UNITED NATIONS
HUMAN RIGHTS
SPECIAL PROCEDURES
SPECIAL RAPPORTEURS, INDEPENDENT EXPERTS & WORKING GROUPS

PALAIS DES NATIONS • 1211 GENEVA 10, SWITZERLAND
www.ohchr.org • TEL: +41 22 917 9000 • FAX: +41 22 917 9008 • E-MAIL: registry@ohchr.org

Mandate of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism

Submission as Amicus Curiae of the UN Special Rapporteur on the promotion and protection of human rights while countering terrorism to the European Court of Human Rights in the case of Mikołaj Pietrzak v. Poland and Dominika Bychawska-Siniarska and others v. Poland - Requests Nos. 72038/17 and 25237/18

INTRODUCTION

1. The United Nations Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism established pursuant to Human Rights Council resolution 40/16 has the honour to submit this amicus brief in the case of *Mikołaj Pietrzak v. Poland and Dominika Bychawska-Siniarska and others v. Poland (Requests Nos. 72038/17 and 25237/18)* for the consideration of the European Court of Human Rights, pursuant to article 36, paragraph 2, of the European Convention on Human Rights.

2. The submission of the present amicus brief is provided by the Special Rapporteur on a voluntary basis without prejudice to, and should not be considered as, a waiver, express or implied, of any privileges or immunities which the United Nations, its officials or experts on mission, pursuant to 1946 Convention on the Privileges and Immunities of the United Nations. Authorization for the positions and views expressed by the Special Rapporteur, in full accordance with her independence, was neither sought nor given by the United Nations, including the Human Rights Council or the Office of the High Commissioner for Human Rights, or any of the officials associated with those bodies.

3. The Special Rapporteur reports regularly to the UN Human Rights Council and General Assembly on the protection of human rights and fundamental freedoms while countering terrorism, countering violent extremism and extremism including broadly related security regulation by states. In this context, the Special Rapporteur has regular dialogue with security entities including Intelligence Services. Her mandate has issued a stand-alone report to the Human Rights Council entitled "Compilation of good practices on legal and institutional frameworks for intelligence services and their oversight", which is of particular relevance to the matters under consideration by this Court.[1] The Special

[1] A/HRC/10/3, paras 25-78; A/HRC/14/46.

Rapporteur also refers to her in-depth analysis on the use of security and counter-terrorism measures against civil society actors.[2]

4. As a result, the Special Rapporteur is in a position to assess the broad human rights implications engaged by the collection of intelligence and the appropriate human rights safeguards which are required to ensure that intelligence collection, use and retention is human rights compliant and shares those insights with the European Court of Human Rights (ECtHR). This case offers an opportunity for the Court, in addressing this important issue, to set international best practice for compliance with human rights standards.

5. The Special Rapporteur notes that the applicants in this case are prominent civil society actors, respectively a lawyer and the chair of the Warsaw Bar Association, two members of the Helsinki Foundation of Human Rights and two members of the Foundation Panoptykon.

6. The Special Rapporteur's intervention is framed with the understanding that the intercept of intelligence material must be authorized by a judicial warrant in Poland.[3] However, more is required to ensure that the national intelligence infrastructure is compliant with the European Convention on Human Rights (ECHR).

7. In the case at hand, it is accepted by the Parties that that an individual, who is the subject of an intelligence operation, cannot access information collected in the course of law enforcement activity, and there is no general entitlement to *post facto* notification of being the subject of intelligence gathering in Poland. There is no legal means available in Poland to review the legality of an interception before an independent body, once surveillance has ceased. Moreover, unless a criminal procedure is initiated after an investigation where intelligence gathering was used, a person will be unable to know whether they have been the subject of surveillance.

8. In the present brief, the Special Rapporteur will provide her views on the challenges for human rights triggered by the use of intelligence gathering (I) and will assess the conditions for the restrictions of these human rights (II). The Special Rapporteur will then provide her assessment on the systems of protection in the context of intelligence gathering (III) to finally discuss the matter of use of intelligence on civil society actors and concerning political participation (IV).

9. The Special Rapporteur is of the view that there is an absolute necessity, in the context of intelligence gathering, to guarantee that three levels of protection of human rights are established through: i) a judicial order authorizing intelligence gathering; ii) an independent oversight mechanism; iii) a *post facto* notification to the individuals concerned. She underscores the harm to a democratic society and

[2] A/HRC/40/52.
[3] According to art. 19(1)(8) of the Police Act.

to the rule of law when surveillance of civil society actors and legal counsel is undertaken in the absence of robust checks and oversight of intelligence agencies.

I. VIEWS OF THE SPECIAL RAPPORTEUR ON THE IMPORTANCE OF HUMAN RIGHTS COMPLIANT INTELLIGENCE GATHERING

10. The Special Rapporteur notes that intelligence gathering is an increasing pervasive aspect of state security practices and the scope of intelligence gathering, use, storage and exchange has intensified among states in recent decades. The United Nations General Assembly has highlighted that: "the rapid pace of technological development enables individuals all over the world to use new information and communication technologies and at the same time enhances the *capacity of governments, companies and individuals to undertake surveillance*, interception and data collection, which may violate or abuse human rights, in particular the right to privacy."[4] The drive to 'datafication', namely the pervasive and wide-ranging use of data collection in the context of the work of intelligence services creates obvious human rights and rule of law challenges.[5]

11. To that end, General Assembly resolution 68/167 on the *Right to Privacy in the Digital Age* calls on States to do the following:

> (c) To review their procedures, practices and legislation regarding the surveillance of communications, their interception and the collection of personal data, including mass surveillance, interception and collection, with a view to upholding the right to privacy by ensuring the full and effective implementation of all their obligations under international human rights law;
>
> (d) To establish or maintain existing independent, effective domestic oversight mechanisms capable of ensuring transparency, as appropriate, and accountability for State surveillance of communications, their interception and the collection of personal data.

12. Intelligence gathering, storage and use are sites of interaction between the "open state" (typified by open rule of law-based processes such as courts), and the "closed" or "secret state"(typified by sealed and non-transparent sites such as intelligence operations and certain aspects of the functioning of the security sector).[6] This Court plays a crucial mediating role in ensuring that the operation of the "secret state" within the Council of Europe is subject to the rule of law, conforms with essential legal guarantees and is not a grey zone defined by a lack human rights compliant activity by state agents.

---

[4] A/RES/68/167; A/RES/69/166; A/RES/71/199 (emphasis added). The Special Rapporteurs also note that the right to privacy is found in Convention on the Rights of the Child (article 16); International Convention on the Protection of the Rights of All Migrant Workers and Members of Their Families (article 14).

[5] See generally Gavin Sullivan, *The Law of the List, UN Counterterrorism Sanctions and the Politics of Global Security Law*, Cambridge University Press, 2020.

[6] Fionnuala Ní Aoláin and Colm Campbell, "Managing Terrorism (9)", *Journal of National Security Law & Policy,* 367-412, 2018.

13. In general terms, the stated main function of intelligence agencies is to detect potential national security threats, by gathering data and information in such a way as not to alert those targeted. This might be done through a range of special investigative techniques such as secret surveillance, interception and monitoring of communications, secret searches of premises and objects, and the use of infiltrators. The scale and impact of these measures on the human rights of an increasingly wide array of individuals is extensive.

14. Intelligence gathering involves *inter alia* the gathering of private, intimate, familial, identity-related, religious, sexual or professional information on a person without his/her consent and constitutes a *prima facie* interference with of a number of rights protected by the European Convention on Human Rights (ECHR), including its articles 8, 9, 10, and 13 and the International Covenant on Civil and Political Rights (ICCPR), articles 17, 18, 19 and 26.[7]

15. The right to privacy is expressed in article 12 of the Universal Declaration of Human Rights, article 17 of the International Covenant on Civil and Political Rights (ICCPR) and article 8 of the ECHR. The mandate of the Special Rapporteur stresses that States have an obligation under international human rights law to safeguard the privacy of persons within their jurisdiction. In this sense, the ICCPR guarantees a person's right not to be subjected to "arbitrary or unlawful interference with his privacy, family, or correspondence".

16. Technological advancements have also made surveillance more intrusive on an individual's life, as recognized by the General Assembly in addressing the right to privacy in this digital age.[8] The international and regional recognition of the right to privacy demonstrates a "universal recognition of [its] fundamental importance, and enduring relevance, [...] and of the need to ensure that it is safeguarded, in law and in practice".[9] However, about one third of the world's jurisdictions do not have adequate (or any) privacy protections incorporated in law and practice.[10] Even in the case of countries with relevant protections embedded in domestic law, a comparative analysis shows consistent shortcomings in safeguarding the right to privacy in practice, together with a trend towards

---

[7] Noting also the relevance of the EU Charter of Rights entry into force December 2009, art. 7 (privacy) and art. 8 (data collection). See also the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108). Noting also EU Directive 95/46/EC; and Court of Justice of the European Union (ECJ), *Judgement, Data Protection Commissioner v Facebook Ireland and Maximillian Schrems*, C-131/8, 16 July 2020.

[8] A/HRC/39/29, para. 14; See also Privacy International, "Biometrics: Friend or Foe of Privacy?", 2017, *available at* https://privacyinternational.org/sites/default/files/2017-11/Biometrics_Friend_or_foe.pdf.

[9] A/HRC/39/29, para. 13.

[10] *See*, for example, United Nations Conference on Trade and Development, "Data Protection and Privacy Legislation Worldwide", *available at* *https://unctad.org/en/Pages/DTL/STI_and_ICTs/ICT4D-Legislation/eCom-Data-Protection-Laws.aspx*.

stepping up data collection and retention of data —a trend that risks "creating surveillance states".[11] These regulatory gaps make the intervention of this Court all the more compelling.

17. The Special Rapporteur underscores that the right to privacy functions as a gateway right, namely as a right which enables and supports the promotion and protection of other fundamental rights, and cannot be seen in isolation from that critical scaffolding role it plays in our contemporary society, particularly given the datafication and digitalization of daily lives for most persons.

18. In this context, both the General Assembly and the Human Rights Council have stressed that the right to privacy serves as one of the foundations of democratic societies and, as such, plays an important role for the realization of the rights to freedom of expression and to hold opinions without interference as well as to the freedoms of peaceful assembly and association.[12] The adverse impacts from privacy violations may impede the realisation of a broad spectrum of rights. These include, *inter alia*, the right to equal protection of the law without discrimination, the rights to life, to liberty and security of person, fair trial and due process, the right to freedom of movement, the right to enjoy the highest attainable standard of health, and to have access to work and social security. Such concerns are particularly well-grounded when addressing surveillance and the data that is collected, stored, shared and exchanged from it.

19. The capacity for intelligence gathering by governments to interfere with the right to privacy is thus well recognised. All the more so when the data in question is gathered in secret. Collection, retention, processing, sharing, and other uses of information relating to a person, particularly when done without the person's valid consent which is always the case with secret surveillance, amount to an interference with that person's right to privacy and thus must meet a set of conditions in order for such measures to be human rights-compliant, which will be developed in the following section.[13]

II. Position on lawful restrictions of human rights due to Intelligence gathering

20. When the collection of intelligence data leads to a restriction of the rights mentioned in the first section, it must be prescribed by law, necessary in a democratic society, proportionate and non-discriminatory, as well as justified. Given the covert nature of intelligence collection, which is inherently closed, oversight of the various stages of intelligence gathering is a critical safeguard to prevent abuse.

---

[11] See Paul Bischoff, "Data Privacy Laws & Government Surveillance by Country: Which Countries Best Protect Their Citizens?", *Comparitech*, 15 October 2019, *available at* https://www.comparitech.com/blog/vpn-privacy/surveillance-states/.

[12] A/RES/71/199; A/RES/73/179; A/HRC/RES/34/7.

[13] *See*, ECtHR, *Malone v. The United Kingdom*, Application no. 8691/79, 2 August 1984, paras. 66-68.

21. In this context, human rights compliant "interference" must be foreseeable. Specifically, the law must be "foreseeable as to its effects, that is, formulated with sufficient precision to enable the individual to regulate his conduct"[14] and that the individual affected by it "must be able - if need be with appropriate advice - to foresee, to a degree that is reasonable in the circumstances, the consequences which a given action may entail".[15] This requirement does not call for absolute foreseeability but rather that the law give individuals an adequate indication as to the circumstances in which and the conditions on which public authorities are empowered to interfere with their rights.[16] As an essential aspect of legality, the law must also provide sufficient guidance to those charged with its execution to enable them to ascertain when privacy can be restricted and indicate the scope of any discretion conferred on the competent authorities as well as the manner of its exercise.

22. Interference with privacy must be accessible. What is meant by accessibility 'depends to a considerable degree on the content of the instrument in issue, the field it is designed to cover and the number and status of those to whom it is addressed'.[17] In the national security context, the state is able to access, use and disseminate highly sensitive material from all of its citizens and those within jurisdiction. Since individuals are not able to challenge the issue of a warrant authorising surveillance (or know of its existence), accessibility implies that they must be able to become aware of intercept activity at a later. This requirement would, in the Special Rapporteur's view, require *post facto* notification following the cessation of surveillance by the intelligence agencies.

23. Interference with privacy must provide for adequate safeguards against abuse.[18] Restrictions on privacy must have due regard for the principles of necessity, proportionality and non-discrimination.[19] Each of these three principles applies to each interference under consideration by this Court. Any restrictions on privacy must be clearly targeted at protecting a legitimate aim. At the same time, relevant restrictions impacting on the right to privacy cannot be justified merely by a general reference to a protected interest, such as 'national security'[20] a term which

---

[14] See ECtHR, *Kononov v. Latvia* [GC], Application No. 36376/04, 24 July 2008, para. 108.

[15] *See* ECtHR, *Sunday Times v. The United Kingdom (no. 1)*, Application no. 6538/74, 26 April 1979, para. 49. International Covenant on Civil and Political Rights, General Comment 34, para 25.

[16] *Ibidem.*

[17] *See* ECtHR, *Groppera Radio AG and Others v. Switzerland*, Application no. 10890/84, 28 March 1990, para. 68.

[18] ECtHR, *Kruslin v. France*, Application no. 11801/85, 24 April 1990, paras. 33 and 35; ECtHR, *Huvig v. France*, Application no. 11105/84, 24 April 1990, paras. 32 and 34.

[19] *See*, for example, A/HRC/37/52; HRC, General Comment no. 34, CCPR/C/GC/34, para. 26; ECtHR, *Hirst v The United Kingdom* (GC), Application no. 74025/01, 6 October 2005, para. 62ff; *Georgian Labour Party v. Georgia*, no. 9103/04, 8 July 2008, para. 119.

[20] *See*, for example, ECtHR, *Roman Zakharov v. Russia* [GC], Application no. 47143/06, 4 December 2015, para. 26.

is notoriously broad and ambiguous. As a result, the restriction in each case, and in each use, must meet a legitimate aim.[21] In particular, the Special Rapporteur is of the view that, when surveillance is applied against civil society organisations and members of the legal profession, these requirements must be strictly and exactingly applied.

24. The Special Rapporteur also recalls that, in the case of *Weber and Saravia v. Germany*, this Court required the statutory basis for interception of communications to include six basic elements in order to avoid abuses of power: the nature of the offences which may give rise to an interception order, the definition of the categories of people liable to have their communications intercepted, the limit on the duration of the interception, the procedure to be followed for examining, using and storing the data obtained, precautions to be taken when communicating the data to other parties and the circumstances in which recordings may or must be erased or the tapes destroyed.[22]

25. To summarize this section, the Special Rapporteur reflects the Court's conclusion in *Szabó and Vissy v. Hungary*, according to which "[g]iven the particular character of the interference in question and the potential of cutting-edge surveillance technologies to invade citizens' privacy", secret surveillance could be justified "only if it is strictly necessary, as a general consideration, for the safeguarding the democratic institutions and, moreover, if it is strictly necessary, as a particular consideration, for the obtaining of vital intelligence in an individual operation".[23] In this view, these restrictions should be accompanied by a system of checks and oversight, the core elements of which will be developed in the third section (below).

26. The Special Rapporteur observes that while judicial authorization is an important and necessary safeguard in the intelligence gathering context, as confirmed by the best practices identified and endorsed by her mandate,[24] it is not a sufficient safeguard to protect all of the rights negating consequences of secret surveillance. Other essential safeguards, including *post facto* notification and an effective remedy for breaches are at the core of the rights protecting bundles that ought to be in place when intelligence gathering is carried out in a democratic society.[25] The Special Rapporteur stresses that when the targets of surveillance operations include civil society actors and lawyers, the obligations of the Courts to review

---

[21] *See*, for example, A/HRC/37/52; HRC, General Comment no. 34, CCPR/C/GC/34, para. 26; ECtHR, *Hirst v The United Kingdom* (GC), Application no. 74025/01, 6 October 2005, paras. 62 and ff; ECtHR, *Georgian Labour Party v. Georgia*, Application no. 9103/04, 8 July 2008, para. 119.

[22] ECtHR, *Weber and Savaria v. Germany*, Application No. 54934/00, 29 June 2006, para. 95.

[23] ECtHR, *Szabó and Vissy v. Hungary*, Application No. 37138/14, 2016, para. 73.

[24] Practice 6, in A/HRC/14/46.

[25] In Germany, there is a legal requirement to notify affected individuals of the surveillance measures, although that obligation is subject to certain curtailments (such as no obligation to notify if the G10 Commission, one of the oversight bodies, considers that a threat to the purpose of surveillance cannot be ruled out).

and set appropriate standards for state conduct in compliance with their human rights obligations are more compelling.

III. LEGAL POSITION OF THE SPECIAL RAPPORTEUR ON THE SYSTEMS OF PROTECTION OF HUMAN RIGHTS WHILE GATHERING INTELLIGENCE IN A DEMOCRATIC SOCIETY

27. As discussed above, the Special Rapporteur notes that this Court has acknowledged that all regimes for the interception of communications, including both bulk and targeted systems, have the potential to lead to abuses and can have significant and harmful consequences for society as a whole.[26] In this perspective, this Court has identified three stages of intelligence interception in consideration of the requirements of article 8 of the ECHR:[27]

> 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 effected without the individual's knowledge. Consequently, since the individual will necessarily be prevented from seeking an effective remedy of his or her own accord or from taking a direct part in any review proceedings, it is essential that the procedures established should themselves provide adequate and equivalent guarantees safeguarding his or her rights. In addition, the values of a democratic society must be followed as faithfully as possible in the supervisory procedures if the bounds of necessity, within the meaning of article 8 § 2, are not to be exceeded. In a field where *abuse is potentially so easy* in individual cases and could have such harmful consequences for democratic society as a whole, 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 […].[28]

28. Recognising the multiplying role of the intelligence services post 9/11, the first United Nations Special Rapporteur on Counter-Terrorism and Human Rights, Martin Scheinin, identified "best practices" in the oversight of intelligence agencies. Relevantly, states must ensure that intelligence measures that restrict human rights are subject to a legally prescribed process of authorization, as well as ex post oversight and review.[29] The current Special Rapporteur concurs with those best practices' recommendations[30] and argues for their applicability in the

---

[26] ECtHR, *Klass and Others v Germany*, Application No. 5029/71, 6 September 1978, para. 56.

[27] These factors may come into play at three stages: "*when the surveillance is first ordered, while it is being carried out, or after it has been terminated*". ECtHR, Roman Zakharov v. Russia, (GC), Application no. 47143/06, 4 December 2015, para. 233.

[28] ECtHR, *Roman Zakharov v. Russia*, [GC], Application no. 47143/06, 4 December 2015, para. 233, *emphasis added.*

[29] See A/HRC/14/46, practices 6, 7, 21, 22, 28 and 32.

[30] Drawing on *inter alia* Torsten Wetzling and Kilian Vieth, "Upping the Ante on Bulk Surveillance: An International Compendium of Good Legal Safeguards and Oversight Innovations", *Publication Series on Democracy*, (ed) Vol. 50, Heinrich Böll Foundation, November 2018.

case at hand.

29. In addressing the necessity of oversight and notification, the Special Rapporteur brings the best practice 20 to the notice of the Court:

> Any measures by intelligence services that restrict human rights and fundamental freedoms comply with the following criteria: […] (e) There is a clear and comprehensive system for the authorization, monitoring and oversight of the use of any measure that restricts human rights; (f) Individuals whose rights may have been restricted by intelligence services are able to address complaints to an independent institution and seek an effective remedy.

30. There is a substantial need for sustained intelligence oversight and a rights-based approach to the regulation of intelligence services in democratic states. The Special Rapporteur takes the view that while the specific issues in contention before the Court involve *post facto* notification of surveillance and the right to review personal intercept data, these matters involve the broader framework of intelligence oversight in the relevant country, here Poland. There is therefore a substantial need for independent and consistent intelligence oversight and a right-based approach to the regulation of intelligence services in democratic states, including Poland.

31. This need is prompted by the expanding and pervasive role of intelligence gathering and the technological sophistication of intelligence tools. These issues are exacerbated by ever-broadening definitions of 'national security' and 'terrorism'.[31]

32. The Special Rapporteur reaffirms a number of foundational dimensions of effective oversight for the activities, including surveillance and data collection by intelligence agencies. They include a comprehensive legislative framework that defines the mandate of any intelligence agency and clarifies its special powers; the identification of "threshold criteria" that might trigger a range of human rights intrusive actions by an intelligence agency; clear and legally-based boundaries between permissible targeted surveillance and problematic mass surveillance;[32] robust human rights protections on data collection to prevent racial and ethnic profiling; clearly defined mechanisms to identify and review "over-inclusion"; a fully independent and adequately resources review body and remedies for error and post-facto notification of data collection to targets.

33. The most significant form of oversight are independent permanent offices which can comprehensively and effectively review whether intelligence agencies

---

[31] For the challenges of expanding and vague definitions of terrorism and extremism in national law see the legislative reviews undertaken by the Special Rapporteur's mandate found here: https://www.ohchr.org/EN/Issues/Terrorism/Pages/LegislationPolicy.aspx.

[32] See the UNGA's resolution according to which "no one shall be subjected to arbitrary or unlawful interference" with his or her right to privacy and noted that surveillance laws must be "publicly accessible, clear, precise, comprehensive and non-discriminatory". A/C.3/69/L.26/Rev.1.

actually comply with their duties within the law. Not only are competent and independent oversight bodies early warning systems on rule-of-law compliance but they provide a continuity of oversight, a form of permanent rule of law infrastructure on the activities of the entities who generally exercise substantial power of out sight.[33]

34. Fully independent oversight is a 'best practice' and has also been consistently recommended to States in the context of country assessments by the Special Rapporteur:[34]

> Practice 6. Intelligence services are overseen by a combination of internal, executive, parliamentary, judicial and specialized oversight institutions whose mandates and powers are based on publicly available law. An effective system of intelligence oversight includes at least one civilian institution that is independent of both the intelligence services and the executive. The combined remit of oversight institutions covers all aspects of the work of intelligence services, including their compliance with the law; the effectiveness and efficiency of their activities; their finances; and their administrative practices.
>
> Practice 22. Intelligence-collection measures that impose significant limitations on human rights are authorized and overseen by at least one institution that is external to and independent of the intelligence services. This institution has the power to order the revision, suspension or termination of such collection measures. Intelligence collection measures that impose significant limitations on human rights are subject to a multilevel process of authorization that includes approval within intelligence services, by the

[33] Examples of national good practice is evidenced by Australia, the independent Inspector-General of Intelligence and Security (the "IGIS") has extensive oversight powers in respect of the Australian intelligence community. Mandated by a combination of the Intelligence Services Act 2001, and the Inspector General of Intelligence and Security Act 1986, the IGIS fulfils a monitoring and inspection function with a view to identifying issues or concerns before they develop into systemic problems which then require major remedial action. The role of the IGIS is complemented by the Parliamentary Joint Committee on Intelligence and Security, which provides parliamentary oversight of the administration and expenditure of the Australian intelligence community; and Inspector-General of Intelligence and Security provides independent external oversight and review of the New Zealand intelligence and security agencies, with responsibility for examining issues of legality and propriety. Also similar to Australian, the oversight function of the NZ IGIS is complemented by the Parliamentary Intelligence and Security Committee which is a statutory select committee of the New Zealand parliament, which oversees the New Zealand intelligence and security agencies by examining issues relating to their efficacy and efficiency, budgetary matters and policies. The NZ IGIS and the ISC are mandated to perform their oversight functions pursuant to the Inspector-General of Intelligence and Security Act 1996 and the Intelligence and Securities Act 2017.

[34] See namely A/HRC/40/52/Add.4 ; A/HRC/43/46/Add.1 ; /HRC/40/52/Add.5.

political executive and by an institution that is independent of the intelligence services and the executive.

35. The importance of fully independent oversight is a cornerstone of ensuring that intelligence operations are authorized and data is used in compliance with the law. This is particularly important "in view of the fact that the individuals whose rights are affected by intelligence collection are unlikely to be aware of the fact and, thus, have limited opportunity to challenge its legality".[35] The Special Rapporteur's mandate has noted several preferred features for review mechanisms; including capacity to review all relevant and classified materials,[36] call witnesses[37] and inspect the premises of organisations.[38] Sometimes these powers are backed by threat of sanction.[39] In the absence of comprehensive and independent review and remedy the propensity for abuse is higher, and the test of necessity under article 8(2) of the ECHR calls for particular stringency by this Court. The legitimacy of secret surveillance which engages the professional work of lawyers and the activities of civil society actors in a democratic society, call for particular watchfulness and diligence by this Court, in respect of assessing the 'necessity' of such surveillance and the adequacy of the legal framework that supports it.

36. Moreover, the Special Rapporteur holds that *post facto* notification is the most accessible, meaningful, effective and human rights compliant means to ensure that individuals who have been subject to secret surveillance can vindicate their rights, be consistently provided with an adequate remedy, and enables the conditions and institutions commitments that ensure the overall supervision of intelligence agencies is carried out effectively. Relying on a review carried out by European Agency for Fundamental Rights in its reports on state practice of notification in 2015 and 2017,[40] the Special Rapporteur highlights that in six Member States, individuals are notified or information is provided at the end of surveillance, based on the anticipation that the threat to national security will exist throughout the surveillance.[41] In nineteen Member States, the obligation to inform about the

---

[35] A/HRC/14/46, para. 36.
[36] *Ibid.,* para. 14, Practice 7.
[37] Australia- Section 18, *Inspector-General of Intelligence and Security Act* 1986 (Cth) (Aus).
[38] A/HRC/14/46, para 14, Practice 7.
[39] See *inter alia, ibidem,* where the Special Rapporteur's mandate has recognized that mechanisms to incorporate measures to protect classified information.
[39] *Ibid,* paras. 14-15.
[40] European Opinion Agency for Fundamental Rights, "Surveillance by intelligence services: fundamental rights safeguards and remedies in the EU. Mapping member States' legal frameworks", 2015, *available at* http://fra.europa.eu/en/publication/2015/surveillance-intelligence-services; See European Opinion Agency for Fundamental Rights, "Surveillance by intelligence services: fundamental rights safeguards and remedies in the EU, Volume II: field perspectives and legal update", 2017, p.126*, available at* https://fra.europa.eu/sites/default/files/fra_uploads/fra-2017-surveillance-intelligence-services-vol-2_en.pdf.
[41] Bulgaria (Bulgaria, Special Intelligence Means Act, Art. 34 (g) (3); Croatia (Croatia, Act on the Security Intelligence System of the Republic of Croatia, Art. 40 (1); Denmark (Denmark, *Administration of Justice Act*, Art. 788 (1);

surveillance and the right to access the data are provided for in the law, albeit with restrictions.[42]

37. The need for *post facto* notification becomes most acute when one reviews the totality of a supervision and oversight systems and remedial options. Given the scale, intensity and scope of intelligence gathering, this necessity appears consistent with the Court's recent case law in *Zakharov v. Russia*[43] and *Guzel v. Turkey,*[44] which recommended notification as a form of preferred practice.

38. The Special Rapporteur again underscores the ubiquity of surveillance practices by a range of intelligence actors, and the wide net of those subjected to surveillance in many states. The number of civil society actors targeted by in these surveillance activities amplifies this point. Therefore, unless surveillance is subject to independent and thorough judicial authorization, ongoing independent oversight, and a right of review and remedy by affected persons, it will be difficult to prevent its arbitrary deployment.

IV. Intelligence gathering in the context of freedom of expression and Political Participation by Civil Society Actors

39. The Special Rapporteur recalls that freedom of expression is protected by article 19 of the ICCPR and article 10 of the ECHR. Article 10 protects the right to freedom of opinion and expression and under the ICCPR the freedom of opinion is absolute. Freedom of expression is subject to limitation only in accordance with paragraph 2 of article 10. The State has the burden of proof to demonstrate that any restrictions to the right to freedom of expression is compatible with the Convention. All restrictions must pursue a legitimate aim, in accordance with the law that is sufficiently clear, and conform to the requirements of necessity and proportionality and must be necessary in a democratic society.

40. On one hand, the Special Rapporteur notes that surveillance may be a tool of limitation to freedom of expression and needs to be strictly constrained. Abuse of surveillance capacity is particularly concerning when it appears that such practices

---

Germany (Germany, Federal Constitutional Court (Bundesverfassungsgericht), 1 BvR 2226/94, 14 July 1999, paras. 170 and 287; the Netherlands, and Romania (Romania, Law No. 51/1991 concerning the national security of Romania, Art. 21 (2), referred in European Opinion Agency for Fundamental Rights, "Surveillance by intelligence services: fundamental rights safeguards and remedies in the EU. Mapping member States' legal frameworks", 2015, p. 63.

[42] See European Opinion Agency for Fundamental Rights, "Surveillance by intelligence services: fundamental rights safeguards and remedies in the EU, Volume II: field perspectives and legal update", 2017, p.126, *available at* https://fra.europa.eu/sites/default/files/fra_uploads/fra-2017-surveillance-intelligence-services-vol-2_en.pdf.

[43] ECtHR, *Zakharov v Russia,* Application No. 47143/06, 4 December 2015, paras. 286 and ff. We note that the Court drew support from the directive from the Committee of Ministers regulating the use of persona data in the police sector.

[44] ECtHR, Guzel v. Turkey, Application No. 29483/09, 13 September 2016.

are being used against opposition groups, members of civil society, critics of the government, non-governmental organizations and lawyers exercising their professional duties. It bears reminds that the Human Rights Committee has stressed that "the value [on] uninhibited expression is particularly high" regarding public and political issues.[45] Moreover, the UN Declaration on Human Rights Defenders, in its article 6(b) and (c), holds that everyone has the individual and collective right to freely publish, impart or disseminate views, information and knowledge on all human rights and fundamental freedoms.

41. The Special Rapporteur is thus of the view that sustained surveillance used on civil society actors and against their the legitimate activities of political opposition, critics, dissidents, civil society, human rights defenders, lawyers, religious persons, bloggers, artists, musicians and others seems *per se* incompatible with these rights, while in a democratic society and *prima facia* lacking a legitimate purpose.[46]

42. The Special Rapporteur highlights that the considerable chilling effect of such surveillance on the exercise of the freedom of expression, when civil society actors believe or suspect (but have no means to formally challenge) that they are being targeted. "Targeted surveillance creates incentives for self-censorship and directly undermines the ability of journalists and human rights defenders to conduct investigations and build and maintain relationships with sources of information)".[47] The Special Rapporteur attests to the considerable harms experienced by civil society actors and to reality of shrinking civic space in societies where the intelligence services are subject to few constraints. This makes the adequacy of controls on the exercise of surveillance all the more important in democratic states.

43. On the other hand, the Special Rapporteur recalls that "[a]ccording to the Preamble to the Convention, fundamental human rights and freedoms are best maintained by 'an effective political democracy'".[48] Moreover, the Court has made repeated references to "political rights" and similar formulation in the *travaux préparatoires* for the First Protocol as evidence of the importance of these rights in the European system.[49] The Court's deliberations on political participation has addressed *inter alia* voting systems, disqualifications from voting, the application of the Convention to different kinds of electoral processes, as well as the relationship between expression and assembly with political participation. This amicus brief stresses the broader concept of public participation which functions as the *sine qua non* for electoral participation and legitimacy. In this context, the capacity of independent civil society to engage critically on legal and political affairs is an essential dimension of public participation, and its undue *de facto* restrictions weakens and undermines the democratic process as a whole. The chilling effect of surveillance on civil society

[45] HRC, General Comment no. 34, CCPR/C/GC/34.
[46] A/HRC/37/52, para. 47.
[47] A/HRC/38/35/Add.2, para. 53.
[48] ECtHR, Mathieu-Mohin and Clerfayt v. Belgium, Application No. 27120/95, 2 March 1987, para. 47.
[49] *Ibid.,* paras. 22-23.

actors, in the absence of robust and fulsome oversight poses a significant threat to the character and comprehensiveness of public participation in a democratic polity.

44. The general concept of public participation in government affairs is firmly embedded in formal and informal normative foundations, and formally articulated in article 21 of the Universal Declaration of Human Rights ("The will of the people shall be the basis of the authority of government") and the ICCPR ("To take part in the conduct of public affairs, directly or through freely chosen representatives").[50] According to the Office of the High Commissioner of Human Rights, "[p]articipation makes decision-making more informed and sustainable, and public institutions more effective, accountable and transparent. This in turn enhances the legitimacy of States' decisions and their ownership by all members of civil society".[51] The Council of Europe's Committee of Ministers among other bodies has also noted that citizen participation "is at the very heart of the idea of democracy".[52] The protection of civil society is at the heart of the democratic, and undue interference with the function and capacity of civil society to operate, directly or indirectly, is a matter to be closely overseen by this Court. The use of surveillance in the absence of *post facto* notification and fully independent oversight of the intelligence services makes the potential for abuse significant, and the existence of an effective remedy virtually meaningless in practice.

CONCLUSION

45. The Special Rapporteur stresses the need for a multiple-level mechanism to protect human rights in the context of intelligence gathering, in view of the intensification of intelligence gathering, use, storage and exchange. This mechanism includes a judicial order authorizing intelligence gathering, (which is not disputed in these proceedings); an independent oversight mechanism; and post facto notification to the individuals concerned.

46. The Special Rapporteur also raises deep concern when intelligence gathering and surveillance is targeted at civil society actors and legal counsel. She reminds the

---

[50] See generally, Gregory H. Fox, "The Right to Political Participation in International Law", 17 *Yale Journal of International Law* 539, 1992.

[51] Office of the High Commissioner for Human Rights, "Guidelines for States on the Effective Implementation of the Right to Participate in Public Affairs, Summary", 2018, *available at* https://www.ohchr.org/EN/Issues/Pages/DraftGuidelinesRighttoParticipationPublicAffairs.aspx; Council of Europe: Committee of Ministers, "Guidelines for Civil Participation"; Organization for Security and Co-operation in Europe "Recommendations on Enhancing the Participation of Associations in Public Decision-making Processes", 2015, *available at* https://www.osce.org/odihr/183991 .

[52] Council of Europe: Committee of Ministers, "Guidelines for civil participation in political decision making", CM (2017)83-final, 27 September 2017.

Court of the absolute necessity to guarantee robust checks and oversight of intelligence agencies in such contexts.
