

DRAFT CCBE Recommendations on the protection of client confidentiality within the context of surveillance activities

I. INTRODUCTION

In recent years the CCBE has expressed its deep concerns¹ regarding revelations about the working methods of national intelligence services. These concerns in particular relate 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. Although these technologies may bring benefits in the fight against terrorism and organised crime, they also create a number of specific new problems that have to be addressed, notably those concerning the legality of the interference with fundamental human rights.

Such interference becomes particularly hazardous when the data and communications accessed by governments are those that have been granted special protection by law. This is clearly the case in relation to communications between lawyers and their clients. In all EU Member States, the law protects from disclosure information communicated in confidence between lawyer and client. Without such protection, the very operation of the rule of law is undermined.

Notably, access to justice, the right to a fair trial, and the right to privacy may all be impacted. These rights are protected in numerous domestic and international legal instruments, including the [European Convention on Human Rights](#) (ECHR) and the [EU Charter of Fundamental Rights](#). Undermining the confidentiality of lawyer-client communication – whether that confidentiality is founded upon the concept of professional secrecy or (as it is in some jurisdictions) legal professional privilege – means violating international obligations, denying the rights of the accused, and an overall compromising of the democratic nature of the State.

This has been recognised by various international bodies. For example, the European Parliament adopted in October 2015 a follow-up resolution² on the electronic mass surveillance of EU citizens which underlines that the rights of EU citizens must be protected against any surveillance of confidential communications with their lawyers. Moreover, the European Parliament explicitly called upon the European Commission to adopt a communication in this respect³. Furthermore, the Council of Europe adopted and released several papers on this issue in 2015. The Parliamentary Assembly adopted a resolution⁴ highlighting that the interception of privileged communications of lawyers endangers fundamental rights, and in particular the right to privacy and the right to a fair trial. The Venice Commission released an update⁵ of a previous report on the democratic oversight of the security and intelligence services, which acknowledges that high protection must be afforded to lawyer-client communications, including procedural safeguards and strong external oversight. Finally, the Commissioner for Human Rights highlighted in an issue paper⁶ that the interception of communications between lawyers and their clients can undermine the equality of arms and the right to a fair trial.

¹ [CCBE Statement on mass electronic surveillance by government bodies \(including of European lawyers' data\)](#), 2013; [CCBE Comparative Study on Governmental Surveillance of Lawyers' Data in the Cloud](#), 2014; [European Lawyers Welcome European Parliament Action against Mass Electronic Surveillance](#), 2014; [Letter to Polish Parliament regarding draft law on amendments to the law on Police and other acts in connection with the judgment of the Polish Constitutional Tribunal from 30 July 2014](#), 2016; [CCBE Letter to James Brokenshire MP, Immigration and Security Minister of United Kingdom](#), 2015; [Dutch court upholds lower court ruling banning surveillance of lawyers' communications after successful CCBE intervention](#), 2015; [The CCBE has intervened before the French Constitutional Council to defend the confidentiality of communications between lawyers and their clients](#), 2015.

² European Parliament [Resolution](#), 'Follow-up to the European Parliament resolution of 12 March 2014 on the electronic mass surveillance of EU citizens', 29 October 2015.

³ *Ibid*, §43.

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

⁵ Council of Europe Venice Commission, '[Update of the 2007 Report on the Democratic Oversight of the Security Services and Report on the Democratic Oversight of Signals Intelligence Services](#)', 2015, §18 and 106.

⁶ Council of Europe Commissioner for Human Rights, '[Democratic and effective oversight of national security services](#)', Issue Paper, Council of Europe, 2015, 27.

The importance of this principle therefore cannot be overstated, and yet, it is today under great threat. Recent developments in various European countries compromise the protection traditionally afforded to professional secrecy by democratic states.⁷

The purpose of this paper is to inform legislators and EU policy makers about standards that must be upheld in order to ensure that the essential principle of professional secrecy is not undermined in relation to practices undertaken by the state involving the interception of communication data for the purpose of surveillance and/or law enforcement.

II. PROFESSIONAL SECRECY – MEANING AND SCOPE

Professional secrecy and legal professional privilege

For lawyers to be effective in defending their clients' rights, there must be confidence that communications between lawyers and their clients are kept confidential. This has been recognised throughout Europe for centuries. In essence, without this guarantee, there is a danger that a client would lack the trust which enables him to make full and frank disclosure to his lawyers, and, in turn, the lawyers would lack sufficient (and it may be important) information required to enable the lawyer to give full and comprehensive advice to the client or represent him effectively. 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 and/or representation in any type of legal proceedings.

Although a detailed analysis of legal professional privilege and professional secrecy lies outside the scope of the present document, it is helpful to understand the broad general approach taken by each.⁸

The concept of legal professional privilege attaches to lawyer-client communications a privilege of confidentiality, which belongs to the client. The lawyer comes under an obligation arising from the lawyer-client relationship, to keep confidential all communications between the client and himself falling within the scope of his function as the lawyer instructed by the client, unless the client waives that confidentiality. That civil obligation translates into a deontological one. It is, however, important to understand that the privilege does not attach to communications which do not lie within the scope of the relationship between the client as client and the lawyer as that client's lawyer. For example, it does not apply to communications between an individual and a lawyer, who may well be acting as the client's lawyer in some matters, which relate to a matter which does not lie within the scope of the professional relationship. To take a clear example: if the lawyer is involved not in the criminal defence of a client who has been accused of committing a bank robbery or a terrorist act, but as co-conspirator in planning with the client a bank robbery or terrorist act, then clearly this will lie outside the scope of legal professional privilege. In common law jurisdictions, this is usually referred to as "the iniquity

⁷ For example, in France, the recently-adopted *loi sur le renseignement* would allow intelligence agencies to use wider spying techniques than ever, and to have access to metadata on all communications (including between lawyers and their clients). In The Netherlands – following a challenge brought against the Dutch State in June 2015 by a law firm with the support of the CCBE – the Court ordered the Government to stop all surveillance of lawyers' communications until it provided for sufficient safeguards, including independent oversight, both of which were found to be insufficient. In Poland, the government recently proposed amendments to the Act on Police and to other acts related to the state secret services, in particular, in relation to the regulation of data surveillance and data retention. These amendments include provisions providing unqualified access to information protected by professional secrecy. As a final example, the UK's forthcoming Investigatory Powers Bill has been denounced as a threat to professional secrecy by the UK Bars and Law Societies because it would give wide access to confidential information related to the client without giving statutory protection to legal professional privilege, confining it to a non-legislative 'code of practice'.

⁸ A full discussion can be found in the following reports: ['Report on The professional secret, confidentiality and legal professional privilege in the nine member states of the European Community'](#), CCBE, D.A.O. Edward, Q.C., 1976; ['Update of the Edward's Report on the professional secret, confidentiality and legal professional privilege in Europe'](#), CCBE, 2003; ['Regulated legal professionals and professional privilege within the European Union, the European Economic Area and Switzerland, and certain other European jurisdictions'](#), CCBE, John Fish, 2004.

exception”, though it is important to note that it is not truly an exception: rather it is a matter which does not, in the first place, fall under the scope of legal professional privilege.

Where the basis is professional secrecy, the obligation to keep communications confidential is an absolute one. It is an obligation which rests directly upon the lawyer and, in most jurisdictions, it cannot be waived by the client. Breach of that obligation may extend beyond being essentially a civil and/or deontological one (as with legal professional privilege) and, in some jurisdictions be enforceable in criminal law. Notwithstanding these important differences, the concept of professional secrecy shares with legal professional privilege the understanding that its scope does not extend to cover a case where the lawyer is engaged with the client in the furtherance of a criminal activity.

For clarity purposes, the present document refers to “professional secrecy” as including both concepts.

Without confidentiality, no fair trial

Most legal systems share a common understanding that if the right of the citizen to safeguard confidentiality, i.e. the right of the citizen to be protected against any divulging of his/her communication with his/her lawyer, were to be denied, people may be denied access to legal advice and to justice. Professional secrecy is thus seen as an instrument by which access to justice and the maintenance of the rule of law can be achieved. Indeed, the European Court of Human Rights (ECtHR) has repeatedly linked the respect of professional secrecy to the observance of Articles 6 and 8 of the ECHR. Firstly, the Court considered that “*an accused’s right to communicate with his advocate out of hearing of a third person is part of the basic requirements of a fair trial in a democratic society and follows from Article 6 para. 3 (c) of the Convention*”⁹. Furthermore, the Court stated that “*the right of everyone to a fair trial*”¹⁰ is dependent upon the “*relationship of trust between [the lawyer and the client]*”. Secondly, the Court repeatedly highlighted that undermining professional secrecy may violate Article 8, which protects the right to respect for private and family life. Indeed, the Article “*affords strengthened protection to exchanges between lawyers and their clients*”¹¹. The Court goes on: “*this is justified by the fact that lawyers are assigned a fundamental role in a democratic society, that of defending litigants. Yet they cannot carry out this essential task if they are unable to guarantee to those they are defending that their exchanges will remain confidential*”.

Case law

There is abundant jurisprudence by the European courts both in Luxembourg and Strasbourg that deals with professional secrecy and highlights the importance of this principle. European legal instruments have also enshrined professional secrecy. Additionally, all EU Member States recognise professional secrecy as one of the major objectives and principles of regulation for the legal profession, the violation of which constitutes in some EU Member States not only a professional violation, but also a criminal offence. Moreover, the CCBE in its own CCBE Charter of Core Principles of the European Legal Profession, the CCBE Code of Conduct for European Lawyers and numerous other documents stipulates professional secrecy as one of the core values of the European legal profession. Key decisions of the European courts, relevant European legal instruments as well as the CCBE’s own documents are referred to in more detail below.

Court of Justice of the European Union (CJEU): the AM&S case

In the *AM&S v. Commission* case, the Court of Justice of the European Union (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 EC law.¹² 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

⁹ ECtHR, *S. v. Switzerland* (12629/87), 1991, §48. Also see ECtHR, *Domenichini v. Italy* (15943/90), 1996, §39; ECtHR, *Öcalan v. Turkey* (46221/99), 2005, §1333; ECtHR, *Moiseyev v. Russia* (62936/00), 2008, §209; ECtHR, *Campbell v. the United Kingdom* (13590/88), 1992, §§ 44-48.

¹⁰ ECtHR, *Michaud v. France* (12323/11), 2012, §117-8.

¹¹ Ibid; also see ECtHR, *Kopp v. Switzerland* (23224/94), 1998.

¹² ECtHR, *AM & S v Commission* (155/79), 1982, §16 and 18.

must be protected.¹³ professional secrecy can be relied upon not only by natural persons, but also by companies that may be subject to a Commission investigation, regardless of their legal form. It covers all documents in the hands of the lawyer or the client and applies to communications originating from either.

The CJEU's decision was of particular importance, and still is, since it confirmed the protection of privileged communication (which was disputed up until 1978) and it defined the scope of legal privilege and its practical implications. The CJEU noted that professional secrecy is closely linked to the concept of the lawyer's role as collaborating in the administration of justice by the courts¹⁴. The CCBE intervened in the case in support of the applicant.

In *AM&S* the CJEU defined the scope of professional secrecy in the European Community system, on the basis of the legal traditions common to the Member States. It interpreted Regulation 17 as protecting the confidentiality of written communications between a lawyer and his or her clients, subject to two conditions, incorporating such elements of that protection as were found to be common to the Member States' laws in 1982, namely that such communications: (i) are made for the purposes and in the interests of the client's rights of defence, and (ii) emanate from independent lawyers who are qualified to practice in an EEA country.

With regard to the first requirement, the CJEU emphasized that it must be ensured that the rights of defence may be exercised in full in the context of the Commission's investigation proceedings, and that the protection of the confidentiality of written lawyer-client communications is an essential corollary to the rights of defence. It therefore recognized that all written communications exchanged after the initiation of the proceedings must be protected. However, since the Commission can commence an investigation before the formal initiation of proceedings, the Court held that – in order not to discourage any undertaking from taking legal advice at the earliest opportunity – the protection of professional secrecy extends to any earlier written communications that have a relationship to the subject-matter of that procedure. Legal advice is regarded as a “preparatory” step in the undertaking's defence¹⁵.

Pursuant to the second requirement established in *AM&S*, professional secrecy applies only to written communications emanating from independent lawyers who are entitled to practice their profession in one of the Member States, regardless of whether this is the same Member State in which the client resides.¹⁶ This means that, by definition, communications involving lawyers qualified in third countries such as the United States will not fall to be treated as privileged for the purposes of the EU legal regime, even if those lawyers are based in the EC.

¹³ Ibid. Although *AM&S* was concerned with inspections, it has been generally acknowledged that the principles established in that case also apply to the Commission's requests for information. *AM&S* originated in a dispute about the confidentiality of a series of documents which were found at the premises of *AM&S* - a UK company - during an investigation into a cartel. The company withheld some of the documents on grounds that they were privileged written communications between lawyer and client. The European Commission issued a decision requiring *AM&S* to produce these documents.

¹⁴ Ibid, §24: *As regards the second condition, it should be stated that the requirement as to the position and status as an independent lawyer, which must be fulfilled by the legal adviser from whom the written communications which may be protected emanate, is based on a conception of the lawyer's role as collaborating in the administration of justice by the courts and as being required to provide, in full independence, and in the overriding interests of that cause, such legal assistance as the client needs. The counterpart of that protection lies in the rules of professional ethics and discipline which are laid down and enforced in the general interest by institutions endowed with the requisite powers for that purpose. Such a concept reflects the legal traditions common to the Member States and is also to be found in the legal order of the community, as is demonstrated by article 17 of the Protocols on the Statutes of the Court of Justice of the EEC and the EAEC, and also by article 20 of the protocol on the statute of the Court of Justice of the ECSC.*

¹⁵ Fordham International Law Journal, Volume 28, Issue 4, page 1009, 2004.

¹⁶ ECtHR, *AM & S v Commission* (155/79), §25. The limits of this protection are to be determined by reference to the rules on the practice of the legal profession as set forth in Council Directive 77/249/EEC of March 22, 1977, to facilitate the effective exercise by lawyers of freedom to provide services (OJ L 78/17) and Directive 98/5/EC of the European Parliament and of the Council of February 16, 1998, to facilitate practice of the profession of lawyer on a permanent basis in a Member State other than that in which the qualification was obtained (OJ L 77/36).

Moreover, the notion of “independent lawyer” does not encompass, in the Court’s view, any legal expert who is bound to his or her client by a relationship of employment¹⁷. The Court found that this requirement, as to the position and status of a legal adviser, is based on the “*conception of the lawyer’s role as collaborating in the administration of justice by the courts and as being required to provide, in full independence, and in the overriding interests of that cause, such legal assistance as the client needs*”.¹⁸ Despite its reference to “*the rules of professional ethics and discipline which are laid down in and enforced in the general interest by institutions endowed with the requisite powers for that purpose*” as being the counterpart of the protection of professional secrecy, the Court held in *AM&S* that, based on common criteria found in the national laws of the Member States, a document containing legal advice and exchanged between a lawyer and his or her client is protected against disclosure only if the lawyer is ‘independent’, “*that is to say one who is not bound to his client by a relationship of employment*”.¹⁹

European Court of Human Rights

Judgments of the ECtHR have also recognised a right to confidentiality of communications between lawyer and client on the basis of either Article 8 ‘Right to respect for private and family life’ or Article 6 ‘Right to a fair trial’ of the ECHR.

Article 8 clearly establishes the right of everyone to respect for his correspondence. It protects the confidentiality of communications whatever the content of the correspondence concerned and whatever form it may take. Any interference must be in accordance with the law, pursue a legitimate aim and be necessary in a democratic society to achieve the aim concerned. The latter has been considered by the Court in numerous decisions. It is noteworthy, however, that, although the article 8 right is qualified in the manner explained above, the article 6 right is unqualified.

The jurisprudence of the ECtHR is very rich as far as the confidentiality of lawyer-client communication is concerned and has increasingly developed over the years. Reference is made here to a few key decisions laying down general principles to be observed when it comes to the lawyer-client relationship:

- “(...) *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 (...).*”²⁰
- “(...) *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 (art. 6) of the Convention. (...).*”²¹
- “*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.*”²²

In the case [Foxley v. The United Kingdom](#) (2000), which is of particular interest as far communications between lawyers and clients are concerned, the Court ruled that Article 8 was violated by the interception of correspondence of the applicant with his solicitors. The Court highlighted in this case the need for effective safeguards to ensure minimum impairment of the right to respect for correspondence and also recalled 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:

¹⁷ Some European countries allow for lawyers – registered with a Bar or Law Society – to work in-house for a company. These lawyers are subject to the same professional and ethical rules as outside lawyers.

¹⁸ ECtHR, *AM & S v Commission* (155/79), §24 and 27.

¹⁹ *Ibid.*

²⁰ ECtHR, *S. v. Switzerland* (12629/87), 1991, §48.

²¹ ECtHR, [Niemietz v. Germany](#) (13710/88), 1992, §37.

²² ECtHR, *Kopp v. Switzerland* (23224/94), 1998, §74.

*“43. The Court recalls that the notion of necessity implies that the interference corresponds to a pressing social need and, in particular, that it is proportionate to the legitimate aim pursued. In determining whether an interference is “necessary in a democratic society” regard may be had to the State’s margin of appreciation (see the *Campbell v. the United Kingdom* judgment of 25 March 1992, Series A no. 233, p. 18, § 44). It further observes that in the field under consideration - the concealment of a bankrupt’s assets to the detriment of his creditors - the authorities may consider it necessary to have recourse to the interception of a bankrupt’s correspondence in order to identify and trace the sources of his income. Nevertheless, the implementation of the measures must be accompanied by adequate and effective safeguards which ensure minimum impairment of the right to respect for his correspondence. This is particularly so where, as in the case at issue, correspondence with the bankrupt’s legal advisers may be intercepted. The Court notes in this connection 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 (the above-mentioned *Campbell* judgment, pp. 18-19, §§ 46 and 48)”.*

In the case of [R.E. v. The United Kingdom](#) (2015), the ECtHR, in finding a breach of article 8 of the convention as a result of surveillance of a lawyer-client interview in a police station stated (at paragraph 131:

“The Court therefore considers 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; higher than the degree of intrusion in [Uzun](#) and even in [Bykov](#). Consequently, in such cases it will expect the same safeguards to be in place to protect individuals from arbitrary interference with their Article 8 rights as it has required in cases concerning the interception of communications, at least insofar as those principles can be applied to the form of surveillance in question.”

The tendency of the ECtHR has been to approach the question of interception of lawyer-client communications by looking through the lens of the Article 8 right to privacy of communications, albeit affording to lawyer-client communications a higher degree of protection than that afforded to other private communications. In that context, there have been occasional comments from the Court that exceptions may be permissible, though this is not a matter which has really been explored by the Court.

There would be broad agreement that it may be necessary in a democratic society to permit interception of communications between a lawyer and a client where the lawyer is involved in criminal activity. However, there is a conceptual problem in seeing this as an exception from the protection afforded by article 8 to lawyer-client communications, since such a communication is not in the first place such as would attract either legal professional privilege or professional secrecy. If the language of “exception” is used it invites a balancing exercise under article 8 and precisely where the balance lies in any given case may not be predictable, and may possibly change with time and circumstances.

It is suggested that it would be more appropriate to determine, first, what kind of lawyer-client communication falls within the scope of article 6. The jurisprudence of the ECtHR tends to suggest that this would be regarded as including the communications which are protected under legal professional privilege or professional secrecy obligations in national legal systems. Clearly, communications between a lawyer and his client relating to a joint criminal enterprise would not be so regarded. Once it had been determined that a communication fell within the article 6 protection, then there could be no question of allowing an exception, as article 6 (unlike article 8) does not permit exceptions. However, in relation to communications not falling under article 6, then, since they would remain private communications, it would remain appropriate to undertake a balancing act under article 8. This approach is both intellectually coherent and avoids the trap of there being an ill-defined and, it may be shifting boundary between professional secrets where an exception should, and should not be made. It also has the advantage of being in broad harmony with the approach taken under national systems, whether founded on legal professional privilege or professional secrecy.

Council of Europe [Recommendation](#) Rec (2000)21 of 25 October 2000

In addition to the abundant jurisprudence of the European Courts regarding privileged communications, it is also important to mention the Council of Europe Recommendation Rec (2000) 21 of 25 October 2000 concerning the freedom of exercise of the profession of lawyer in Europe which provides that “*All measures should be taken to ensure the respect of confidentiality of the lawyer-client relationship. Exceptions to this principle should be allowed only if compatible with the Rule of Law.*” (Principle I, paragraph 6) and that “*Professional secrecy should be respected by lawyers in accordance with internal laws, regulations and professional standards. Any violation of this secrecy, without the consent of the client, should be subject to appropriate sanctions.*” (Principle III, paragraph 2)

CCBE documents

The CCBE attaches great attention to the core values of the legal profession in Europe, including professional secrecy. This is also why it is working at the time of the publication of the present paper ‘Towards a model code of conduct’ which will serve as guidance for national Bars and Law Societies when reviewing their own national rules. The model code will deal, amongst others, with confidentiality and taking into account the existing jurisprudence of the European courts.

The CCBE has two key documents which address confidentiality.

- First, the CCBE [Charter of Core Principles of the European Legal Profession](#), which was adopted on 24 November 2006, and contains a list of ten core principles common to the national and international rules regulating the legal profession. The principles of the Charter provide:

“Principle (b) – the right and duty of the lawyer to keep clients’ matters confidential and to respect professional secrecy:

It is of the essence of a lawyer’s function that the lawyer should be told by his or her client things which the client would not tell to others - the most intimate personal details or the most valuable commercial secrets - and that the lawyer should be the recipient of other information on a basis of confidence. Without the certainty of confidentiality there can be no trust. The Charter stresses the dual nature of this principle - observing confidentiality is not only the lawyer’s duty - it is a fundamental human right of the client. The rules of “legal professional privilege” prohibit communications between lawyer and client from being used against the client. In some jurisdictions the right to confidentiality is seen as belonging to the client alone, whereas in other jurisdictions “professional secrecy” may also require that the lawyer keeps secret from his or her own client communications from the other party’s lawyer imparted on the basis of confidence. Principle (b) encompasses all these related concepts - legal professional privilege, confidentiality and professional secrecy. The lawyer’s duty to the client remains even after the lawyer has ceased to act.”

It is important to note that the CCBE Charter is not conceived as a code of conduct. It is, however, aimed at applying to the whole of Europe, reaching out beyond the member, associate and observer states of the CCBE. The Charter aims, *inter alia*, to help bar associations that are struggling to establish their independence; and to increase understanding among lawyers of the importance of the lawyer’s role in society; it is aimed at lawyers, decision makers and the general public.

- Second, the [CCBE Code of Conduct](#) for European Lawyers, which dates back to 28 October 1988 and was last reviewed in 2006, also contains a provision on confidentiality:

“2.3. Confidentiality

2.3.1. It is of the essence of a lawyer’s function that the lawyer should be told by his or her client things which the client would not tell to others, and that the lawyer should be the recipient of other information on a basis of confidence. Without the certainty of confidentiality there cannot be trust. Confidentiality is therefore a primary and fundamental right and duty of the lawyer.

The lawyer’s obligation of confidentiality serves the interest of the administration of justice as well as the interest of the client. It is therefore entitled to special protection by the State.

2.3.2. *A lawyer shall respect the confidentiality of all information that becomes known to the lawyer in the course of his or her professional activity.*

2.3.3. *The obligation of confidentiality is not limited in time.*

2.3.4. *A lawyer shall require his or her associates and staff and anyone engaged by him or her in the course of providing professional services to observe the same obligation of confidentiality.”*

Unlike the Charter, the Code is a text which is binding on all CCBE Member Bars and Law Societies, meaning that all lawyers who are members of the bars of these countries (whether their bars are full, associate or observer members of the CCBE) have to comply with the Code in their cross-border activities within the European Union, the European Economic Area and the Swiss Confederation as well as within associate and observer countries.

The above shows that the confidentiality of communications between clients and lawyers is given particularly high attention by the European courts and relevant European bodies. Confidentiality is not only seen as the lawyer’s duty, but as a fundamental human right of the client. 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.

III. CCBE RECOMMENDATIONS

1. Overarching principle

Any direct or indirect surveillance of lawyers undertaken by the State should fall within the bounds of the rule of law, and should particularly guarantee the right to a fair trial, access to justice, and professional secrecy.

2. Need for legislative control

2.1 All surveillance activities need to be regulated with adequate specificity (for example, a clear definition of “national security”) and transparency.

It cannot, in a democratic society, be permissible for security services to be non-transparent, unaccountable and operating outside a proper, binding legal framework. Without such controls, there is a risk of arbitrary disregard for human rights in general and professional secrecy in particular. In fact, placing the mandate of surveillance agencies into primary legislation is a requirement of the ECHR²³.

In certain states where there is a regulatory framework, important protections have been incorporated (if at all) not in primary legislation but in non-binding codes of practice, guidelines and the like (for example, in the United Kingdom under the Regulation of Investigatory Powers Act 2000). Though such codes and guidance may have their place, the substantive protection of professional secrecy must be enshrined in primary legislation, making the security services accountable before the courts for the way in which they perform their functions.

2.2 Legislation governing surveillance activities needs to provide for explicit protection of professional secrecy and remove deliberate targeting of client-lawyer communications from the scope of intelligence agencies’ powers.

²³ Council of Europe Venice Commission, ‘[Update of the 2007 Report on the Democratic Oversight of the Security Services and Report on the Democratic Oversight of Signals Intelligence Services](#)’, 2015, page 18: “Most democratic states, in recognition of the impact strategic surveillance has on human rights, have placed at least part of the mandate of the signals intelligence function in primary legislation. [This] is also a requirement of the ECHR.”

As such, the level of protection of professional secrecy afforded by law must always be of the highest level, regardless of whether the surveillance measure is undertaken for the purpose of law enforcement (e.g. by police and judicial services) or for the protection of national security (e.g. by national intelligence agencies). The intrusive nature and potential impact of both type of activities on the individual's right to a fair trial is identical and therefore requires an equivalent high level of legal protection.

A cautionary tale is the UK case of [Re McE](#)²⁴. In that case, the House of Lords, interpreted the absence of a specific protection of legal professional privilege as impliedly permitting legally privileged material to be intercepted, with the result that (as a matter of statutory interpretation) Parliament was taken to have decided to over-ride legal professional privilege. The decision has been widely criticised, but it is noteworthy that the text of the proposed new legislation which was debated in Parliament replicates, in this respect, the wording of the 2000 act with the intention of depriving material covered by professional secrecy of protection.

2.3 Legislation must provide sufficient guarantees in the event of full or partial outsourcing of surveillance activities to private entities, so as to ensure that the government always remains in full control of, and fully responsible for, the entire surveillance process, data, and use of data.

The outsourcing of surveillance activities to private entities may divert responsibility away from police, judicial or national security departments and onto small companies that cannot be held accountable to constitutional prohibitions. Therefore, private entities that are involved in the surveillance process must be subject to stringent deontological rules and confidentiality requirements, and be under a contractual obligation to provide full transparency and governmental access to their technical and organisational arrangements governing the surveillance activities. State entities must be provided with sufficient expertise and resources in order to be able to remain in full control of any surveillance activities that are outsourced to private entities.

2.4 Legislation should not prevent lawyers from adequately protecting the confidentiality of their communications with clients (through e.g. encryption methods), and should not give state agencies or law enforcement privileged access to encrypted data.

Lawyers keep sensitive information (from trade secrets to private life details), which were trustfully provided to them by clients and may not be disclosed. This makes lawyers particularly vulnerable to unlawful attacks by the government or private hackers, and requires adequate cryptographic protection. The right to data protection also covers data security, as protected by Article 8 of the ECHR, article 8 of the Charter of Fundamental Rights in the EU²⁵, as well as by the [1981 Data Protection Convention of the Council of Europe](#), and the current [2008 Data Protection Framework Decision](#). However, an even broader scope of rights may be affected by a lack of data security, such as economic rights, privacy, and due process²⁶. Therefore, decryption may only be permissible if it is legally defined and any decision allowing the decryption of protected lawyer-client communications must be granted by an independent judge, on a case-by-case basis, and following due process.²⁷

3. Scope of admissible interception

3.1 Only communications falling outside the scope of professional secrecy may be intercepted.

As discussed above, the first question to be asked when it is sought to intercept communications protected by professional secrecy is whether the communication falls within the scope of professional secrecy. If it does, then, consistently with article 6 ECHR, there should be no question of interception being permitted. If it does not, it would then be appropriate to consider whether and to what extent an exception might be made to the article 8 protection of private communications. In many cases (for example, where the communication relates to the furtherance of a criminal purpose) that may be a relatively easy balance to strike.

²⁴ House of Lords, UKHL 15, 2009.

²⁵ Ibid.

²⁶ Ibid.

²⁷ Ibid.

3.2 Security agencies should be required to use all technological means available to leave material protected by professional secrecy out of the scope of surveillance operations.

It is appreciated that a distinction may fall to be made between targeted and non-targeted surveillance, and, particularly in the case of the latter, there may also be a danger of the accidental interception of communications subject to professional secrecy. For example, in the Netherlands, there exists a telephone number recognition system which is capable of recognising lawyers' telephone numbers and cutting surveillance. Part of the discussion in the case of *Prakken d'Oliveira*²⁸ concerned the extent to which this system should be used by the security services.

3.3 Interception should be permitted only when the body wishing to undertake surveillance can show that there are compelling reasons giving rise to a sufficient degree of suspicion to justify such interception. The process of interception should not be used as means of obtaining material upon which a suspicion might be based. Intervention should not be targeted at material protected by legal professional secrecy obligations. Therefore, a warrant to intercept should not be granted to intercept communications with a lawyer unless there is compelling evidence that the material will not be protected by professional secrecy.

3.4 Legislative controls should be in place to regulate the process of examining material potentially protected by professional secrecy so as to eliminate the risk that it may subsequently be used. Notwithstanding the abovementioned safeguards, there may still be a risk that communications protected by professional secrecy are accidentally intercepted. Therefore, intelligence gathering agencies must be transparent about the information collected, including how, and to what extent, communications potentially protected by professional secrecy will be sought to be intercepted, what are the risks of such communications subject to professional secrecy being in fact intercepted, what safeguards are in place to prevent this occurring and, if it does accidentally occur, what steps will be taken to prevent the material being used.

4. Judicial and independent oversight

A. Nature of oversight

4.1 In case of interception of lawyer-client communications, there needs to be supervision at all stages of the surveillance procedure, on a case-by-case basis.

In a democratic society, external oversight is indispensable, as relying only on internal and governmental controls (such as ministerial authorisation) of surveillance activities is insufficient²⁹. This is particularly true considering that, as pointed out by the ECtHR in 1978³⁰, surveillance activities are necessarily carried out without the knowledge of the targeted individual. As a consequence, the person will be prevented from seeking an effective remedy or from taking a direct part in any review proceedings. It is then essential that the established procedures themselves adequately safeguard the individual's rights.

4.2 Supervisory control must be entrusted to a judicial body.

Judicial oversight is an important safeguard against arbitrariness: only a judge can offer the necessary guarantees of independence, impartiality and a proper procedure. Indeed, the ECtHR considered in 1978³¹ that, 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. The Court tied this to the principle of the rule of law. Moreover, it is

²⁸ Hague Court of Appeal, *Prakken D'Oliveira and others v. The State of The Netherlands*, n. 200 174 280/01, 2015.

²⁹ Report and Recommendations of the U.S.A. President's Review Group on Intelligence and Communications Technologies, '[Liberty and Security in a Changing World](#)', 2013: "Americans must never make the mistake of wholly "trusting" our public officials.", page 118. Also see Venice Commission, '[Update of the 2007 Report on the Democratic Oversight of the Security Services and Report on the Democratic Oversight of Signals Intelligence Services](#)', 2015, page 31.

³⁰ ECtHR, *Klass and Others v. Germany* (5029/71), 1978, §55.

³¹ *Ibid*, §56.

important to give adequate guarantees to the separation of powers, and thus not to entrust a parliamentary or administrative body with such a quasi-judicial supervisory role³².

4.3 The judge supervising the surveillances activities should be both financially and politically independent from the executive and should be irremovable³³. The judge giving approval to a request for interceptions should not be the same supervising their implementation.

The only way to ensure that judicial authorisation will be given out in an impartial and objective manner is to ensure the full independence of the judicial oversight body. This means that the judicial oversight body may not be placed in subordination to or under the effective control or influence of the executive branch of government or of the department seeking authorisation.

For instance, the ECtHR in 1998³⁴ considered that it was astonishing that a task such as determining whether conversations between a lawyer and their client related to activities other than counsel would be left to a member of the executive without supervision by an independent judge. This issue was deemed especially grave because of the sensitive nature of confidential relations between a lawyer and their clients, which directly concerns the rights of the defence³⁵. The only body allowed to take the decision to interfere with the confidentiality of lawyer-client communications must be independent³⁶.

4.4 Prior external, and where called for, conditional, authorisation of the imposition of any interception measure is required.

In order to respect professional secrecy and the confidentiality of sensitive information as much as possible, it is important to establish that *prior* judicial authorisation must be the norm, and only in exceptional circumstances should *a posteriori* judicial review be allowed. The supervision must be carried out ahead of the implementation of the surveillance measure in order to prevent the surveillance from taking place if found unlawful. Moreover, this prior judicial authorisation should only be valid for a defined and reasonable period of time, so as to enable a regular assessment of the situation and the lawfulness of the imposed measures.

As mentioned, *a posteriori* control may be allowed in special circumstances. It may be the case when the threat is imminent and that no judge is immediately available to grant authorisation. To prevent *a posteriori* controls, it is important that the government takes all necessary measures to ensure that the judicial body is, to the extent possible, available at all times.

4.5 Once authorisation has been granted, a separate body, meeting the same requirements as the one granting authorisation, needs to supervise the implementation of the interception measure for which permission was granted. This body must have the power to terminate interception and/or destroy gathered data if it finds that the surveillance measures are implemented in an unlawful manner.

In order to prevent abuse by the surveillance authorities and law enforcement authorities, it is important that an independence and judicial body monitors the implementation of the measure. So as to be comprehensive and efficient, it must comprise in particular: (i), substantial compliance with the permission as it was granted including, where applicable, any conditions attached thereto, (ii) the retention of gathered data, (iii) the sharing of gathered data with other governmental agencies or governments, (iv) the selection and analysis of the gathered data, (v) the conditions under which it becomes mandatory to notify the object of the interception thereof and (partial) disclosure of the gathered data.

Although there is a requirement for judicial oversight both prior to the exercise of a power of surveillance (by the imposition of a legal requirement that a judicial warrant is required for the exercise of that power) and *ex post facto* (for example to deal with a complaint that the security agency acted

³² Venice Commission, '[Update of the 2007 Report on the Democratic Oversight of the Security Services and Report on the Democratic Oversight of Signals Intelligence Services](#)', 2015, page 32.

³³ Subject to fixed terms and rules such as misconduct and health issues.

³⁴ ECtHR, *Kopp v. Switzerland* (23224/94), 1998.

³⁵ *Ibid*, §74.

³⁶ Hague Court of Appeal, *Prakken D'Oliveira and others v. The State of The Netherlands*, n. 200 174 280/01, 2015, 2.7-8.

unlawfully in a given case), it does not necessarily follow that the prior and ex post facto supervision require to be carried out by the same body (for example, the granting of a warrant may lie with a single judge, whereas ex post facto control might be exercised by a special judicial tribunal), provided that the requirements set out above are met by each.

B. Mandate of the oversight body

4.6 The oversight body or bodies should be charged with ensuring that surveillance measures do not infringe professional secrecy.

To that end, in considering whether to grant a warrant for interception, the oversight body should seek to review the lawfulness and effectiveness of the surveillance measure (Amsterdam Standard 1): in the case of communications with lawyers the oversight body should require compelling evidence that the communication does not fall within the scope of material protected by professional secrecy.

The body should be satisfied that there are in place appropriate measures to minimise the risk of the accidental recovery of communications protected by professional secrecy, to assess objectively whether the material accidentally recovered falls outside the scope of professional secrecy, and to limit and control any possibility of any material which is so protected and which is accidentally recovered being made use of.

The body exercising ex post facto control should also require to ensure that the security agency has not infringed any of the foregoing principles.

C. Powers of the oversight bodies

4.7 In order to fulfil its mandate, the oversight body must be given proportionate, adequate, and binding powers by law. These competences must enable the body to make fully informed and enforceable decisions.

In order to make fully informed decisions, the oversight bodies should have access to:

- All evidence that the communications in question are not covered by professional secrecy, and that there is no other way to get criminal evidence than to intercept these communications. In case of *ex post facto* oversight, this would include all intercepted material³⁷.
- Any policies drawn up by the State to control and supervise the surveillance of conversations covered by professional secrecy.
- Orders received by private entities to provide information to the government.

It is important to stress that if the supervisory bodies do not at the very least have the power to terminate the surveillance of lawyer-client communications, the bodies will not be able to fulfil their mandate³⁸. Therefore, in order to make enforceable decisions, the oversight bodies should be able to:

- Provide authorisation of the surveillance measure (if deemed lawful and effective).
- Quash any interception order it deems unlawful³⁹.
- Order the authorities to cease and discontinue the direct and indirect tapping, receiving, recording, monitoring, and transcribing of any form of communication by and with lawyers, if found unlawful.
- Order the permanent destruction⁴⁰ of direct and indirect tapping, receiving, recording, monitoring, and transcribing of any form of communication by and with lawyers, if found unlawful. In particular, in the case of *ex post facto* oversight, the body should be able to prohibit the passing of illegally obtained information on to the Prosecutor's Office.

5. Use of intercepted material

³⁷ ECtHR, *Zakharov v. Russia* (47143/06), 2015, §280; see also ECtHR, *Kennedy v. UK* (26839/05), 2010, §166.

³⁸ Hague Court of Appeal, *Prakken D'Oliveira and others v. The State of The Netherlands*, n. 200 174 280/01, 2015, 2.9.

³⁹ See *Telegraaf v. Netherlands* (39315/06), 2012; see also ECtHR, *Kennedy v. UK* (26839/05), 2010.

⁴⁰ ECtHR, *Kennedy v. UK* (26839/05), 2010, §168.

5.1 Any intercepted material obtained without (prior) judicial authorisation and in violation with the principle of professional secrecy should be ruled inadmissible in a court of law.

As repeatedly recognised by the ECtHR⁴¹ professional secrecy is inextricably linked with the right to a fair trial. Firstly, the Court considered that *“an accused’s right to communicate with his advocate out of hearing of a third person is part of the basic requirements of a fair trial in a democratic society and follows from Article 6 para. 3 (c) of the Convention”*⁴². Furthermore, the Court stated that *“the right of everyone to a fair trial”*⁴³ is dependent upon the *“relationship of trust between [the lawyer and the client]”*. Secondly, the Court repeatedly highlighted that undermining professional secrecy may violate Article 8, which protects the right to respect for private and family life. Indeed, the Article *“affords strengthened protection to exchanges between lawyers and their clients”*⁴⁴. It follows from this reasoning that any evidence obtained in violation of the principle of professional secrecy should not be admissible in court, unless the surveillance measure was duly authorised by an independent judicial oversight body as set out in section 4. Conversely, material which has been lawfully obtained should be admissible as evidence in court.

5.2 Any lawfully intercepted material should be used solely for the exact purpose for which the authorisation of the oversight body was granted. Any other use would be a violation of the principle of professional secrecy, and should accordingly be ruled inadmissible in a court of law.

5.3 When intercepted material is ruled unlawful, it has to be destroyed. This includes all information related to the communication, such as the participants, the time, the location, and all other relevant information.

6. Legal remedies

6.1 In order to provide effective legal protection against unlawful surveillance, it is necessary that legal remedies and sanctions are available to lawyers.

In 2006, the ECtHR established that – at least once security measures have been disclosed – legal remedies must become available to the individual concerned⁴⁵.

6.2 In particular, once surveillance measures are disclosed, lawyers have the right to be informed of the data collected as a result of direct or indirect surveillance. This right is unrestricted, i.e. it cannot not limited by secrecy interests of the government and is enforceable against European and national authorities. It is important to point out that the ECtHR has passed a judgement restraining this right of information by granting the government the right to balance national security interests against the seriousness of the interference with the citizens’ right to respect for private life article 8 (06/06/2006 - 62332/00). However, as explain above, the right of citizen to confer confidentially with their lawyers is part of the basic requirements of a fair trial in a democratic society and follows from Article 6 para. 3 (c) of the ECHR. Unlike article 8, article 6 does not permit exceptions and therefore there can be no question of allowing such a balancing exercise in case the surveillance measure is targeting communication data that is covered by professional secrecy.

6.3 Once surveillance measures have been disclosed, targeted lawyers and clients should be able to challenge their legality before a judge. At least the following remedies should be made available:

Preventive measure

Lawyers and their clients should be able to request preventive measures. The preventive measure should be available against both direct and indirect surveillance. Lawyers and their clients may not

⁴¹ ECtHR, *S. v. Switzerland* (12629/87), 1991, §48; *Domenichini v. Italy* (15943/90), 1996, §39; *Öcalan v. Turkey* (46221/99), 2005, §1333; *Moiseyev v. Russia* (62936/00), 2008, §209; *Campbell v. the United Kingdom* (13590/88), 1992, §§ 44-48.

⁴² ECtHR, *S. v. Switzerland* (12629/87), 1991, §48.

⁴³ ECtHR, *Michaud v. France* (12323/11), 2012, §117-8.

⁴⁴ *Ibid.* Also see ECtHR, *Kopp v. Switzerland* (23224/94), 1998.

⁴⁵ ECtHR, *Segerstedt-Wiberg and Others v. Sweden* (62332/00), 2006, §117.

actually be aware that they have been under surveillance, and for those reasons, should not be obliged to prove that they have been under surveillance as they would regularly be unable to do so, at least in cases of mass surveillance. Accordingly, the Venice Commission⁴⁶ suggested that a general complaints procedure be established. [The case of *Zhakarov v. Russia*⁴⁷ or *Szabó and Vissy v. Hungary*⁴⁸ may also be referred to in this respect]

Request for deletion

Lawyers should be able to file a request for deletion of any data unlawfully obtained. This would be in line with the statement of the Council of Europe Commissioner for Human Rights⁴⁹, who has named the requirement to delete or correct personal data one of the most common and necessary remedies in relation to personal data collection and use by security services.

Compensation for financial as well as non-pecuniary damages

Lawyers should be compensated for any financial damages caused by unlawful surveillance. Additionally, lawyers should be compensated for non-pecuniary damages. This follows the jurisprudence of the ECtHR, which awarded in 2015⁵⁰ the amount of 4.500 Euros as just satisfaction (for 'moral prejudice') to a Bulgarian criminal defense lawyer whose communication had been intercepted.

Background

CCBE actions

Bibliography

⁴⁶ Council of Europe Commissioner for Human Rights, '[Democratic and effective oversight of national security services](#)', Issue Paper, Council of Europe, 2015, page 51.

⁴⁷ ECtHR, [Zakharov v. Russia](#) (47143/06), 2015.

⁴⁸ ECtHR, [Szabó and Vissy v. Hungary](#) (37138/14), 2015.

⁴⁹ Council of Europe Commissioner for Human Rights, '[Democratic and effective oversight of national security services](#)', Issue Paper, Council of Europe, 2015, page 51.

⁵⁰ ECtHR, [Pruteanu v Romania](#) (30181/05), 2015, §64.