council of Europe, Recommendation No. R (2000) 7 of the Committee of Ministers to member states on the right of journalists not to disclose their sources of information, Appendix: Principle 6, 8 March 2000.
[281] European Data Protection Supervisor, *Preliminary Remarks on Modern Spyware*, 15 February 2022.
[282] *Highly intrusive spyware threatens the essence of human rights*, cited above.
[283] *The Right to privacy in the digital age*, cited above.

offences and involve a covered person;[284] (iv) no other less restrictive measure would be adequate and sufficient to obtain the information sought.

96. The extensively intrusive powers offered by spyware threaten the work product of journalists and the willingness of sources to speak with them. The Pegasus scandal showed that journalists were apparently being targeted simply because they are journalists, which is unacceptable in a democratic society. The Venice Commission considers that legislation should narrowly define the possible targets of the surveillance measures, and provide that certain categories of persons whose interactions may be protected by professional privilege as well as journalists are in principle excluded, with certain limited exceptions. When it is alleged on justified grounds that such persons are committing a specific, defined and serious offence and are posing a defined specific threat to national security, and that court ordered investigation is thus necessary, the Venice Commission considers, in line with the case-law of the ECtHR, that strongly enhanced standards must apply, including higher thresholds before approving surveillance operations and more demanding internal and external oversight (see paragraph 92 above).

C. Scope *ratione materiae* of targeted surveillance measures

97. It is also important that legislation sets out clearly the nature of the offences which may give rise to an interception order. As mentioned earlier, the conditions of clarity and foreseeability of the law do not require States to set out exhaustively the specific offences which may give rise to interception. However, sufficient detail should be provided on the nature of the offences in question.[285] While States have in principle the sovereign authority to determine what is, and is not a serious offence under national law, the ECtHR has made it plain that this is a smaller subset of the overall group of offences: a State is not free to expand this category so that it in practice covers a majority of all offences.[286] This is valid *a fortiori* for intrusive surveillance measures.[287]

98. When it comes to threats to national security, as illustrated above, the requirement of "foreseeability" of the law does not go so far as to compel States to enact legal provisions listing in detail all conduct that may prompt a decision to subject an individual to secret surveillance on "national security" grounds. However, the scope of any discretion conferred on the competent authorities needs to be strictly defined, notably concerning the discretion regarding the material and personal scope of the [judicial] pre-authorisation (see the ECtHR's findings at paragraph 81 above). Moreover, as already mentioned, well-functioning oversight becomes even more important. The CJEU has developed specific standards on national security, finding, among others, that Member States when taking measures to safeguard national security must be able to demonstrate that there are sufficiently solid grounds that they are confronted with a serious threat to national security which is shown to be genuine and present or foreseeable;[288] they should prove that it is necessary to rely on any derogation from EU law in order to safeguard

[284] Article 4 § 3(c) of the Act refers to such persons as "*media service providers, their editorial staff or any persons who, because of their regular or professional relationship with a media service provider or its editorial staff, might have information related to or capable of identifying journalistic sources or confidential communications*".
[285] ECtHR, *Kennedy v. the United Kingdom*, cited above, § 159.
[286] ECtHR, *Iordachi and Others v. Moldova*, no. 25198/02, 10 February 2009, § 44.
[287] As an example, the EU Media Freedom Act provides that intrusive surveillance software should only be deployed on media professionals if it occurs in investigations of offences listed in Article 2(2) of Council Framework Decision 2002/584/JHA punishable in the Member State concerned by a custodial sentence or a detention order of a maximum period of at least three years or in investigations of other serious offences punishable in the Member State concerned by a custodial sentence or a detention order of a maximum period of at least five years, as determined by the national law of that Member State, and provided that no other less restrictive measure would be adequate and sufficient to obtain the information sought.
[288] CJEU, *La Quadrature du Net*, cited above, § 137.

national security,[289] and that the need to protect national security could not have been achieved by applying the relevant EU law provisions.[290]

D. Time-limits of targeted surveillance measures

99. The question of the overall duration of targeted surveillance measures may be left to the discretion of the authorities responsible for issuing and renewing interception warrants, provided that adequate safeguards exist, such as a clear indication in domestic law of the period after which an interception warrant will expire, the conditions under which a warrant can be renewed and the circumstances in which it must be revoked.[291] The ECtHR has criticised domestic legislation which did not lay down a clear limitation in time for the authorisation of a targeted surveillance measure.[292] The CJEU held that when a Member State adopts a legislative measure providing for the real time collection of traffic and location data targeted towards an individual, this must be limited in time, to what is "strictly necessary".[293] The Venice Commission considers that the longer an interference in privacy continues, the greater its effects on human rights and freedoms will be, thus requiring stronger justification. Long periods will be more difficult to justify under the principles of necessity and proportionality.

100. The duration issue apart, the Venice Commission considers that it is also necessary in this context to take account of how intrusive into one's privacy a surveillance measure is. The more intrusive a measure is, the shorter the periods of authorisation should be. In any case where a long period of surveillance is authorised, or where a short period is to be (frequently and repeatedly) renewed, it is particularly important to impose a duty on the investigating body immediately to inform the authorising court/body and/or the oversight body, if conditions change during the course of the investigation. It is indeed possible that an investigation launched in good faith into a serious crime for which intrusive surveillance is permitted morphs, with the elapse of time, into an investigation into a less serious crime or which intrusive surveillance is not permitted – in this case the more intrusive form of surveillance should be immediately halted.

101. Time limits can also apply in another sense, i.e. sunset clauses, specifying that the surveillance-related legislation will expire after a given number of years (see for example footnote 243 above). This can be combined with a requirement to make an official inquiry into how the legislation has been used, and to make this investigation public (at least to the extent that this is possible). This is a best practice which will hopefully serve to reassure the public that powers are not being abused.

E. Test of least possible intrusiveness

102. When it comes to conditions which are to be written into the law, a standard requirement for all special investigative methods is to impose a "least intrusive means" test – this is a natural corollary of the principle of proportionality. The ECtHR has made this clear in the framework of bulk interception,[294] but this applies *mutatis mutandis* to targeted surveillance measures. This requires the requesting body to demonstrate to the authorising body that the information sought through the investigation cannot be obtained by less intrusive means. In doing so any positive effects of such a particular, specific data processing should be assessed, preferably through a collection of independent evidence sources and comparative practices.

---

[289] *See, mutatis mutandis*, CJEU, *European Commission v. Republic of Poland and Others*, Joined Cases C-715/17, C-718/17 and C-719/17, §§152 and 159.
[290] *See, mutatis mutandis*, CJEU, *European Commission v. Republic of Austria ("State printing office")*, Case C-187/16, §§ 78-80.
[291] ECtHR, *Roman Zakharov v. Russia* [GC], cited above, § 250.
[292] ECtHR, *Iordachi and Others v. Moldova*, cited above, § 45.
[293] CJEU, *La Quadrature du Net*, cited above, § 189.
[294] ECtHR, *Big Brother Watch and Others v. the United Kingdom* [GC], cited above, § 448.

103. The authorisation procedure and the oversight should be rigorous, to avoid that such requirements become mere formalities rather than substantive legal requirements to be clearly satisfied. This is not simply a question of legal security. As using spyware still tends to be a very resource-intensive process, the investigating police or security agencies should also have a strong interest in efficiently governing their resources.[295]

F. Authorisation and review of targeted surveillance measures by a judicial or other independent body

104. Under the case-law of the ECtHR, review and supervision of secret surveillance measures may come into play at three stages: when the surveillance is first ordered, while it is being carried out, or after its termination. As regards the first two stages, the very nature and logic of secret surveillance dictate that not only the surveillance itself but also the accompanying review should be carried out without the individual's knowledge. Consequently, since individuals will necessarily be prevented from seeking an effective remedy of their own accord or from taking a direct part in any review proceedings, it is essential that the procedures established should themselves provide adequate guarantees safeguarding his or her rights. In a field where abuse of power is potentially so easy and could have such harmful consequences for a democratic society as a whole, the Court has held that it is in principle desirable to entrust supervisory control to a judge, judicial control offering the best guarantees of independence, impartiality and a proper procedure.[296]

105. Having a purely political authorising procedure, i.e. where the police or a security agency seeks authorisation from the responsible government minister is not acceptable under both the ECHR[297] and the ICCPR. It is possible, however, to combine the two procedures, whereby authorisation is sought from a government minister (who would presumably concentrate on the issue of suitability) whereas the issue of legality is determined by the court. As the ECtHR has ruled repeatedly, beginning with the *Klass* case, judicial authorisation is preferable, as it offers the best guarantees of independence, impartiality and a proper procedure.[298] However, in certain areas there can exist reasons to replace a court with an expert authorising body, provided this body satisfies high standards of independence. The Venice Commission considers, in line with the ECtHR's practice, that having an expert authorisation body can be more justifiable as regards bulk surveillance,[299] but that judicial authorisation is to be preferred in targeted surveillance. This does not rule out having a degree of specialisation in the court or courts which can authorise the use of spyware (see paragraph 111 below).

106. In the context of secret surveillance, the ECtHR has found that, in exceptional cases of urgency, it is possible for the targeted surveillance measure to be carried out without prior authorisation, provided that the court or relevant independent body authorises it within a short deadline.[300] Recently, the ECtHR has found that a period of five days for a court to grant or dismiss *ex-post* the request for a targeted surveillance measure did not provide sufficient safeguards since the application of the emergency authorisation procedure was justified only by the risk of loss of the evidence, and not by the seriousness or nature of the offence. The Court

---

[295] *Device investigative tools used by the Royal Canadian Mounted Police (RCMP) and related issues*, cited above, p. 21

[296] ECtHR, *Roman Zakharov v. Russia* [GC], cited above, § 233.

[297] ECtHR, *Big Brother Watch and Others v. the United Kingdom* [GC], cited above, § 351. See also a recently reported judgment (in Maltese only) of the First Hall of the Civil Court of Malta (acting as Constitutional Court) which has found that the right to a fair hearing of an applicant whose telephone had been tapped was breached as the wiretaps had been done under a warrant issued by the executive rather than a judicial authority.

[298] See ECtHR, *Klass and Others v. Germany, no. 5029/71, 6 September 1978, §§ 55-56,* and *Roman Zakharov v. Russia* [GC], cited above, § 233.

[299] *See* Venice Commission, CDL-AD(2015)010, cited above, §§ 210, 250; CDL-AD(2015)011, cited above, §§ 24, 115-122; *see also* ECtHR, *Big Brother Watch and Others v. the United Kingdom* [GC], cited above, § 351, quoting the Chamber Judgment *Big Brother Watch and Others v. the United Kingdom*, nos. 58170/13 62322/14 24960/15, 13 September 2018, §§ 318-320.

[300] ECtHR, *Ekimdzhiev and Others v. Bulgaria*, no. 70078/12, 11 January 2022, §323.

found that given the dangers that recourse to such a non-judicial emergency procedure entails for the private sphere of the individual subject to secret surveillance, the applicable legislation should contain sufficient safeguards to ensure that its use is sparing and limited to duly justified cases, including safeguards against the repetitive use of the measure in question.[301]

1. Criteria of assessment by authorising court/independent body

107. The ECtHR has emphasised that the authorising court/independent body must be able to assess the reasonableness of the use of the measure in the particular case and it has found violations of the ECHR in instances in which there was no indication that the judges who had issued the warrants had undertaken any supervisory function.[302]

108. In this respect, the ECtHR also scrutinises the scope of review (whether the judge applies a "necessity" or "proportionality" test) and the content of the interception authorisation. It is common to require the investigating agency to provide the basis of the authorisation to the court or independent authorising body, usually expressed in (some level of) "concrete" or "factual" indications of an ongoing/impending criminal offence, or threat to national security, together with some sort of evidentiary threshold.

109. Targeted surveillance is sometimes authorised not only for investigating past or present (ongoing) offences or threats to national security but also potential, future offences or threats to national security. The Venice Commission believes that, in general, the legislation should provide for higher material standards and evidential thresholds when it comes to authorising the use of spyware to investigate impending/future offences or threats (e.g. as regards concrete indications). Judicial or independent authorisation which does not examine these crucial issues is not a real safeguard. All such requirements to provide concrete/factual indications and satisfy given evidential thresholds must be accompanied by the requesting authority's duty to document this in the application. This is necessary, partly because the conditions might well change during the investigation and partly because it will be necessary for the follow-up oversight which must occur.

110. Lastly, the requesting authority should continuously examine the persistence of the reasons for the surveillance and inform the authorising body when and if the reasons for the application of the measure change. If such reasons no longer apply, surveillance must be immediately terminated.[303]

2. Specialisation of judicial and other independent bodies

111. Some States have provided for a degree of specialisation, for example as regards the prosecutors and/or the courts, or as noted above, in creating specialised independent authorisation bodies for targeted surveillance. Different levels of authorisation can also be foreseen corresponding to different types of investigation/data sought or as regards how the surveillance is performed, physically or remotely.[304] As already noted (footnote 265 above),

[301] ECtHR, *Pietrzak and Bychawska-Siniarska and Others v. Poland*, cited above, § 208.
[302] ECtHR, *Ekimdzhiev and Others v. Bulgaria*, cited above, §§307-322; *Haščák v. Slovakia*, cited above; *Zoltán Varga v. Slovakia*, cited above.
[303] *See* for example, in the Slovak Republic, Articles 4 § 6 and 6 § 1 PAIA.
[304] In the Netherlands, the Board of Procurators General (the national leadership of the Public Prosecution Service) gives permission to use spyware in criminal investigations. In Switzerland, for intelligence measures carried out in the territory of the Federation, the intelligence measure must be authorised by the president of a special section of the Federal Administrative Court. In addition, the measure must be approved by the Minister of Defence after consultation with the Minister of Foreign Affairs and the Minister of Justice; cases of particular importance may be referred to the Federal Council (the Swiss government). In Spain a Supreme Court magistrate (from the administrative or criminal chamber) and a substitute are appointed to authorise interceptions of communications by intelligence services. In Sweden, Section 14 of the Act (2020:62) on Secret data reading provides that in specific cases in connection with foreign terrorist suspects, a specialised court (the Stockholm district court) is competent.

specialised units also exist in some law enforcement agencies. Such units provide the necessary technical support for the deployment of intrusive surveillance software, but also support operational units in meeting the legal requirements needed for the use of such software. There can be advantages for efficiency and oversight in concentrating competence to a particular specialist body within law enforcement or security/intelligence. Moreover, as also noted, it can assist in maintaining confidentiality in handling the information obtained vis a vis other parts of the investigating organisation). In any event, rules must exist, and be strictly followed, limiting the information which may be stored, analysed and communicated to other parts of the investigating agency, or outside of the agency. [305]

112. As the Venice Commission has noted previously, there can be advantages in a degree of specialisation, in that by means of frequent repetition, those involved in the authorisation process become more expert in it. Thus, a more expert body might be more willing to set more, and more effective, conditions on the authorisations it issues. At the same time, it is important to avoid "case hardening" (a tendency of the specialised judges to identify with the security officials) and maintain public confidence in the integrity of the authorisation system.[306]

3. Privacy/security advocates

113. The Venice Commission has previously found that the fact that authorisation of surveillance measures is carried out without the individual's knowledge, can, to some extent, be compensated for by the presence, in the authorisation procedure, of privacy advocates, i.e. legal professionals that represent the interests of targeted persons and organisations in the authorisation procedure.[307] Whether or not such advocates can be a real safeguard in the process depends on a number of factors. The prosecutor (or requesting body) will usually be in possession of much more evidential elements. A security screened advocate is not acting directly for the suspect and cannot, obviously, consult with him or her. The advocate may be given only a very short time to familiarise themselves with the file, and thus be at a procedural disadvantage compared to the prosecutor. In Sweden, a Commission of Inquiry found that the requirement to involve a security screened advocate seldom if ever leads to an authorisation being refused.[308] On the other hand, the mechanism can still have some value in that it can lead to conditions being imposed to minimise the intrusion into privacy, for the target or others affected by the surveillance. Moreover, it can formalise the process of obtaining authorisation, making it clearer that it is the requesting body which has the burden of showing the need for use of surveillance, and that all the conditions for surveillance are fulfilled.

G. National systems of oversight

114. Oversight is essential to help to ensure that spyware - which entails such significant interferences with privacy and data protection rights - is used in accordance with the law. Oversight is also necessary to guard against abuse by police and intelligence agencies and provides guarantees that these agencies fulfil their mandates and use their powers and resources appropriately and effectively.

115. The Venice Commission has emphasised in the context of control over security agencies, that the primary guarantee against abuse of powers is the internal oversight carried out by the security services themselves, in order to ensure that the staff working in the agencies are committed to the democratic values of the State and to respecting human rights.[309] A similar point can be made as regards law enforcement.

[305] ECtHR, *Centrum för Rättvisa v. Sweden* [GC], cited above, § 276.
[306] Venice Commission, CDL-AD(2015)010, cited above, §§ 221-223.
[307] Venice Commission, CDL-AD(2015)011, cited above, § 100; CDL-AD(2016)012, cited above, § 97.
[308] See the Swedish official inquiry into secret surveillance, SOU 2012:44.
[309] Venice Commission, CDL-AD(2015)010, § 134.

116. Nonetheless, external oversight is also necessary, to reassure parliament and the public that internal oversight routines are being followed properly.[310] Although it is in principle desirable to entrust authorising control to a court, *post hoc* oversight by non-judicial bodies may be considered compatible with the ECHR, provided that the oversight body is independent of the authorities carrying out the surveillance, and is vested with sufficient powers and competence to exercise an effective and continuous control,[311] and to ensure effective protection against abuse, including investigative and remedial powers. Oversight bodies' mandates complement each other, so that, overall they provide continuous control and ensure proper safeguards. Such complementarity can be achieved with informal cooperation between oversight bodies or statutory means.[312] In the framework of "bulk interception", the ECtHR noted the need for "end to end" safeguards, covering the whole process of surveillance, including the issue of transfer of information/material to other organisations than the one doing the investigation, in one's own and other states.[313]

117. A difference exists between security/intelligence oversight and oversight of the police/law enforcement. Law enforcement surveillance operations tend to end up in prosecution, and so there is, ultimately, an opportunity for *post hoc* judicial control. This tends not to be the case for security/intelligence work, and so specialised control/oversight bodies need to be established. As observed above, the existence of Parliamentary supervisory committees is a common feature of the oversight system for security/intelligence in member States.[314] Parliaments enjoy democratic legitimacy and can hold the executive accountable for the way it directs and oversees the activities of the security services.[315] Having said this, the Venice Commission has previously warned against the shortcomings of purely parliamentary oversight.[316] Expert bodies, which carry out the oversight of the activities of intelligence services in a number of states, have proved to be more successful and effective in several states, or likewise a combination of a specialised body and a parliamentary body.[317]

118. Where a State has not established a specialised security oversight body, Data Protection Authorities (DPAs) may play an important role in the system of oversight of security and intelligence as a whole, in particular as regards security files (although it has to be noted that many DPAs do not have powers to investigate matters of national security).[318] Providing independent oversight institutions with sufficient powers and human (including technically qualified and specialised professionals), financial and technical resources is key, especially considering the extensive powers and capacities that intelligence services generally have and the secret nature of many of their activities. Along with discussing annual reports, inquiries and periodic audits, DPAs should be able to initiate full-scale as well as ad-hoc investigations and have permanent, full and direct access to classified information, and documents to fulfil their mandate effectively.

119. The Venice Commission shares the view of the EU Fundamental Rights Agency according to which bodies exercising oversight over intelligence services should evolve in a similar fashion to intelligence laws and capacities of intelligence services. Greater powers and competencies of the latter must be balanced by a greater degree of independent oversight, along with adequate resources and expertise to ensure effective oversight.[319] Cooperation between relevant oversight

[310] See also Article 11 § 3 of Convention 108+.
[311] ECtHR, *Roman Zakharov v. Russia* [GC], cited above, § 275.
[312] FRA Report, Section 1.2, Opinion 6.
[313] *See, for example*, ECtHR, *Big Brother Watch v. the United Kingdom* [GC], cited above, § 350; *Centrum för Rättvisa v. Sweden* [GC], cited above.
[314] *See* section IV.E above and FRA Report, cited above, § 1.5.2.
[315] *Democratic and effective oversight of national security services*, cited above, p. 45.
[316] In the context of strategic surveillance, *see* Venice Commission, CDL-AD(2015)011, cited above, §§ 108-109.
[317] Venice Commission, CDL-AD(2015)010, cited above, §§ 228-250.
[318] FRA Report, Section 2.3.
[319] FRA Report, Section 1.2, Opinion 3.

authorities should ensure the "end-to-end" oversight vouched for by the ECtHR.[320] It is important that a holistic approach is taken to the issue of oversight, and that oversight powers provided for by the law are given effect in practice.

H. Notification of targeted surveillance measures

120. The ECtHR requires that the individual placed under surveillance normally be informed subsequently, so that he or she can be involved in monitoring the measure. It has thus laid down a general obligation of retrospective notification, subject to exceptions.[321] Where there is no standing complaints mechanism, then the total absence of a requirement to notify the subject of interception at some point after the surveillance has ceased has been found to be incompatible with the Convention, in that it deprives the interception subject of an opportunity to seek redress for unlawful interferences with his Article 8 rights and renders the remedies available under the national law theoretical and illusory rather than practical and effective.[322] Conversely, the Court has found that the absence of any obligation to notify the person concerned of the interception measure at any stage of its application was compatible with the Convention, where persons who suspected that their communications were or had been the subject of interception could refer the matter to an independent complaints body, with full powers of investigation, and whose jurisdiction was not subject to notification of the interception.[323] Although it may not be possible to require notification in all cases, it is desirable to notify the person targeted by surveillance as soon as notification can be given without jeopardising the purpose of the measures and after the surveillance measures have been lifted.[324] In a recent judgment, relying *inter alia* on the findings of a previous Venice Commission Opinion, the ECtHR found that the absence of a notification obligation in the Polish context of secret surveillance, even after a certain period of time had elapsed, was one of the elements that led to conclude that the overall legal framework was in violation of Article 8 of the Convention.[325]

121. As already mentioned above, notification of an individual target may obviously jeopardise confidential methods or on-going operations. Nevertheless, it is important to provide for a general obligation of the relevant authorities to notify the target *ex-post*, and to formulate exceptions from this rule. A decision in a specific case that a target cannot be notified, even after the termination of the surveillance, should always be notified to the external oversight body and, normally, approved by that body. When there is notification, and the person therefore learns about the surveillance, *ex parte* proceedings before the court issuing the surveillance warrant may be supplemented by fully adversarial proceedings in which the court would examine the lawfulness of the surveillance *de novo*. Indeed, notification is primarily a mechanism for obtaining redress. The Venice Commission has held that it is necessary for individuals who claim to have been adversely affected by the exceptional powers of security and intelligence agencies to have some avenue for redress.[326]

122. Article 13 of the ECHR requires States to put in place an effective remedy mechanism for alleged violations of Convention rights. Also, Article 12 of Convention 108+ requires appropriate

[320] ECtHR, *Segerstedt-Wiberg and Others v. Sweden*, cited above; see also FRA Report, Section 3. To be also noted that Article 17 of Convention 108+ requires a mandatory cooperation of supervisory authorities in cross-border cases.
[321] ECtHR, *Roman Zakharov v. Russia* [GC], cited above, §§ 286 et ff.
[322] ECtHR, *Association for European Integration and Human Rights and Ekimdzhiev v. Bulgaria*, no. 62540/00, 28 June 2007, §§ 90-91.
[323] ECtHR, *Kennedy v. the United Kingdom*, cited above, § 167.
[324] ECtHR, *Pietrzak and Bychawska-Siniarska and Others v. Poland*, cited above, § 238.
[325] *Ibidem*, §§ 238-247; *see* Venice Commission, CDL-AD(2016)012, cited above. Similar requirements have been imposed by the European Court of Justice in the *Tele2 and Watson* and *Quadrature du Net* cases, cited above.
[326] For an overview of the Venice Commission's findings on complaints mechanisms *see* Venice Commission, CDL-AD(2015)010, cited above, §§ 251 ff.

judicial and non-judicial sanctions and remedies for violations of the provisions of the Convention.[327]

123. The Fundamental Rights' Agency of the European Union has highlighted the need to ensure minimum requirements for remedies to be effective:[328] first of all non-judicial bodies must be independent; in addition, they must: (i) raise awareness of surveillance measures among individuals, either through notification or through any other opportunity to obtain information about interceptions; (ii) ensure access to classified information for remedial bodies; (iii) ensure appropriate redress, for example the destruction of the data collected or monetary relief; and (iv) ensure proper expertise within remedial bodies.

I. Protection of third parties from measures related to spyware use

124. One of the special features of spyware use is that, depending upon the circumstances, it can be done remotely (remote code execution) or physically (although this is presumably rarer, as it requires the police or security agency to have temporarily obtained access to a suspect's device). A particular feature of remote code execution is that the exploitation of a vulnerability which allows the police or security agency to access the suspect's device might exacerbate software and hardware vulnerabilities of devices belonging to third parties.[329] A difficult balance has to be struck here. On the one hand, the police/security agency may have good reasons for keeping quiet about a given vulnerability, which they have found or created, as this will allow them to exploit this for investigative purposes in the future. On the other, leaving such vulnerabilities open means that malevolent actors, such as members of organised crime groups etc. may also find and exploit them. Legislation should therefore provide for the protection of third parties from the exploitation, by the law enforcement or intelligence agencies, of software vulnerabilities. Moreover, the law enforcement or intelligence agency should not leave the security of the affected software or hardware generally in a worse condition than before an operation was started.

125. In one State it was suggested that the police/security agency establish a mechanism which properly weighs the advantages and disadvantages of remaining silent/disclosing in each case and to document its decision-making in the matter (allowing future oversight, and if need be, accountability). Moreover, it was suggested to provide for a central register of vulnerabilities for each agency.[330]

J. Duty to destroy "surplus information"

126. As already mentioned, the use of spyware enables such measures as real-time monitoring of communications, movements or online activities, search of the stored data on the device and activation of an in-built camera and microphone for surveillance. The use of spyware against a mobile device can thus lead to the collection of "surplus information", i.e. information not pertinent to the particular investigation/surveillance for which authorisation has been given. Such collection poses particularly serious risks to privacy and other fundamental rights of the target and those

[327] Insofar as DPAs are concerned, the FRA Report, cited above, Section 2.3, provides an overview of the remedial powers of DPAs in Europe.
[328] FRA Report, Section 2.1.
[329] The Italian Data Protection Authority has emphasised to the risks for confidentiality in the case where the inoculation of intrusive surveillance tool is not direct but takes place by downloading applications from platforms freely accessible to any user. In this case, there is a risk of installation by third parties that are completely unrelated to the purposes of the investigation. Therefore, this risk should be eliminated by only allowing the use of applications that prevent the acquisition by third parties, or by providing that the capturing activity should only start after verifying that the software is uniquely associated to the device corresponding to the one covered by the authorisation decree, *see Documento approvato dalla 2ª Commissione permanente (Giustizia) nella seduta del 20 settembre 2023 a conclusione dell'indagine conoscitiva sul tema delle intercettazioni*, cited above, p. 43.
[330] Review report 53 on the use of the investigatory power to hack by the AIVD and the MIVD in 2015, cited above, p. 25.

within his or her contacts and raises serious questions about the proportionality of any use of spyware.

127. The ECtHR has consistently underlined the need for a requirement to destroy immediately any data that are not relevant to the purpose for which they have been obtained.[331] It is particularly important that such provisions exist as regards the use of spyware because of the multiplicity of different types of information, some of it particularly sensitive personal information, which can emerge from this activity.[332]

128. Two different types of information can emerge from an investigation/surveillance which were not part of the justification for issuing the authorisation to use spyware. The first is personal information not concerning an offence or a threat to national security. Such information should be subject to an immediate destruction requirement.[333] This should be backed up by oversight.[334] The second type of information is information indicating that a different threat to national security,[335] or crime, has occurred, or is occurring or will soon occur, i.e. different from that for which authorisation was been granted.

129. To avoid misuse of spyware and maintain public confidence that the system is not being abused, a sensible rule is usually to require the destruction of this information. One can envisage an exception where the offence, or threat to national security in question, while not part of the basis of the original authorisation, is nonetheless of sufficient seriousness (a real and serious threat), were it known at the time, to fulfil the conditions for authorising the use of spyware in the first place.[336] Allowing such an exception presupposes some form of layered access to the material gathered (see footnote 265 above). Moreover, to prevent this exception from, in practice, becoming the rule, there should be a requirement to seek and obtain permission to retain such narrowly defined information from the court (or independent body) which authorised the original warrant in the first place. All such grants of permission should also be documented and followed up by external oversight.

K. Control of spyware export

130. As indicated above, according to the PACE Resolution 2513(2023), some Council of Europe member States may have also exported Pegasus or similar spyware to third countries with oppressive and authoritarian regimes. In Resolution 2045(2015), PACE urged member and observer States to, *inter alia*, refrain from exporting advanced surveillance technology to authoritarian regimes.[337] A connected issue is the fact that commercial spyware is developed by private companies. As the Pegasus revelations have shown, private companies have been involved not only in the production of spyware but also in providing spyware as a service. In this regard, outsourcing "core" State functions such as surveillance to companies interested in selling

[331] ECtHR, *Roman Zakharov v. Russia* [GC], cited above, § 255, referring to *Klass and Others v. Germany*, cited above, § 52.
[332] The Constitutional Court of the Republic of Moldova, in its judgment no. 31 of 23 September 2021 found that it is necessary for the defence to have the opportunity to have access, either at the end of the criminal investigation or at the end of the trial on the merits, to the metadata obtained as a result of the application of secret surveillance, even when the destruction of information obtained from secret surveillance of metadata has been ordered because deemed irrelevant by the investigating judge.
[333] See for example Section 23 of the Swedish Act (2020:62) on Secret data reading.
[334] There can obviously be difficulties in reconciling oversight with destruction requirements, as if these operate properly, there is nothing for the oversight body to "oversee". However, one can document the fact that information was destroyed, and the date on which it occurred. Moreover, the oversight body can check that whatever automated destruction requirements that exist are working, e.g. by testing these with hypothetical information.
[335] This obviously presupposes that threats to national security can be specified with sufficient precision.
[336] *See* for example Sections 28-31 of Swedish Act (2020:62) on Secret data reading.
[337] PACE, Resolution 2045(2015), *Mass Surveillance*, 21 April 2015, § 19.

their services and making a profit, especially in an unregulated private industry, carries very high risks of abuse of such technologies, in addition to the risk of the lack of accountability.[338]

131. Spyware is classed as a dual-use technology (i.e. that can be used for both civilian and military purposes); hence the need to receive an export licence. Successful governance of the spyware industry entails effective export controls. Regulation (EU) 2021/821 has set up a regime for the control of exports, brokering, technical assistance, transit and transfer of dual-use items (the Dual-Use Regulation).[339] Global rules have been established in the Wassenaar Arrangement, to which 31 Council of Europe member States are parties to.[340] The Wassenaar Arrangement was concluded in 1999 as a multilateral export control agreement among States in order to contribute to regional and international security and stability, promotes transparency and greater responsibility in transfers of conventional arms and dual-use goods and technologies. However, the Arrangement lacks guidelines or enforcement measures that would directly address human rights violations caused by surveillance tools.[341]

132. The Venice Commission considers that participating States to the Wassenaar Arrangement could explore the possibility of conditioning technology licensing rules on the receiving State's (and the producing company's) compliance with human rights standards.[342] Insofar as private companies are concerned, the granting of export licenses could be conditioned on the implementation of the United Nations Guiding Principles on Business and Human Rights with respect to the design, sale, transfer, or support of such technologies.[343] This is compliant with relevant recommendations made by PACE[344] and by the European Parliament[345] And also follows the line now adopted by states participating in the Joint Statement on Efforts to Counter the Proliferation and Misuse of Commercial Spyware (see footnote 249 above). The commitments made there could be developed further by following key recommendations contained in the 2019 report of the UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression are, among others: (i) to establish an immediate moratorium on the global sale and transfer of private surveillance technology until rigorous human rights safeguards are put in place to regulate such practices and guarantee that governments and non-State actors use the tools in legitimate ways;[346] and (ii) for companies to put in place robust safeguards to ensure that any use of their products or services is compliant with human rights standards. These safeguards include contractual clauses that prohibit the customisation, targeting, servicing or other use that violates international human rights law, technical design

---

[338] See, *mutatis mutandis*, Venice Commission, CDL-AD(2009)038, *Report on private military and security firms and erosion of the state monopoly on the use of force*.
[339] Regulation (EU) 2021/821 of the European Parliament and of the Council of 20 May 2021 setting up a Union regime for the control of exports, brokering, technical assistance, transit and transfer of dual-use items (recast).
[340] Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies. Wassenaar Arrangement Participating States are Argentina, Australia, Austria, Belgium, Bulgaria, Canada, Croatia, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, India, Ireland, Italy, Japan, Latvia, Lithuania, Luxembourg, Malta, Mexico, Netherlands, New Zealand, Norway, Poland, Portugal, Republic of Korea, Romania, Russian Federation, Slovakia, Slovenia, South Africa, Spain, Sweden, Switzerland, Türkiye, Ukraine, United Kingdom and United States.
[341] 2019 UN SR Report, cited above, §§ 34-35.
[342] As suggested by Privacy International, licensing might be denied where there is a "substantial risk that those exports could be used to violate human rights, where there is no legal framework in place in a destination governing the use of a surveillance item, or where the legal framework for its use falls short of international human rights law or standards", *see*, D. Kaye, *The Spyware State and the prospects for accountability*, The Global Forum, Global Governance 27 (2021) Brill Nijhoff, pp. 487-488.
[343] United Nations, Special Representative of the Secretary-General on the issue of human rights and transnational corporations and other business enterprises, *Guiding Principles on Business and Human Rights: Implementing the United Nations "Protect, Respect and Remedy" Framework*. See also the UK Foreign, Commonwealth & Development Office, *The Pall Mall Process: tackling the proliferation and irresponsible use of commercial cyber intrusion capabilities*, in particular § 8.
[344] PACE, Resolution 2513(2023), cited above, § 14.9.
[345] EP Recommendation. cited above, § 56.
[346] 2019 UN SR Report, cited above, § 66(a).

features to flag, prevent or mitigate misuse, and human rights audits and verification processes.[347]

133. In line with the multi-Government commitment referenced at paragraphs 73 and 132 above and so as to promote transparency and effective oversight the Venice Commission also considers that governments should as a matter of good practice make annual public statements indicating whether they have licensed spyware from commercial providers and if so from which commercial entity[348] as well as considering any other suitable and appropriate transparency measure such as publishing regular reports on the use of spyware and on threats posed by foreign commercial spyware.

VI. Conclusion

134. By letter of 6 December 2023, the then-President of the Parliamentary Assembly of the Council of Europe (PACE), Mr Tiny Kox, requested the Venice Commission, pursuant to Resolution 2513 (2023) of the Parliamentary Assembly on "Pegasus and similar spyware and secret state surveillance", to conduct a study on the legislative framework and practice on targeted surveillance of all member States (in priority Poland, Hungary, Greece, Spain and Azerbaijan; and then Germany, Belgium, Luxembourg, the Netherlands and all the other member States). In reply to the request, the Venice Commission has conducted a comparative study to assess the existing rules on targeted surveillance and notably on the use of spyware in its member States. The Venice Commission has considered the legal provisions of the States that sent official information to PACE and of those on which the members of the Venice Commission/experts provided information by replying to a questionnaire which was prepared by the rapporteurs. The complexity of the legislative frameworks in question, the lack of comprehensive and practical information on the implementation of existing international standards, such as Article 9 of Convention 108, as well as the scarce specific regulation of spyware were an important factor to consider when preparing the report.

135. Spyware is an unprecedently intrusive surveillance tool that can be used for interference with electronic devices, notably smartphones or computers, without the user's knowledge, and which allows the operator to penetrate the devices and, depending on the specific tool, track geolocation in real-time, read all data stored, all communications made (bypassing possible safeguards, such as encryption) and taking control of whatever hardware and software is available on the device, such as microphones or cameras. If kept unregulated, spyware might turn into a 24-hour surveillance device, gaining complete access to all sensors and information on the personal device. This would turn it into a surveillance weapon that could be used to curtail human rights, censor and criminalise criticism and dissent and harass (if not suppress) journalists, human rights activists, political opponents, or repress civil society organisations, as shown by the multiple allegations and revelations. It is therefore crucial to provide for clear contours concerning the use of spyware by State in order to prevent and eradicate abusive practices.

136. Drawing on the jurisprudence of the ECtHR on targeted surveillance, the Venice Commission's previous reports, other European and international standards such as Convention 108+ as well as on the comparative analysis of relevant legislation in the Venice Commission's member states, the present report has attempted to identify the minimum safeguards that should be in place, when dealing with such intrusive measures of targeted surveillance, to prevent any abuse of power. Ultimately, it will be for the ECtHR, in the context of deciding the "spyware" cases which are currently pending or may be brought before it, to set the applicable specific standards in this domain.

---

[347] *Ibidem,* § 67 (b).

[348] Recent press reporting in relation to litigation in the United States suggests that Governments may be dependent on commercial operators themselves to carry out monitoring through spyware.

137. The Venice Commission finds that the use and development of intrusive surveillance software such as spyware should only be possible if the relevant legal framework meets certain strict requirements. The following safeguards, at a minimum, need to be in place:

- All significant provisions regulating the use of an intrusive surveillance tool such as spyware (if any) must be set out in primary legislation, which should clearly define the (restricted) scope *ratione materiae, personae* and *temporis* of targeted surveillance through spyware, which cannot be likened to other measures of targeted surveillance;
- In particular, legislation should narrowly define the possible targets of the surveillance measures, and provide that certain categories of persons whose interactions may be protected by professional privilege as well as journalists are in principle excluded, with certain limited exceptions;
- Domestic legislation must make a clear distinction of the type of investigation/surveillance in the context of which use of spyware may be authorised and the personal data that may be sought; such distinction should affect the assessment of the necessity and proportionality of measures taken;
- The requesting authorities (law enforcement or intelligence agency) should always demonstrate that the information sought in the investigation was necessary to the legitimate purpose and could not be obtained by less intrusive means;
- There must be well-regulated *ex-ante* authorisation procedures before a court or another independent body (or in exceptional and urgent cases, rules which provide for the swift confirmation by such court or independent body of the targeted surveillance measure); and the duration of the surveillance measures must be limited to what is strictly necessary;
- The whole surveillance process needs to be backed up by effective external independent oversight institutions, which are sufficiently resourced, qualified and specialised, and cannot be entrusted exclusively to the executive;
- The agency carrying out the authorised investigation/surveillance, and accessing the data, must not access more data than is permitted by the authorisation it has received: any data that are not relevant to the purpose for which they have been obtained should be identified without (undue) delay and permanently destroyed;
- The persons under surveillance must be notified subsequently, subject to exceptions defined by law, so that they can be involved in monitoring and challenging the measure; whenever this is not possible (eg. national security issues) a standing complaints mechanism must be introduced;
- Legislation should provide for the protection of third parties from the exploitation, by the law enforcement or intelligence agencies, of software vulnerabilities;
- States should condition technology export licensing rules on the receiving State's (and the producing company's) compliance with the human rights standards identified in this report;
- Governments should make annual public statements indicating whether they have licensed spyware from commercial providers and if so from which commercial entity as well as considering any other suitable and appropriate transparency measure such as publishing regular reports on the use of spyware and on threats posed by foreign commercial spyware.

138. The Venice Commission remains at the disposal of the Parliamentary Assembly for further assistance in this matter.