CONFERENCE OF INGOs
OF THE COUNCIL OF EUROPE

CONFERENCE DES OING DU
CONSEIL DE L'EUROPE

Recommendation CONF/PLE(2017)REC1 adopted by the Conference of INGOs on 27 January 2017

"Surveillance of lawyers: the need for standards safeguarding client confidentiality"

The Conference of International Non-Governmental Organisations (INGOs) of the Council of Europe:

Considering the concerns expressed by various international governmental and non-governmental organisations[1] in relation to state bodies having secret and/or insufficiently controlled investigatory powers, as well as their using highly sophisticated and far-reaching interception and tracking technologies to access communication data belonging to citizens in an indiscriminate, large-scale and non-suspicion-based manner.

Stressing that although certain interception and tracking technologies may sometimes be useful in the fight against terrorism and organised crime, they also create a number of problems, notably concerning the compatibility of the interference with the principles of professional secrecy and legal professional privilege[2].

Considering that 'government' surveillance activities may involve the national government itself, government at different levels (federal, state, or local), governmental agencies, tax authorities, independent agencies carrying out public law functions, the police, prosecutors, intelligence services, and others.

Emphasising that mass surveillance severely undermines the rights of persons seeking legal advice and representation to have their communications with their lawyers to be kept confidential and the obligations upon lawyers to maintain such confidentiality, such rights and obligations of professional confidentiality being critical elements of broader fundamental rights, including the

[1] For example, reference is made to the reports set out in footnotes 9-13 of the Parliamentary Assembly of the Council of Europe, the Council of Europe Venice Commission, the Council of Europe Commissioner for Human Rights, and the European Parliament. Furthermore, ten non-governmental human rights organisations brought a legal challenge (launched in April 2015) against the United Kingdom in the European Court of Human Rights over mass surveillance.

[2] All European countries have provisions in order to ensure the protection of the right and duty of the lawyer to keep clients' matters confidential. In some jurisdictions in Europe, that is achieved by attaching to those communications the protection of **legal professional privilege**, and in other jurisdictions by treating them as **professional secrets**. Both approaches, however, seek to achieve the same end: the protection of information generated within the lawyer-client relationship for the purpose of giving or receiving legal advice (in both contentious and non-contentious matters) and/or representation in any type of legal proceedings, whether civil or criminal in nature. For more background information, see Council of Bars and Law Societies of Europe, Recommendations on the protection of client confidentiality within the context of surveillance activities, 28 April 2016, pages 9-10.

rights to a fair trial (article 6 ECHR), to privacy (article 8 ECHR), to freedom of information and to expression (article 10 ECHR).

Further emphasising that these rights are the cornerstones of democracy, and their infringement also jeopardises the rule of law.

Highlighting that targeted government surveillance activities must be strictly regulated and supervised by independent judicial authorities and comply with the principles of legality, need and proportionality.[3]

Considering that the confidentiality of lawyer-client communications[4] is seen not only as the lawyer's duty, but as a fundamental human right of the client, and that without the certainty of confidentiality there cannot be trust, which is key to the proper functioning of the administration of justice and the rule of law.

Emphasising that the lawyer's obligation of confidentiality serves the interest of administration of justice as well as the interest of the client, and that it is therefore entitled to special protection by the State.

Underlining that the confidentiality of communications between clients and lawyers is protected both under the European Convention on Human Rights and the law of the European Union, and is given high importance by the European Court of Human Rights[5], the Court of Justice of the European Union[6], and other relevant European bodies.

---

[3] See 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'.

[4] For the purpose of this recommendation, the term 'lawyer-client communications' refers to any communications with or between lawyers in the course of their professional activities, including any data covered by professional secrecy or legal professional privilege.

[5] For example, in the following cases: *S. v. Switzerland* (12629/87, 1991) (*"(…) If a lawyer were unable to confer with his client and receive confidential instructions from him without such surveillance, his assistance would lose much of its usefulness, whereas the Convention is intended to guarantee rights that are practical and effective (…)."*); *Pruteanu v Romania* (30181/05, 2015) ("*The interception of conversations between a lawyer and his client unquestionably undermines professional secrecy, which is the basis of the relationship of trust between them"* [unofficial translation]); *Niemietz v. Germany* (13710/88, 1992) (*"(…) it has, in this connection, to be recalled that, where a lawyer is involved, an encroachment on professional secrecy may have repercussions on the proper administration of justice and hence on the rights guaranteed by Article 6 of the Convention. (…)"*); *Kopp v. Switzerland* (23224/94, 1998) (*"Above all, in practice, it is, to say the least, astonishing that this task should be assigned to an official of the Post Office's legal department, who is a member of the executive, without 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 defence*."). More specifically, the Court has ruled on the compatibility with article 8 of searches and seizures carried out at a lawyer's offices or home *(see Niemietz v. Germany ; Roemen and Schmit v. Luxembourg, no. 51772/99; Sallinen and Others v. Finland, no. 50882/99, 27 September 2005; André and Another v. France, 24 July 2008 ; Xavier Da Silveira v. France, 21 January 2010),* search and seizure of electronic data in a law firm (*see Sallinen and Others, Wieser and Bicos Beteiligungen GmbH v. Austria, 16 October 2007,* and *Robathin v. Austria, no. 30457/06, 3 July 2012),* interception of correspondence between a lawyer and his client *(see Schönenberger and Durmaz v. Switzerland, 20 June 1988, Series A no. 137),* tapping of a lawyer's telephone (see *Kopp v. Switzerland*, 25 March 1998), obligation for lawyers to report their "suspicions" regarding money laundering activities of their clients *(Michaud v. France)*, search and seizure of correspondence between lawyers and their clients in companies' premises by national competition authorities (*Vinci Construction and GMT genie civil and services v. France,* no. 63629/10 and 60567/10, 2 April 2015*)* and access to a bank account of a lawyer *(Brito Ferrinho Bexiga Villa-Nova v. Portugal, no. 69436/10, 1 December 2015).*

[6] In the *AM & S v Commission* case (155/79, 1982), the CJEU acknowledged that the maintenance of confidentiality as regards certain communications between lawyer and client constitutes a general principle of law common to the laws of all Member States and, as such, a fundamental right protected by EU law. The Court 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"*, and that, therefore, the confidentiality of certain lawyer-client communications must be

Referring in particular to the *Michaud* case[7], which states that *"while Article 8 [of the ECHR] protects the confidentiality of all "correspondence" between individuals, it 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. […] Indirectly but necessarily dependent thereupon is the right of everyone to a fair trial, including the right of accused persons not to incriminate themselves."*

Recalling that the Recommendation of the Council of Europe adopted on 25 October 2000[8] states that "*all measures should be taken to ensure the respect of confidentiality of the lawyer-client relationship"*, and that *"exceptions to this principle should be allowed only if compatible with the Rule of Law*."

Recalling that Resolution 2045 of 21 April 2015[9] of the Council of Europe Parliamentary Assembly states that *"surveillance practices disclosed so far endanger fundamental human rights*", especially *"when confidential communications with lawyers"* are intercepted.

Recalling that the 2015 Update[10] 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' states that lawyers are *"privileged communicants"* requiring a very high protection.

Recalling that the 2015 Issue Paper[11] by the Council of Europe Commissioner for Human Rights on 'Democratic and effective oversight of national security services' states that *"the interception of communications between lawyers and their clients […] can undermine the equality of arms and the right to a fair trial especially where security services are party to the litigation concerned"*.

Recalling that the European Parliament resolution[12] of 12 March 2014 on surveillance stresses 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"*.[13]

---

protected. See also CJEU, Conclusions of the Advocate General Léger, *J.C.J. Wouters, J.W. Savelbergh, Price Waterhouse Belastingadviseurs BV v. Algemene Raad van de Nederlandse Orde van Advocaten,* in Case C-309/99, 10 July 2001, §182, and CJEU Conclusions of the Advocate General Poiares Maduro *Ordre des barreaux francophones et germanophone and Others v Conseil des ministres,* in Case C-305/05, §42-44, 14 December 2006.

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

[8] Council of Europe, Recommendation No R(2000)21 of the Committee of Ministers to members states on the freedom of exercise of the profession of lawyer, 25 October 2000, §6.

[9] Council of Europe Parliamentary Assembly, Resolution 2045, 21 April 2015, §4.

[10] 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, §18.

[11] Council of Europe Commissioner for Human Rights, Issue Paper on 'Democratic and effective oversight of national security services', 2015, p. 27.

[12] 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, §11.

[13] Also see: European Parliament, Resolution on the 'follow-up to the European Parliament resolution of 12 March 2014 on the electronic mass surveillance of EU citizens' which stated that "*mass surveillance severely undermines the rights of EU citizens to be protected against any surveillance of confidential communications with their lawyers"*, 29 October 2015, §43.

Considering the Recommendations[14] adopted by the Council of Bars and Law Societies of Europe on the protection of client confidentiality within the context of surveillance activities.

Noting the calls which have been made by various organisations[15] for a global digital rights charter and a digital habeas corpus, which should also provide additional protection to lawyer-client communications.

Stressing the need for standards, the Conference of INGOs of the Council of Europe:

1. **urges** the Committee of Ministers of the Council of Europe to adopt and implement the recommendations listed below, so as to ensure that the principles of professional secrecy and legal professional privilege are not undermined by practices undertaken by the state involving the interception for the purpose of surveillance of communications between lawyers and clients and other data protected by legal professional privilege or obligations of professional secrecy:

   a) Any direct or indirect surveillance undertaken by the State should fall within the bounds of the rule of law, respecting the principle that all data and communications protected by legal professional privilege and by obligations of professional secrecy are inviolable and not amenable to interception or surveillance.
   b) All surveillance activities require to be regulated with adequate specificity through primary legislation providing for explicit protection of lawyer-client communications. Also in the case for the outsourcing of surveillance activities to private entities, the government must always remain fully in control of the entire surveillance process. Decryption of secured data may be permissible only if it is legally defined and following due process and prior judicial authorisation.
   c) Only communications falling outside the scope of professional secrecy or legal professional privilege may be intercepted. No system protects communications where the lawyer is involved in the furtherance of a criminal purpose. The objective should be to ensure the inviolability of material which falls within the scope of lawyer-client confidentiality. Therefore, a warrant to intercept communications with a lawyer should not be granted unless there is compelling evidence that the material sought to be intercepted will not be protected by legal professional privilege or professional secrecy. State agencies or law enforcement authorities should be required to use all technological means availableto leave material protected by professional secrecy and legal professional privilege out of the scope of surveillance operations[16].

---

[14] Council of Bars and Law Societies of Europe, Recommendations on the protection of client confidentiality within the context of surveillance activities, 28 April 2016.

[15] For example, the 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, §132), European Digital Rights (EDRi), the Fédération des Barreaux d'Europe (Data Retention and Legal Professional Privilege, adopted by the FBE Congress in Bilbao in May 2015).

[16] The use of electronic communications services or other cloud services by lawyers should be protected in the same way regardless of whether the content is stored in a data centre, or in a computer at the lawyer's office or on his person. Content that contains a professional secret or legally privileged information, and that is processed by an electronic communication service or a cloud service provider (including an email service provider), should not be accessible to government agencies. Electronic communications services and cloud service providers should be required to offer lawyers an option for indicating such information – of course, only after careful verification as to whether that user is indeed a lawyer as claimed. For example, in the Netherlands, there exists a telephone number recognition system which is capable of recognising lawyers' telephone numbers and cutting surveillance.

d) Prior judicial, and where required, conditional, authorisation of interception of lawyer-client communications, is required. *A posteriori* judicial review should be allowed (if at all) only in exceptional circumstances. Once judicial authorisation has been granted, it is necessary to ensure that an independent judicial body with the power to terminate interception and/or destroy intercepted material, supervises all stages of the surveillance procedure. To that end, the oversight body must be given sufficient powers by law in order to take enforceable decisions and be financially and politically independent.

e) Any intercepted material obtained without judicial authorisation and in violation of the protection of client confidentiality should be ruled inadmissible in a court of law and be required to be destroyed. Any material lawfully obtained should be admissible as evidence in court and disclosed to all parties to the case.

f) It is necessary that legal remedies should be made available to lawyers and their clients who have been the subject of unlawful surveillance and that a system of sanctions be introduced. Lawyers and their clients have the right to be informed of the data collected as a result of direct or indirect surveillance once it has been disclosed that surveillance measures have been undertaken, and should be able to challenge the legality of such measures in court. All government authorities which have been found to have been undertaking unlawful surveillance activities should be made liable to having sanctions imposed upon them.

2. **urges** the development and adoption of Recommendations by the Committee of Ministers of the Council of Europe on the protection of lawyer-client communications in the context of surveillance activities on the basis of the standards outlined above.

3. **invites** the Committee of Ministers of the Council of Europe to develop a definition of “national security” with adequate specificity so as to ensure that government activities can be effectively reviewed in court to ensure compliance with a strict test of what is necessary and proportionate.