IN THE EUROPEAN COURT OF HUMAN RIGHTS

Application nos. 72038/17 and 25237/18

BETWEEN:

Pietrzak

and

Bychawska-Siniarska

Applicants

and

Poland

Respondent

WRITTEN SUBMISSIONS ON BEHALF OF THE INTERNATIONAL COMMISSION OF JURISTS

1. Introduction

In this submission, the ICJ will address (1) the application of the principles of prescription by law, necessity and proportionality, in circumstances when mass and targeted surveillance interferes with the right to respect for private life under Article 8 ECHR, in particular when it affects lawyers and human rights defenders; (2) the obligations of States under Article 8 and 6 ECHR to ensure respect for the confidentiality of lawyer-client relations and the principle of legal professional privilege. It will be argued that secret surveillance, in particular where it interferes with the confidentiality of communications of lawyers and human rights defenders, and endangers lawyer-client privilege protected under Articles 8 and 6 ECHR, should be subject to specific safeguards and to particularly strict scrutiny of its necessity and proportionality.

2. Article 8 ECHR and mass and targeted surveillance

As this Court has acknowledged in its jurisprudence, all regimes for the interception of communications – including bulk and targeted systems – have the potential to be abused,[1] and therefore to lead to violations of the right to respect for private life. In the intervener's submission, the high risk of abuse of mass surveillance should inform the assessment, under Article 8(2) ECHR, of whether the interference with Article 8 rights occasioned by the surveillance has an adequate legal basis, is necessary in a democratic society to achieve a legitimate aim and is proportionate to the aim pursued. When the potential interference with Article 8 rights that is contested is secret surveillance, the lawfulness of the interference is closely related to the question whether the "necessity" test has been complied with.[2] In conducting such an assessment, special attention should be paid to the quality of the law and to the existence of safeguards against abuse, as well as to their adequacy and effectiveness.

2.1. Existence of a legal basis and quality of the law

For law to be of sufficient quality to meet the requirements of Article 8.2, "*it should be accessible to the person concerned, who must, moreover, be able to foresee its consequences for him, and compatible with the rule of law*".[3] With respect to this, the grounds upon which a warrant for surveillance may be issued must be sufficiently clear, and domestic law must give individuals an adequate indication of the circumstances in which their communications might be intercepted and selected for examination.[4]

The requirement of accessibility warrants that the nature of the offences or the grounds that might give rise to an interception order must be stated in a simple, clear and understandable manner, and must be officially published and accessible to the public. This Court has found that this requirement was not fulfilled when the domestic law "did not set out in a form accessible to the public

[1] ECtHR, *Klass and Others v Germany*, (5029/71, 1978) para.56
[2] ECtHR, *Big Brother Watch and Others v. UK* (58170/13 62322/14 24960/15, 2018),para.322.
[3] ECtHR, *Weber and Saravia v. Germany* (54934/00, 2006), para. 84; See also ECtHR, *Kruslin v. France*, (11801/85, 1990), para. 27; ECtHR, *Huvig v. France*, (11105/84, 1990), para. 26; ECtHR, *Perry v. UK,* (63737/00, 2003), para. 45.
[4] ECtHR, *Big Brother Watch and Others v. UK* op cit para. 330.

any indication of the procedure to be followed for selecting for examination, sharing, storing and destroying intercepted material."[5]

International human rights expert bodies have also emphasized the importance of accessibility of the law in the context of mass surveillance.[6] The United Nations High Commissioner for Human Rights, in a report on the right to privacy in the digital age, stated that:

> *"Secret rules and secret interpretations – even secret judicial interpretations – of law do not have the necessary qualities of "law". Neither do laws or rules that give the executive authorities, such as security and intelligence services, excessive discretion. The secret nature of specific surveillance powers brings with it a greater risk of arbitrary exercise of discretion which, in turn, demands greater precision in the rule governing the exercise of discretion, and additional oversight. … Vague and overbroad justifications, such as unspecific references to "national security" do not qualify as adequately clear laws. Surveillance must be based on reasonable suspicion and any decision authorizing such surveillance must be sufficiently targeted. The law must strictly assign the competences to conduct surveillance and access the product of surveillance to specified authorities*".[7]

With regard to the requirement of foreseeability, this Court has ruled that, especially when executive power may be exercised in secret, it is "essential to have clear, detailed rules on interception of telephone conversations, especially as the technology available for use is continually becoming more sophisticated".[8] This Court has also held that, "the law must indicate the scope of any such discretion conferred to the competent authorities and the manner of its exercise with sufficient clarity to give the individual adequate protection against arbitrary interference".[9]

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.[10] In *Roman Zakharov,* the Court applied these requirements to interception ordered on grounds of national security.[11]

---

[5] ECtHR, *Liberty and Others v. UK*, (58243/00, 2008), para. 69.
[6] See, among others, Office of the Special Rapporteur for Freedom of Expression of the Inter-American Commission on Human Right Freedom of Expression and the Internet (31 December 2013), para. 153.
[7] Report of the Office of the United Nations High Commissioner for Human Rights, The Right to Privacy in the Digital Age, U.N. Doc. A/HRC/27/37, 30 June 2014, paras. 29 and 35.
[8] ECtHR, *Weber and Saravia v. Germany*, op cit, para. 93.
[9] Ibid, para. 94. See ECtHR, *Roman Zakharov v. Russia* (47143/06, 2015), para. 229; ECtHR, *Malone v. The United Kingdom,* (8691/79, 1985), para. 67; ECtHR, *Leander v. Sweden*, (9248/81, 1987), para. 51; ECtHR, *Huvig v. France*, (11105/84, 1990), para. 29; ECtHR, *Rotaru v. Romania*, (28341/95, 2000), para. 55; ECtHR, *Weber and Saravia v. Germany,* op cit, para. 93.
[10] ECtHR, *Weber and Saravia v. Germany*, op cit, para. 95.
[11] ECtHR, Roman Zakharov v. Russia op cit, para.231.

The **legal basis** should refer in a clear manner to the nature of offences that could give rise to an interception order, the scope of its application, as well as the categories of people that might be considered liable to have their communications monitored.[12] In *Klass and Others v. Germany*, this Court clarified that:

> *"A series of limitative conditions have to be satisfied before a surveillance measure can be imposed. Thus, the permissible restrictive measures are confined to cases in which there are factual indications for suspecting a person of planning, committing or having committed certain serious criminal acts; measures may only be ordered if the establishment of the facts by another method is without prospects of success or considerably more difficult; even then, the surveillance may cover only the specific suspect or his presumed "contact-persons". Consequently, so-called exploratory or general surveillance is not permitted by the contested legislation*".[13]

The **duration** of secret surveillance measures should be indicated clearly and mechanisms should be foreseen that ensure that warrants permitting such measures are kept under continuous review.[14] Whenever the initial period of surveillance may be renewed, a limit should be also established so that sufficient guarantees exist, and surveillance is not routinely renewed for an indefinite period.[15]

Domestic law should contain rules governing the storage, use, destruction and communication of intercepted data, so that the risk of unauthorized access or disclosure is reduced. In *Roman Zakharov v. Russia*, the Court deplored the lack of a requirement to destroy immediately any data that was not relevant to the purpose for which it was obtained. The Court concluded that the automatic storage for six months of clearly irrelevant data could not be considered justified under Article 8.[16]

Other additional relevant factors should also be evaluated, such as arrangements for supervising the implementation of the surveillance, notification mechanisms and remedies provided by national law.[17] 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*".[18]

With regard to the first two stages of authorization and unfolding of the surveillance operation, the Court reiterated that*, "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".*[19] The Court also observed that, in this this context, supervisory judicial control offers the best guarantees of

[12] ECtHR, *Malone v. UK*, op cit, para. 70; ECtHR, *Roman Zakharov v. Russia*, op cit, para. 243.
[13] ECtHR, *Klass and Others v. Germany*, op cit, para. 51.
[14] ECtHR, *Big Brother Watch and Others v. UK*, op cit para. 360.
[15] ECtHR, *Roman Zakharov v. Russia*, op cit, paras. 251 - 252.
[16] Ibid., paras. 255-256
[17] Ibid para. 238.
[18] Ibid para. 233.
[19] Ibid., para. 233.

independence, impartiality and a proper procedure.[20] In this connection, judicial scrutiny should not be limited in scope and the judicial body must have access to information about the organization and tactics of operational search. Court authorizations cannot be too broad or fail to mention the duration for which the interception was authorized and give a very wide discretion to the law-enforcement authorities.[21]

In relation to the third stage – after the surveillance has been terminated – the Court has affirmed the essential role of the notification of the surveillance activity.[22] In the absence of a notification procedure, the Court has considered that there is little scope for effective recourse to the courts.[23] This point has also been stressed by the UN High Commissioner for Human Rights[24] and the Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms while countering terrorism.[25]

The need for effective scrutiny has in particular been highlighted by the UN High Commissioner for Human Rights who has recommended that surveillance measures should be *"authorized, reviewed and supervised by independent bodies at all stages, including when they are first ordered, while they are being carried out and after they have been terminated"*.[26] The High Commissioner further emphasized that:

> *"Oversight bodies should be independent of the authorities carrying out the surveillance and equipped with appropriate and adequate expertise, competencies and resources. Authorization and oversight should be institutionally separated. Independent oversight bodies should proactively investigate and monitor the activities of those who conduct surveillance and have access to the products of surveillance and carry out periodic reviews of surveillance capabilities and technological developments. The agencies carrying out surveillance should be required to provide all the information necessary for effective oversight upon request and regularly report to the oversight bodies, and they should be required to keep records of all surveillance measures taken. Oversight processes must also be transparent and subject to appropriate public scrutiny and the decisions of the oversight bodies must be subject to appeal or independent review"*.[27]

2.2. Necessity and proportionality

In cases of secret surveillance, this Court clarified in *Szabó and Vissy v. Hungary*, that "[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,*

[20] Ibid., para. 233.
[21] Ibid., paras. 265,- 267
[22] Ibid., para. 234.
[23] Ibid., paras. 298-300.
[24] Report of the United Nations High Commissioner for Human Rights on the right to privacy in the digital age, U.N. Doc. A/HRC/39/29 (3 August 2018), para. 41.
[25] Report of the Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms While Countering Terrorism, U.N. Doc. A/69/397 (23 September 2014), para. 46.
[26] Report of the United Nations High Commissioner for Human Rights on the right to privacy in the digital age, U.N. Doc. A/HRC/39/29 (3 August 2018), para. 39.
[27] Ibid, para. 40.

moreover, if it is strictly necessary, as a particular consideration, for the obtaining of vital intelligence in an individual operation."[28]

In the submission of the intervener, due to the scale of intrusion on privacy that mass surveillance entails, when intelligence services systematically collect communications data on a massive scale and retain it for future search and use, such measures entail a high risk of disproportionality. In *Mustafa Sezgin Tanrıkulu v. Turkey*, for example, this Court found a violation of Article 8 because the National Intelligence Agency had permission to intercept all domestic and international communications for a month and a half with a view to identifying suspected acts of terrorism.[29]

The Court of Justice of the EU (CJEU) considered in its Schrems decision of 2014, that the strict "necessity and proportionality" assessment could not be satisfied where legislation authorized "*on a generalized basis, storage of all the personal data of all the persons whose data has been transferred […], without any differentiation, limitation or exception being made in the light of the objective pursued and without an objective criterion being laid down by which to determine the limits of the access of the public authorities to the data, and of its subsequent use".*[30] In its 2020 Schrems decision, the CJEU further found that where there was bulk collection of "*a relatively large volume of signals intelligence information or data under circumstances where the Intelligence Community cannot use an identifier associated with a specific target … which allows, in the context of the surveillance programmes …., access to data in transit to the United States without that access being subject to any judicial review, does not, in any event, delimit in a sufficiently clear and precise manner the scope of such bulk collection of personal data*."[31] Therefore, the interference with privacy rights through the surveillance programme in issue could not be considered to be proportionate or limited to what was strictly necessary.[32]

Where surveillance affects human rights defenders and lawyers, these considerations should be applied with particular regard to their role, including the specific regime governing the protection of lawyer-client communications, (see below Section 3) and the public watchdog role played by civil society organizations involved in matters of public interest, which warrants particular protection.[33]

The interveners therefore submit that the nature of mass surveillance entails particularly high risks of disproportionate interference with Article 8 rights, in particular in the absence of strong judicial safeguards, and that the necessity and proportionality of the intrusion into privacy rights of human rights defenders and of lawyers requires particularly strict scrutiny, in light of the important role these actors play in the defence of human rights.

---

[28] ECtHR, *Szabó and Vissy v. Hungary* (37138/14, 2016), para. 73.
[29] ECtHR, *Mustafa Sezgin Tanrıkulu v. Turkey* (27473/06, 2017), para. 64.
[30] CJEU, *Digital Rights Ireland v. Minister of Communications & Others*, cases C-293/12 and C-594/12, 8 April 2014, paras. 54-55.
[31] Data Protection Commissioner v Facebook Ireland and Maximilian Schrems, Case C-311/18, 16 July 2020, Para.183
[32] Ibid, Para.184
[33] ECtHR, *Gusova v Bulgaria*, (6987/07, 2015), para. 38.

3. The confidentiality of lawyer-client relations and the principle of legal professional privilege

3.1 International law and standards concerning lawyer-client confidentiality

The principle of confidentiality of communications between lawyers and their clients is well established in international human rights law as an element of both the right to a fair trial[34] and of rights to respect for private and family life, the home[35] and correspondence.[36] It is also acknowledged as being an "indispensible feature of the rule of law" that is "essential to public trust and confidence in the administration of justice and the independence of the legal system".[37]

Considering the right to respect for private life, in *Michaud v. France*, the Court held that "*Article 8 … affords strengthened protection to exchanges between lawyers and their clients. This is justified by the fact that lawyers are assigned a fundamental role in a democratic society, that of defending litigants. Yet lawyers cannot carry out this essential task if they are unable to guarantee to those they are defending that their exchanges will remain confidential"*.[38] In *R.E. v. United Kingdom*, the Court considered *"that the surveillance of a legal consultation constitutes an extremely high degree of intrusion into a person's right to respect for his or her private life and correspondence"*.[39] Heightened protection of the privacy of lawyer-client communications has similarly been applied by the Inter-American Court of Human Rights which affirmed in the *Tristán Donoso v. Panamá* case that since the conversation at stake "*was held between the alleged victim [a lawyer] and one of his clients, it should even be afforded a greater degree of protection on account of professional secrecy*".[40]

In *S. v. Switzerland*, this Court affirmed that the right to communicate with a lawyer in private is also "part of the basic requirement of a fair trial in a democratic society", under Article 6.3.c.[41] This was reaffirmed in *Michaud v. France*, where this Court held that "*[i]t is the relationship of trust between [a lawyer and client], essential to the accomplishment of that mission, that is at stake. Indirectly but necessarily dependent thereupon is the right of everyone to a fair trial, including the right of accused persons not to incriminate themselves*".[42] The UN Human Rights Committee, in interpreting the right to a fair trial under article 14 ICCPR, has stated that "counsel should be able to meet

[34] UN Human Rights Committee, General Comment No. 32, op cit, para. 34; UN Human Rights Committee, *Gridin v. Russian Federation*, UN Doc. CCPR/69/D/770/1997, Views of 20 July 2000, para. 8.5; ECtHR, *S. v. Switzerland,* (12629/87 and 13965/88, 1991), para. 48

[35] ECtHR, *Iordachi and Others v. Moldova*, (25198/02, 2009), para. 34

[36] ECtHR, *Niemietz v. Germany*, (13710/88, 1992), paras. 29 to 32; ECtHR, *Wieser and Bicos Beteiligungen GmbH v. Austria*, (74336/01, 2007), paras. 43 to 45.

[37] Commentary on IBA International Principles on Conduct for the Legal Profession, para. 4.2; See also Code of Conduct for European Lawyers, para. 2.3.1; Parliamentary Assembly of the Council of Europe (PACE), Resolution on Mass Surveillance 2045, 21 April 2015, para. 4.

[38] ECtHR, *Michaud v. France* (12323/11, 2012), para. 118.

[39] ECtHR, *R.E. v. United Kingdom* (62498/11, 2015), para. 131.

[40] IACtHR, *Tristán Donoso v. Panamá, Judgment (on Preliminary Objection, Merits, Reparations, and Costs*), Series C No. 193 (27 January 2009), para. 75.

[41] ECtHR, *S. v. Switzerland* op cit, para. 48, 117-118. See also, ECtHR, *Niemietz v. Germany* op cit, para. 37; ECtHR, *Domenichini v. Italy* (15943/90, 1996), para. 39; ECtHR, *Öcalan v. Turkey* (46221/99, 2005), para. 1333; ECtHR, *Moiseyev v. Russia* (62936/00, 2008), para. 209; ECtHR, *Campbell v. the United Kingdom* (13590/88, 1992), paras 44-48.

[42] *Michaud v France*, (12323/11, 2012) para.118

their clients in private and to communicate with the accused in conditions that fully respect the confidentiality of their communications."[43]

The importance of lawyer-client confidentiality is affirmed in both global and regional standards on the role of lawyers. The UN Basic Principles on the Role of Lawyers affirm that "Governments shall recognize and respect that all communications and consultations between lawyers and their clients within their professional relationship are confidential."[44] Recommendation No. R(2000)21 of the Committee of Ministers to Member States on the freedom of exercise the profession of a lawyer, likewise affirms that "[l]awyers should have access to their clients, including in particular to persons deprived of their liberty, to enable them to counsel in private and to represent their clients according to established professional standards [and that all] necessary measures should be taken to ensure the respect of the confidentiality of the lawyer-client relationship. Exceptions to this principle should be allowed only if compatible with the Rule of Law."[45] The Standards for the Independence of the Legal Profession of the International Bar Association (IBA) hold that States should respect the "confidentiality of the lawyer-client relationship, including protection of the lawyer's files and documents from seizure or inspection and protection from interception of the lawyer's electronic communications".[46]

Reflecting international human rights law, the Court of Justice of the European Union has acknowledged that lawyer-client confidentiality constitutes a general principle of law common to the laws of all Member States and, as such, a fundamental right protected by EU law.[47] The Court has held that "*any person must be able, without constraint, to consult a lawyer whose profession entails the giving of independent legal advice to all those in need of it*".[48] Moreover, in general terms, States' obligation to protect lawyer-client confidentiality has been explicitly recognized in article 4 of the European Union Directive on the Right of Access to a Lawyer (Directive 2013/48/EU) which provides that "*Member States shall respect the confidentiality of communication between suspects or accused persons and their lawyer in the exercise of the right of access to a lawyer provided for under this Directive. Such communication shall include meetings, correspondence, telephone conversations and other forms of communication permitted under national law*".[49] The European Parliament has also recognized the importance of lawyer-client confidentiality, recalling in a Resolution regarding the US NSA surveillance programme that "*any uncertainty about the confidentiality of communications between lawyers and their clients could negatively impact on EU citizens' right of access to legal advice and access to justice and the right to a fair trial"*.[50]

---

[43] UN Human Rights Committee, General Comment no. 32 on the Right to a Fair Trial, CCPR/C/GC/32, para.34
[44] Principle 22.
[45] Recommendation No. R(2000)21 of the Committee of Ministers to members stated on the freedom of exercise of the profession of a lawyer, 25 October 2000, paras 5 and 6.
[46] IBA Standards on the Independence of the Legal Profession (Adopted 1990), Standard 13
[47]CJEU, *AM & S v Commission* case (155/79, 1982), paras. 16 and 18.
[48] Ibid.
[49] Directive 2013/48/EU of the European Parliament and of the Council of 22 October 2013 on the right of access to a lawyer in criminal proceedings and in European arrest warrant proceedings, and on the right to have a third party informed upon deprivation of liberty and to communicate with third persons and with consular authorities while deprived of liberty.
[50] European Parliament, Resolution on the US NSA surveillance programme, surveillance bodies in various Member States and their impact on EU citizens' fundamental rights and on transatlantic cooperation in Justice and Home Affairs, 12 March 2014, para. 11.

3.2 Safeguards for lawyer-client confidentiality

Although exceptions to the confidentiality of lawyer-client communications may, in certain circumstances, be permitted, this is the case only on condition that adequate safeguards against abuse are in place.[51] This Court has highlighted the need for effective procedural safeguards when communications that might encompass lawyer-client material are intercepted.[52] In *Foxley v. UK*, it was held that these must "*ensure minimum impairment of the right to respect for his correspondence [and] that the lawyer-client relationship is, in principle, privileged and correspondence in that context, whatever its purpose, concerns matters of a private and confidential nature*".[53] In *Kopp v. Switzerland*, the need was further underlined for "*supervision by an independent judge, especially in this sensitive area of the confidential relations between a lawyer and his clients, which directly concern the rights of the defense*".[54]

States must comply with adequate guarantees to ensure that the confidentiality of lawyer-client relations and the principle of legal professional privilege are protected against arbitrary mass surveillance. Indeed, this Court ruled in *Kopp v. Switzerland* that a *"law [that] does not clearly state how, under what conditions and by whom the distinction is to be drawn between matters specifically connected with a lawyer's work under instructions from a party to proceedings and those relating to activity other than that of counsel"*[55] is insufficient to protect lawyer-client confidentiality.[56] In *Iordachi and Others v. Moldova*, it found a violation of Article 8, because, although the Moldovan legislation guaranteed the secrecy of lawyer-client communications, it did not provide for any procedure which would give substance to that provision.[57] Furthermore, the Court stated it was "*struck by the absence of clear rules defining what should happen when, for example, a phone call made by a client to his lawyer is intercepted.*"[58]

The same logic was applied in the case of *Sommer v. Germany*, which dealt with protection of the professional confidentiality of lawyers. The Court stated that: "I*n the context of covert intelligence-gathering, it is essential to have clear, detailed rules governing the scope and application of measures, as well as minimum safeguards concerning, inter alia, duration, storage, usage, access of third parties, procedures for preserving the integrity and confidentiality of data and procedures for its destruction, thus providing sufficient guarantees against the risk of abuse and arbitrariness*".[59]

Furthermore, the Court considered that the suspected involvement of a lawyer in a crime as a justification for surveillance operations cannot be merely vague and unspecific.[60]

---

[51] ECtHR, *Erdem v Germany*, (38321/97, 2001), paras. 65 to 69
[52] ECtHR, *Niemietz v. Germany* op cit, para. 37; ECtHR, *Matheron v. France* (57752/00, 2005), paras. 36-43; ECtHR, *Pruteanu v Romania* (30181/05, 2015), para. 49.
[53] ECtHR, *Foxley v. UK* (33274/96, 2000), para. 43
[54] ECtHR, *Kopp v. Switzerland* (23224/94, 1998), para. 74.
[55] Ibid, para. 73.
[56] Ibid, para. 75.
[57] ECtHR, *Iordachi and Others v. Moldova*, op cit, para. 50.
[58] Ibid, para. 50.
[59] ECtHR, *Sommer v. Germany*, (73607/13, 2017), para. 53.
[60] Ibid, para. 61.

The importance of procedural safeguards to protect confidentiality of lawyer-client and similar professional ocmmuicatins has been also emphasized by the Council of Europe Venice Commission, which declared that "*methods must be devised to provide lawyers and other privileged communicants and journalists with some form of protection, such as requiring a high, or very high, threshold before approving signals intelligence operations against them, combined with procedural safeguards and strong external oversight*".[61]

As regards the particular concerns relating to confidentiality of the communications of human rights defenders, it is of relevance that this Court has clarified that when an NGO is involved in matters of public interest, it is exercising a role as a public watchdog of similar importance to that of the press and warrants similar protections to those afforded to the press.[62] This enhanced protection for civil society working on matters of public interest is reflected in the standards set out in the UN Declaration on the Right and Responsibility of Individuals, Groups and Organs of Society to Promote and Protect Universally Recognized Human Rights and Fundamental Freedoms. It affirms the right to promote and strive for the protection and realization of human rights (article 1), and rights to provide advice and assistance on human rights: Article 9.3.c states that everyone has the right "to offer and provide professionally qualified legal assistance or other relevant advice and assistance in defending human rights and fundamental freedoms", while Article 9.4 recognizes the right to "unhindered access to and communication with international bodies with general or special competence to receive and consider communications on matters of human rights and fundamental freedoms". These rights also imply the need for confidentiality of such assistance, advice and communications, in order to ensure their effectiveness.

In light of the above, the interveners submit that the need to ensure effective and confidential communication in the representation of victims of human rights violations before national or international courts should apply not only to registered members of the bar association, but also to civil society representatives who provide advice and assistance on human rights law and assist individuals in accessing remedies for violations of human rights before national and international courts and mechanisms. The interveners submit that safeguards for the confidentiality of communications in regard to such advice and assistance are essential to its effectiveness.

In light of this Court's jurisprudence and other applicable international standards and jurisprudence, the ICJ submits that it is clearly established that the surveillance of lawyer's communications jeopardizes the right to a fair trial under Article 6 ECHR as well as the right to respect for private life, the home and correspondence under Article 8 ECHR.

On the basis of the same rationale, the ICJ further contends that human rights defenders who represent clients before national and international courts or other human rights bodies also warrant a comparable level of protection of their communications from surveillance. **The ICJ therefore submits that, in order**

[61] 2015 Update of the Council of Europe Venice Commission Report on the 'Democratic Oversight of the Security Services and Report on the Democratic Oversight of Signals Intelligence Services", para. 18.
[62] ECtHR, *Gusova v Bulgaria*, (6987/07, 2015), para. 38.

to effectively preserve the right to privacy and the right to a fair trial, States have the obligation to establish effective safeguards against intrusion through mass surveillance on the confidentiality of communications of lawyers and human rights defenders related to their representation of their clients.

In order to respect this principle, surveillance of these categories of professionals may be permitted only in very exceptional circumstances, and must be subject to the highest level of safeguards for the authorization and conduct of surveillance, including judicial authorization and post-surveillance, notification and remedies.