

# CCBE RECOMMENDATIONS:

On the protection of client confidentiality  
within the context of surveillance activities

## CONTACT:

Council of Bars and Law Societies of Europe  
Conseil des barreaux européens  
Rue Joseph II, 40/8  
1000 Brussels  
T +32 (0)2 234 65 10


Follow us on   

[www.ccbe.eu](http://www.ccbe.eu)  
[ccbe@ccbe.eu](mailto:ccbe@ccbe.eu)

Cover illustration / *illustration de la couverture:*

© Rzoog - Fotolia.com

## EXECUTIVE SUMMARY



*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.*

– the CCBE Code of Conduct, Article 2.3

The purpose of this paper is to inform legislators and policy makers about standards that must be upheld in order to ensure that the essential principles of professional secrecy and legal professional privilege are not undermined by practices undertaken by the state involving the interception of communications and access to lawyers' data for the purpose of surveillance and/or law enforcement.

Part I outlines the meaning and scope of client confidentiality by putting it into the context of the rights enshrined under EU law and the European Convention on Human Rights, as well as the approach taken by the European courts. The paper demonstrates that the confidentiality of communications between clients and lawyers is protected both under the Convention and EU law and accorded particularly high importance by the European courts and other relevant European bodies. Confidentiality is seen not only 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.

The recommendations which follow in Part II seek to ensure respect for that principle by setting out the following main conditions:

- 1. OVERARCHING PRINCIPLE:** 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.
- 2. NEED FOR LEGISLATIVE CONTROL:** all surveillance activities need to be regulated with adequate specificity through primary legislation providing for explicit protection of lawyer-client communications. Also in the case of 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.
- 3. SCOPE OF ADMISSIBLE INTERCEPTION:** 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.
- 4. JUDICIAL AND INDEPENDENT OVERSIGHT:** in the case of communications with lawyers, it is essential that

judicial authorisation is obtained in advance of the imposition of any interception measure. Moreover, there requires to be supervision at all stages of the surveillance procedure by an independent judicial body with the power to terminate interception and/or destroy the material which has been intercepted. To that end, the oversight body must be given adequate powers by law in order to take enforceable decisions.

5. **USE OF INTERCEPTED MATERIAL:** any intercepted material obtained without (prior) judicial authorisation and in violation with 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.
6. **LEGAL REMEDIES AND SANCTIONS:** it is necessary that legal remedies are 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.

# TABLE OF CONTENTS

<b>EXECUTIVE SUMMARY</b> .....	<b>1</b>
<b>INTRODUCTION</b> .....	<b>4</b>
<b>PART I: PROFESSIONAL SECRECY AND LEGAL PROFESSIONAL PRIVILEGE - MEANING AND SCOPE</b> .....	<b>8</b>
Professional secrecy and legal professional privilege .....	9
Without confidentiality, no fair trial .....	10
Case law .....	11
Council of Europe Recommendation No R(2000)21 of 25 October 2000 .....	16
CCBE documents .....	16
<b>PART II: CCBE RECOMMENDATIONS</b> .....	<b>18</b>
Overarching principle .....	19
Need for legislative control .....	19
Scope of admissible interception .....	20
Judicial and independent oversight .....	22
Nature of oversight .....	22
Mandate of the oversight body .....	24
Powers of the oversight bodies .....	24
Use of intercepted material .....	25
Legal remedies and sanctions .....	26
<b>CONCLUSION</b> .....	<b>28</b>
<b>HISTORICAL BACKGROUND - CCBE ACTIONS IN RELATION TO SURVEILLANCE</b> .....	<b>30</b>
<b>BIBLIOGRAPHY</b> .....	<b>32</b>

# INTRODUCTION

#1



In recent years the CCBE has expressed its deep concerns<sup>1</sup> 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 resolution<sup>2</sup> 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 respect<sup>3</sup>. Furthermore, the Council of Europe adopted and released several papers on this issue in 2015. The Parliamentary Assembly adopted a resolution<sup>4</sup> 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 update<sup>5</sup> 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 paper<sup>6</sup> that the interception of communications between lawyers and their clients can undermine the equality of arms and the right to a fair trial.

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 and legal professional privilege by democratic states.<sup>7</sup>

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.

7 For example, in France, the recently-adopted loi sur le renseignement would allow intelligence agencies to use wider spying techniques than

---

**The purpose of this paper is to inform legislators and policy makers about standards that must be upheld in order to ensure that the essential principles of legal professional privilege and professional secrecy are not undermined by practices undertaken by the state and involving the interception of communications and access to lawyers' data for the purpose of surveillance and/or law enforcement.**

The paper does not seek to set out a common European approach as such, for it recognised both that there are important differences between legal professional privilege and professional secrecy and that there may be differences between the understanding of the precise nature and scope of professional secrecy in different jurisdictions. However, whatever the precise approach of different jurisdictions, all member states of the Council of Europe are bound by the European Convention on Human Rights (ECHR) and, additionally, member states of the EU are bound by the provisions of EU law. Therefore, the approach of this paper is to undertake an analysis of the approach of the European Court of Human Rights (ECtHR) and the Court of Justice of the European Union (CJEU), in order to discern minimum standards which apply across Europe. It is accepted, of course, that some jurisdictions may have in place standards which exceed those minimum standards.

For the purpose of this paper, the terms “state” or “government”, are left deliberately broad and imprecise as those terms may refer to the national government itself, to government at different levels (federal, state, or local) to governmental agencies, to tax authorities, to independent agencies carrying out public law functions, to the police, to prosecutors, to intelligence services and to others. The Recommendations are concerned with access by the state in all its forms and manifestations to data and communications between clients and lawyers.

---

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 Parliament recently amended the Act on Police and other acts related to the state secret services, in particular, in relation to the regulation of data surveillance and data retention. These amendments entered into force on 7 February 2016 and include provisions providing unqualified access to information protected by professional secrecy. As a final example, the first draft of the UK's forthcoming Investigatory Powers Bill was denounced as a threat to legal professional privilege by the UK Bars and Law Societies because it would have given 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'. Later drafts, which have incorporated protections in the Bill itself have been criticised as giving inadequate protection.





PART I:  
PROFESSIONAL SECRECY  
AND LEGAL PROFESSIONAL  
PRIVILEGE

MEANING AND SCOPE

#2



## 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<sup>8</sup> 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. Without that trust, the client would not have the assurance that he can be full and frank with his lawyer, which is essential for providing full and accurate legal advice and support and is therefore a crucial guarantee for the fair trial process.

Because of this policy imperative, 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.

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.<sup>9</sup>

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 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. In some jurisdictions professional secrecy has a constitutional status aimed to guarantee fundamental rights such as fundamental right to privacy, right to

<sup>8</sup> ECtHR, *André v France* (18603/03), 2008, §41: "professional secrecy [...] is the basis of the relationship of trust existing between a lawyer and his client."

<sup>9</sup> 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; Legal Professional Privilege and European Case Law, CCBE, Georges-Albert Dal (editor), 2010.

secrecy of communications, right to defence and fair trial. In some jurisdictions, violation of professional secrecy by a lawyer is a criminal offence, it is legislated into the Criminal Code and disclosure of information under the professional secrecy umbrella can be punished with imprisonment. 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.

## 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 and legal professional privilege are thus seen as instruments by which access to justice and the maintenance of the rule of law can be achieved. Indeed, the ECtHR has repeatedly linked the respect for legal professional privilege and professional secrecy to the observance of Articles 6 and 8 of the ECHR. First, 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”*<sup>10</sup>. Furthermore, the Court stated that *“the right of everyone to a fair trial”*<sup>11</sup> is dependent upon the *“relationship of trust between [the lawyer and the client]”*. Secondly, the Court repeatedly highlighted that undermining professional secrecy or legal professional privilege 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”*<sup>12</sup>. 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”*.

Further, in EU Law, Article 4 of the Right of Access to a Lawyer Directive (Directive 2013/48/EU) provides:

*“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.”*

It should be noted that the obligation on member states to respect confidentiality is an absolute one. Although the scope of the directive is limited to criminal law, Article 4 reflects the principle of the inviolability of professional secrecy and legal professional privilege.

In that respect, Recital 34 of Directive 2013/48/EU is inconsistent with the clear terms of Article 4, quoted above.

In particular Recital 34 states that *“This Directive [2013/48/EU] should be without prejudice to a breach of confidentiality which is incidental to a lawful surveillance operation by competent authorities. This Directive should also be without prejudice to the work that is carried out, for example, by national intelligence services to safeguard national security in accordance with*

<sup>10</sup> 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.

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

<sup>12</sup> *Ibid*; also see ECtHR, *Kopp v. Switzerland* (23224/94), 1998.



*Article 4(2) of the Treaty on European Union (TEU) or that falls within the scope of Article 72 TFEU, pursuant to which Title V on an area of Freedom, Security and Justice must not affect the exercise of the responsibilities incumbent upon Member States with regard to the maintenance of law and order and the safeguarding of internal security”.*

By contrast, the substantive provisions of Directive 2013/48/EU allow temporary derogation under Articles 3(5) and (6) and Article 5(3) only. Such temporary derogation is subject to the requirements of Article 8 of the Directive. Should “national security” reasons be argued as an exception or justification per se, this “exception” (especially the basic lack of a clear definition of what constitutes ‘national security’ in itself) would render it impossible for suspects or accused persons to effectively invoke the right of confidentiality of communication with their lawyer.

Therefore, where there is a conflict, the CJEU ought to prefer the clear terms of the substantive provision in Article 4 of Directive 2013/48/EU.

## Case law

There is abundant jurisprudence by the European courts both in Luxembourg and Strasbourg that deals with professional secrecy and legal professional privilege and which highlights the importance of these principles. European legal instruments have also enshrined legal professional privilege and professional secrecy. Additionally, all EU Member States recognise professional secrecy or legal professional privilege 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 and legal professional privilege as being numbered among 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: 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.<sup>13</sup> 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 protected.<sup>14</sup> Legal professional privilege and 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 professional secrecy and its practical implications. The CJEU noted that professional secrecy and

<sup>13</sup> CJEU, *AM & S v Commission* (155/79), 1982, §16 and 18.

<sup>14</sup> *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.

legal professional privilege are closely linked to the concept of the lawyer's role as collaborating in the administration of justice by the courts<sup>15</sup>. The CCBE intervened in the case in support of the applicant.

In *AM&S*, the CJEU defined the scope of professional secrecy/legal professional privilege 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 and legal professional privilege 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 defence<sup>16</sup>.

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.<sup>17</sup> 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.

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 employment. 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*”.<sup>18</sup> 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*”.<sup>19</sup>

15 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.*

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

17 CJEU, *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).

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

19 Ibid.



However, some European countries allow for lawyers, registered with a Bar or Law Society, to work as an in-house lawyer for a company. In many of those jurisdictions, these lawyers are subject to the same or similar professional and ethical rules as other lawyers and enjoy the protection of legal professional privilege or professional secrecy under the relevant national laws.

### **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 (...).”<sup>20</sup>
- “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”<sup>21</sup>
- “(...) 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. (...)”<sup>22</sup>
- “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.”<sup>23</sup>

In the case *Foxley v. The United Kingdom*<sup>24</sup>, which is of particular interest as far as 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

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

<sup>21</sup> ECtHR, *Pruteanu v Romania* (30181/05), 2015, §49. [unofficial translation]

<sup>22</sup> ECtHR, *Niemietz v. Germany* (13710/88), 1992, §37.

<sup>23</sup> ECtHR, *Kopp v. Switzerland* (23224/94), 1998, §74.

<sup>24</sup> ECtHR, *Foxley v. UK* (33274/96), 2000.

case the need for effective safeguards<sup>25</sup> 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:

*“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 *Michaud v France*, the Court stated:

*“118. The result is that while Article 8 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. 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. It is the relationship of trust between them, 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.*

*“119. This additional protection conferred by Article 8 on the confidentiality of lawyer-client relations, and the grounds on which it is based, lead the Court to find that, from this perspective, legal professional privilege, while primarily imposing certain obligations on lawyers, is specifically protected by that Article.”*

In the case of *R.E. v. United Kingdom*<sup>26</sup>, 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:

*“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*<sup>27</sup> and even in *Bykov*<sup>28</sup>. 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.”*

<sup>25</sup> Also see ECtHR, *Niemietz v. Germany* (13710/88), 1992, §37, ECtHR, *Matheron v. France* (57752/00), 2005, §36-43, and ECtHR, *Pruteanu v Romania* (30181/05), 2015, §49.

<sup>26</sup> ECtHR, *R.E. v. United Kingdom* (62498/11), 2015, §131.

<sup>27</sup> ECtHR, *Uzun v. Germany* (35623/05), 2010.

<sup>28</sup> ECtHR, *Bykov v. Russia* (4378/02), 2009.





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. Although this has led to a consistent recognition by the Court of the need for strengthened protection of communications between lawyers and their clients, there have been occasional comments from the Court that exceptions may be permissible, though the nature and extent of any such exceptions is not a matter which has really been explored by the Court.

This leaves unanswered the precise question:

What are the respective contributions which Article 6 and Article 8 of the ECHR can make to ensuring the protection of legal professional privilege and professional secrecy?

It is suggested that the starting point may be to identify what is, and what is not protected by legal professional privilege and professional secrecy. As explained above, no system of legal professional privilege or professional secrecy protects communications where the lawyer is involved in the furtherance of a criminal purpose (the so-called “iniquity exception”). The proper concern of legal protection should be ensuring the inviolability of material which falls within the scope of legal professional privilege or of an obligation of professional secrecy.

In this regard, Article 6 provides a useful filtering mechanism, though it cannot be relied upon to protect every communication comprehended within legal professional privilege and professional secrecy obligations. This is because, although the scope of Article 6 is wide (concerning as it does the right to a fair trial in both criminal and civil matters, with the Article 6 protection extending back to the time of first consultation) it is not all-embracing as there will be legally privileged or secret communications which do not fall within the scope of Article 6 – for example communications regarding contract negotiations or other non-contentious matters. However, if a legally privileged communication, or a communication protected by an obligation of professional secrecy does fall within the ambit of Article 6, then, given the absolute nature of the protection afforded by Article 6, there should be no possibility of interception being permitted.

As explained, however, not every professional secret or privileged communication will enjoy the protection of Article 6, and here the protection of Article 8 becomes essential. Article 8 is qualified, requiring the performance of a balancing act – confidentiality as against the interests of the state in a democratic society of protecting its citizens. However, the clear jurisprudence of the ECtHR as articulated in *Michaud* is to accord heightened protection under Article 8 to communications falling within the protection of legal professional privilege and professional secrecy. It is difficult to see why the heightened protection afforded to communications falling under legal professional privilege or professional secrecy under Article 8 ought not in principle to be equivalent to the protection afforded to legally privileged material and professional secrets falling under the ambit of Article 6.

Therefore, the answer to the question posed above is that in considering a request to permit the interception of communications between a lawyer and a client, the first matter to be determined is whether the communication falls within the proper scope of professional secrecy or legal professional privilege.

If the communication is protected by legal professional privilege or professional secrecy<sup>29</sup>, then the next stage should be to determine whether it falls within the scope of Article 6. If it does, then there should be no possibility of it being intercepted or made subject to surveillance.

<sup>29</sup> As noted above, communications in furtherance of a criminal purpose would not fall within the scope of either legal professional privilege or professional secrecy.

In relation to such privileged communications not falling under Article 6, then, since they would remain private communications, it may be appropriate to undertake a balancing act under Article 8. However, these communications would still fall within the heightened protection afforded under Article 8, and the *Michaud* principles would therefore apply. The application of those principles ought to lead to a result which is similar to the protection afforded under Article 6.

## Council of Europe Recommendation No R(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 importance to the core values of the legal profession in Europe, including professional secrecy and legal professional privilege. For this reason, it is working at the time of the publication of the present paper on finalising a further document, ‘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 other matters, with confidentiality, taking into account the existing jurisprudence of the European courts.

The CCBE also presently 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 foregoing discussion demonstrates that the confidentiality of communications between clients and lawyers is accorded particularly high importance by the European courts and other relevant European bodies. Confidentiality is seen not only 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.**

PART II:  
CCBE RECOMMENDATIONS

#3



The preceding analysis of the law affirms the position of the CCBE that data and communications protected by legal professional privilege and by obligations of professional secrecy are inviolable and not amenable to interception or surveillance. The recommendations which follow seek to ensure respect for that principle.

## Overarching principle

Any direct or indirect surveillance undertaken by the State should fall within the bounds of the rule of law, and, in particular, such surveillance should respect the protection afforded by professional secrecy obligations and legal professional privilege. This protection is, in contentious matters, an essential component in guaranteeing the right to a fair trial, and in all matters is a foundational principle of the rule of law.

## 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 or legal professional privilege in particular. The placing of the mandate of surveillance agencies into primary legislation is a requirement of the ECHR<sup>30</sup>.

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, important areas of regulation and control are not found under the Act, but in non-binding Codes of Practice). Though such codes and guidance may have their place, the substantive protection of professional secrecy and legal professional privilege 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 legal professional privilege and to remove deliberate targeting of client-lawyer communications from the scope of intelligence agencies’ powers.**

As such, the level of protection of professional secrecy or legal professional privilege 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.

<sup>30</sup> 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.”

A cautionary tale is the UK case of *Re McE*<sup>31</sup>. 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 legal professional privilege 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 authorities privileged access to encrypted data.**

Lawyers keep sensitive information (from trade secrets to details of their private life), which were provided to them by clients in confidence 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 EU<sup>32</sup>, 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 process<sup>33</sup>. Therefore, decryption may be only 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.<sup>34</sup>

## Scope of admissible interception

**3.1 Only communications falling outside the scope of professional secrecy or legal professional privilege may be intercepted.**

As discussed above, the first question to be asked when it is sought to intercept communications protected by legal professional privilege or professional secrecy is whether the communication in question falls within the scope of those protections. If it does, then, the next question to

<sup>31</sup> House of Lords, *RE McE*, 2009, UKHL 15.

<sup>32</sup> *Ibid.*

<sup>33</sup> *Ibid.*

<sup>34</sup> *Ibid.*



be asked is whether it falls within the scope of Article 6 ECHR. If it does, then, consistently with Article 6 ECHR, there should be no question of interception being permitted. If it does not, then, it would be necessary to consider the matter under Article 8, where it would enjoy the heightened protection accorded to lawyer-client communications. The result of the heightened protection ought to lead to the same outcome as would result from the application of Article 6.

**3.2 State agencies or law enforcement authorities should be required to use all technological means available to leave material protected by professional secrecy and legal professional privilege 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 legal professional privilege or 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*<sup>35</sup> 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 privilege or 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 legal professional privilege or professional secrecy.

**3.4 Legislative controls should be in place to regulate the process of examining material potentially protected by legal professional privilege or professional secrecy so as to eliminate the risk that it may subsequently be used.**

Notwithstanding the above-mentioned safeguards, there may still be a risk that communications protected by legal professional privilege or 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 legal professional privilege or professional secrecy may accidentally be intercepted, what are the risks of such communications subject to legal professional privilege or 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.

Any accidental interception of communications subject to legal professional privilege or professional secrecy must be notified to the lawyer as soon as reasonably practicable after the body undertaking the surveillance measure becomes aware of it.

<sup>35</sup> Hague Court of Appeal, *Prakken D'Oliveira and others v. The State of The Netherlands*, n. 200 174 280/01, 2015.

# Judicial and independent oversight

## *Nature of oversight*

**4.1 In the event that a warrant is granted for the interception of lawyer-client communications, there requires 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 insufficient<sup>36</sup>. This is particularly true considering that, as pointed out by the ECtHR in 1978<sup>37</sup>, surveillance activities are necessarily carried out without the knowledge of the targeted individual. As a consequence, the person against whom surveillance has been undertaken will be prevented from seeking an effective remedy or from taking a direct part in any review proceedings. It is therefore 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 1978<sup>38</sup> 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 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 role<sup>39</sup>.

**4.3 The judge supervising the surveillance activities should be both financially and politically independent from the executive and should be irremovable<sup>40</sup>. The judge giving approval to a request for interception should not be the same as the judge supervising the implementation of any interception for which permission may have been given.**

It is essential that judicial control is not only exercised independently, without fear or favour, but is seen to have been so exercised. Therefore, it is essential that the supervising judge or other judicial oversight body, should in no way be placed in subordination to or under the effective control or influence of the executive branch of government, the department seeking authorisation or any other similar person or body.

For example, in the Kopp case, the ECtHR<sup>41</sup> considered that it was “astonishing” that a task such as determining whether conversations between a lawyer and his client related to activities other than the giving of legal counsel would be left to a member of the executive without supervision by an independent judge. The only body allowed to take the decision to interfere with the confidentiality of lawyer-client communications must be independent<sup>42</sup>.

36 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.

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

38 Ibid, §56.

39 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; also see § 85 in ECtHR, *Szabó and Vissy v. Hungary* (37138/14), 2015.

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

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

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





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

In order to respect professional secrecy, legal professional privilege, and the confidentiality of sensitive information to its fullest extent, it is essential that judicial authorisation is obtained in advance, and that *a posteriori* judicial review is allowed only in exceptional circumstances. The supervision must be carried out ahead of the implementation of the surveillance measure in order to prevent the unauthorised and, hence, unlawful, surveillance from taking place. The necessity of prior authorisation has previously been clearly set out by the ECtHR in connection with confidentiality of journalistic sources; clearly, the same reasoning also applies to lawyer-client communications.<sup>43</sup>

In a number of jurisdictions, a special role is accorded to the president of the bar or other bar authority. In many of those jurisdictions, the bar authority is involved in supervising the execution of a warrant against an individual lawyer and, in a few, the bar authority is involved in considering, at the time of application for a warrant, whether any of the material is likely to be affected by an obligation of professional secrecy or legal professional privilege and, therefore, falls to be excluded from the ambit of the warrant. The importance of the role of the president of the bar or other bar authority was confirmed by the ECtHR in the *Michaud v. France* case<sup>44</sup> (which in this respect affirmed the earlier jurisprudence of the Court).

Therefore, in those jurisdictions in which such a role is accorded to the president of the bar or other bar authority, the special rules governing the granting or execution of the warrant should continue to be respected.

In all cases, any prior judicial authorisation should be valid only 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 above, *a posteriori* control might be allowed in special circumstances, for example when a severe threat is imminent and no judge is immediately available to grant authorisation. However, it is suggested that this should truly be a measure which should be available only in extremis: to prevent the need arising for *a posteriori* controls, it is suggested that there should be a clear obligation upon the state to take all necessary measures to ensure that the judicial body is, so far as 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 the material which has been intercepted if it finds that the surveillance measures were implemented in an unlawful manner.**

In order to prevent abuse by the surveillance and law enforcement authorities, it is important that an independent and judicial body monitors the implementation of the measure. So as to be comprehensive and efficient, implementation must meet the requirement of compliance with the permission as it was granted including, where applicable, any conditions attached thereto or inherent therein, including conditions as to: (i) the retention of intercepted material, (ii) the sharing of such material with others (be they other agencies or foreign governments), (iii) the selection and analysis of the gathered data, (iv) the circumstances under which it becomes

<sup>43</sup> See *Telegraaf v. Netherlands* (39315/06), 2012: “post factum, whether by the Supervisory Board, [...], cannot restore the confidentiality of journalistic sources once it is destroyed.” § 101.

<sup>44</sup> ECtHR, *Michaud v. France* (12323/11), 2012, and cited case law.

mandatory to notify the subject of the interception about the interception, and (v) disclosure (whether complete or partial) of the material, which has been intercepted and collected.

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 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.

### ***Mandate of the oversight body***

#### **4.6 The oversight body or bodies should be charged with ensuring that surveillance measures do not infringe legal professional privilege or 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: 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 legal professional privilege or professional secrecy. Any oversight should also ensure that existing procedural safeguards in relation to lawyers (for example, the involvement of the president of the bar or other bar authority) are respected.

The body should be satisfied that there are in place appropriate measures to minimise the risk of the accidental recovery of communications protected by legal professional privilege or professional secrecy, to assess objectively whether the material accidentally recovered falls outside the scope of those protections, 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 be required to ensure that the security agency has not infringed any of the foregoing principles.

### ***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 or legal professional privilege, and that there is no way to obtain evidence other than to intercept these communications. In case of *ex post facto* oversight, this would include all intercepted material<sup>45</sup>.
- Any policies, codes of practice and guidelines, drawn up by the State to control and supervise the surveillance of matters which are, or might potentially be, covered by professional secrecy or legal professional privilege.

<sup>45</sup> ECtHR, *Zakharov v. Russia* (47143/06), 2015, §280; see also ECtHR, *Kennedy v. United Kingdom* (26839/05), 2010, §166.



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 mandate<sup>46</sup>. 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 they determine to be unlawful<sup>47</sup>.
- 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 destruction<sup>48</sup> 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 or other organ or agency of the government engaged in prosecution or representing or advising the government in a civil matter.

## Use of intercepted material

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

As repeatedly recognised by the ECtHR<sup>49</sup> professional secrecy and legal professional privilege are inextricably linked with the right to a fair trial. Reference is made to the discussion of case law in section II above. It follows from this that any evidence obtained in violation of the principles of professional secrecy or legal professional privilege should be admissible in court only if the surveillance measure was duly authorised by an independent judicial oversight body as set out in section 4. Furthermore, in order to avoid the risk that the state may make use of lawfully intercepted material in shaping and informing its tactics and approach to legal proceedings whilst keeping the defence in ignorance of that material (and, hence, unable to expose it to judicial scrutiny) material which has been lawfully obtained should both be disclosed to the lawyers acting for the party in respect of whose confidential or privileged data or communications surveillance has taken place and be admissible as evidence in court.

### **5.2 Any lawfully intercepted material should be used solely for the purpose for which the authorisation of the oversight body was granted.**

Any other use would be a violation of the principles of professional secrecy or legal professional privilege, and should accordingly be ruled inadmissible in a court of law.

### **5.3 When intercepted material is ruled unlawful, it should be required to be destroyed.**

This includes all information related to the communications in question, such as the participants, the time, the location, and all other relevant information.

<sup>46</sup> Hague Court of Appeal, *Prakken D'Oliveira and others v. The State of The Netherlands*, n. 200 174 280/01, 2015, 2.9.

<sup>47</sup> See *Telegraaf v. Netherlands* (39315/06), 2012; see also ECtHR, *Kennedy v. United Kingdom* (26839/05), 2010.

<sup>48</sup> ECtHR, *Kennedy v. UK* (26839/05), 2010, §168.

<sup>49</sup> 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.

## Legal remedies and sanctions

**6.1 In order to provide effective legal protection against unlawful surveillance, it is necessary that legal remedies are made available to lawyers and their clients who have been the subject of unlawful surveillance; further, where appropriate, sanctions should be imposed upon those persons and agencies who have undertaken such unlawful surveillance.**

This is a principle established in a Judgment of the ECtHR in 2006 requiring that, at least once the existence of surveillance measures has been disclosed – legal remedies must be made available to the individual concerned<sup>50</sup>. Such remedies should be available equally for surveillance which was unlawful by reason both of never having been authorised and for surveillance originally authorised but carried out in an unlawful manner or having its authorisation removed.

**6.2 In particular, once it has been disclosed that surveillance measures have been undertaken, lawyers and their clients 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 be limited by claimed security interests of the state) and is enforceable against European and national authorities. The ECtHR has indicated<sup>51</sup> that this right to be informed was limited to the extent that the government has the right to balance national security interests against the seriousness of the interference with the citizens' right to respect for private life under Article 8. However, if, as explained above, the material obtained through surveillance falls under the protection of Article 6, then there ought to be no possibility of such a balancing exercise being permissible under Article 8. Unlike Article 8, Article 6 does not permit exceptions. Therefore, there can be no question of allowing such a balancing exercise in cases where the surveillance measure is targeting material covered by legal professional privilege or professional secrecy and falling within Article 6. Furthermore, given the heightened protection afforded to lawyer-client communications under Article 8, the outcome of any balancing exercise, in principle, ought not to differ from the outcome that would result from the application of Article 6.

**6.3 Once the existence of surveillance measures has been disclosed, lawyers and clients who have been affected should be able to challenge the legality of such measures before a judge.**

As a minimum requirement, the following remedies should be made available:

### *Preventive measures*

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 actually be aware that they have been under surveillance. For this reason, they should not be required to prove that they have been under surveillance. Although generally true of any form of surveillance, this may especially be the case where there has been mass surveillance. Because of the likely ignorance on the part of the person concerned of the fact of surveillance, the Venice Commission<sup>52</sup> suggested that a general complaints procedure be established.

<sup>50</sup> ECtHR, *Segerstedt-Wiberg and Others v. Sweden* (62332/00), 2006, §117.

<sup>51</sup> *Ibid.*

<sup>52</sup> Council of Europe Commissioner for Human Rights, 'Democratic and effective oversight of national security services', Issue Paper, Council of Europe, 2015, page 51.



Such an approach has also been taken by the ECtHR in several cases related to governmental surveillance. For example, in the cases of *Zhakarov v. Russia*<sup>53</sup> and *Szabó and Vissy v. Hungary*<sup>54</sup>, the Court made it clear that if applicants could at least possibly have been affected by surveillance, and are not sufficiently protected by national law, they are not obliged to prove that they personally have been under such surveillance. Even if effective national legal protection is provided, the ECtHR desists from the prerequisite of being personally affected. However, the applicant must show that, due to his personal situation, he is potentially at risk of being subjected to surveillance measures.

#### *Request for deletion*

Lawyers and their clients should be able to require the destruction or deletion of any material which has been unlawfully obtained. There is support for such an approach in statement of the Council of Europe Commissioner for Human Rights<sup>55</sup>.

#### *Compensation for both financial and non-pecuniary losses*

Lawyers and their clients should be compensated for any financial damage caused by unlawful surveillance. Additionally, they should be compensated for such non-pecuniary damages as they can establish. This follows the jurisprudence of the ECtHR, which awarded in 2015<sup>56</sup> the amount of 4.500 Euros as just satisfaction (for 'moral prejudice') to a Bulgarian criminal defence lawyer whose communications with his client had been intercepted.

### **6.4 All government authorities which have been found to have been undertaking unlawful surveillance activities should be made liable to having sanctions imposed upon them.**

A comprehensive and effective system of sanctions is required in order to deter future possible infringements.

In relation to digital surveillance in particular, in view of the Council Framework Decision 2005/222/JHA of 24 February 2005 on attacks against information systems, every Member State should have implemented a system of multiple criminal offences in order to cover the various unlawful surveillance methods. The Council Framework Decision allowed for certain exceptions within the national regulations, in particular for minor offences. It is the CCBE's position that any such exceptions are not applicable to the surveillance of lawyer communications as these by definition cannot constitute minor offences.

As a consequence, any unlawful surveillance measure infringing legal professional privilege or professional secrecy should be susceptible to criminal or other appropriate sanctions.

53 ECtHR, *Zhakarov v. Russia* (47143/06), 2015.

54 ECtHR, *Szabó and Vissy v. Hungary* (37138/14), 2016.

55 Council of Europe Commissioner for Human Rights, 'Democratic and effective oversight of national security services', Issue Paper, Council of Europe, 2015, page 51.

56 ECtHR, *Pruteanu v Romania* (30181/05), 2015, §64.

# CONCLUSION

#4



Whilst it is appreciated that it is an obligation of the state to its citizens to ensure their safety and security, legal professional privilege and professional secrecy are essential underpinnings of the rule of law. Where the state seeks to abrogate or erode the principles of legal professional privilege and professional secrecy, even in the name of national security, this constitutes an attack on the rule of law itself.

However, the supposed conflict between, on the one hand, the imperative to protect national security and, on the other hand, the defence of legal professional privilege and professional secrecy is illusory. Both may co-exist as essential components in a mature and fully functioning democratic society which functions in accordance with the rule of law. It has been the purpose of the present paper to lay out with clarity how that end may be achieved.

HISTORICAL BACKGROUND

CCBE ACTIONS IN RELATION TO  
SURVEILLANCE

#5





Ever since the Snowden revelations of 2013, the CCBE has been releasing statements, studies, and letters to denounce the violations of professional secrecy by states and governmental bodies carrying out unlawful surveillance activities.

In early July 2013, the CCBE published its first [statement](#) denouncing the threat represented by state bodies with secret investigatory powers and sophisticated interception technologies.

In October 2013, the CCBE outlined its first [recommendations](#) to safeguard professional secrecy against governmental surveillance.

In December 2013, the CCBE participated in the LIBE Committee Inquiry on Electronic Mass Surveillance of EU citizens. Following a six-month inquiry, the European Parliament approved in March 2014 a [resolution](#) concluding among other matters that it is “crucial that the professional confidentiality privilege of lawyers [...] is safeguarded against mass surveillance activities” and “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.” The same resolution also proposes the introduction of a “Digital Habeas Corpus” to protect fundamental rights including the rule of law and the confidentiality of lawyer-client communications. This resolution was [welcomed by](#) the CCBE.

In April 2014, the CCBE published a [comparative study](#) on governmental surveillance of data held by lawyers in the cloud, outlining the extent to which, in different European jurisdictions, such electronic data is susceptible to governmental access, and the rules and conditions surrounding such access.

Following the continuing important developments in relation to governmental surveillance activities and their impact on lawyers and their clients, the CCBE decided to establish, in March 2015, a separate Working Group on Surveillance.

In March 2015, the CCBE [wrote](#) to the UK Immigration and Security Minister and to the Minister of State at the Foreign and Commonwealth Office. The letters expressed concern about the existence of policies in the UK which permit access by staff of the Security Services there to confidential lawyer-client communications, and seeking clarifications on the matter. Finally, the CCBE [wrote](#) in January 2016 to the Marshal of the Polish Parliament, expressing concerns about a draft law on amendments to the Act on Police and to other acts related to the state secret services, and in particular in relation to the regulation of data surveillance and data retention.

Moreover, the CCBE has been involved in two court cases. First, the CCBE [intervened](#) in 2015 before the French Constitutional Council to defend the confidentiality of communications between lawyers and their clients. It submitted comments as part of the review of the bill on intelligence, and made several suggestions to bring the law into compliance with the right to privacy and the right to legal advice. Second, in May 2015, the CCBE successfully [intervened](#) before The Hague District Court in a challenge brought against the Dutch State by the law firm Prakken d’Oliveira and the Dutch Association of Criminal Defence Lawyers (NVSA). The Court was questioned on the legality of eavesdropping by domestic intelligence agencies on lawyers’ calls and communications. In its verdict delivered on July 1st, the court recognised that the ability to communicate confidentially with a lawyer is a fundamental right which was breached under Dutch surveillance policy. The court therefore ordered the Dutch government to stop all interception of communications between clients and their lawyers under the current regime within six months. In response, the Dutch State fast-tracked an appeal against the judgement. In turn, on 25 August 2015, the CCBE challenged the grounds of the appeal, and on 27 October 2015 the Dutch Court of Appeal dismissed all the grounds of appeal alleged by the Dutch State and [upheld the lower court ruling](#) banning the surveillance of communications protected by legal professional secrecy.

# BIBLIOGRAPHY

#6



### *Article 29 Working Party*

- [Joint Statement of the European Data Protection Authorities Assembled in the Article 29 Working Party](#), 26 November 2014.
- [Working Document on surveillance of electronic communications for intelligence and national security purposes](#), 5 December 2014.

### *CCBE*

- [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.
- [CCBE Comparative Study on Governmental Surveillance of Lawyers' Data in the Cloud](#), 2014.
- [CCBE Statement on mass electronic surveillance by government bodies \(including of European lawyers' data\)](#), 2013.
- [Charter of Core Principles of the European Legal Profession and Code of Conduct for European Lawyers](#), 2013.
- [Legal Professional Privilege and European Case Law](#), CCBE, Georges-Albert Dal (editor), 2010.

### *Council of Europe*

- Council of Europe Parliamentary Assembly, [Resolution 2045](#), 21 April 2015.
- 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
- Council of Europe Commissioner for Human Rights, '[Democratic and effective oversight of national security services](#)', Issue Paper, Council of Europe, 2015.
- Council of Europe [Recommendation](#) Nr. R (2000) 21 on the freedom of exercise of the Profession of lawyer, 25 October 2000.
- Council of Europe, [European Convention on Human Rights](#), 1950.

---

### *European legislation*

- [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 \(OJ L 294/1\).](#)
- [Charter of Fundamental Rights of the European Union, 2000.](#)
- [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 \(OJ L 77/36\).](#)
- [Council Directive 77/249/EEC of March 22, 1977, to facilitate the effective exercise by lawyers of freedom to provide services \(OJ L 78/17\).](#)

### *European Parliament*

- European Parliament [Resolution](#) on the follow-up to the European Parliament resolution of 12 March 2014 on the electronic mass surveillance of EU citizens, 29 October 2015.
- LIBE Committee of the European Parliament [Study](#), 'The law enforcement challenges of cybercrime: are we really playing catch-up?', October 2015.
- LIBE Committee of the European Parliament [Study](#), 'Cybersecurity in the European Union and Beyond: Exploring the Threats and Policy Responses', September 2015.
- 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.

### *United Nations*

- United Nations Human Rights Council [Resolution](#), 'The right to privacy in the digital age', 24 March 2015.



## Reports and Articles

- [Ten standards for oversight and transparency of national intelligence services](#), University of Amsterdam, Institute for Information Law, 2015.
- Peter Carter QC and Bankim Thanki QC, 'Legal Professional Privilege – The Law in Summary', Briefing Paper, 2015.
- 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.
- '[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.
- '[Update of the Edward's Report on the professional secret, confidentiality and legal professional privilege in Europe](#)', CCBE, 2003.
- Eric Gippini-Fournier, '[Legal Professional Privilege in Competition Proceedings Before the European Commission: Beyond the cursory Glance](#)', Fordham International Law Journal, Volume 28, Issue 4, 2004.
- '[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.

## Case Law

### European Court of Human Rights

- ECtHR, [Szabó and Vissy v. Hungary](#) (37138/14), 2016.
- ECtHR, [R.E. v. United Kingdom](#) (62498/11), 2015.
- ECtHR, [Pruteanu v Romania](#) (30181/05), 2015.
- ECtHR, [Zakharov v. Russia](#) (47143/06), 2015.
- ECtHR, [Michaud v. France](#) (12323/11), 2012.
- ECtHR, [Telegraaf v. Netherlands](#) (39315/06), 2012.
- ECtHR, [Kennedy v. United Kingdom](#) (26839/05), 2010.
- ECtHR, [Saknovskiy v. Russia](#) (21272/03), 2010.
- ECtHR, [Uzun v. Germany](#) (35623/05), 2010.
- ECtHR, [Bykov v. Russia](#) (4378/02), 2009.
- ECtHR, [André v France](#) (18603/03), 2008.

- ECtHR, Moiseyev v. Russia (62936/00), 2008.
- ECtHR, Zagaria v. Italy (58295/00), 2007.
- ECtHR, Segerstedt-Wiberg and Others v. Sweden (62332/00), 2006.
- ECtHR, Öcalan v. Turkey (46221/99), 2005.
- ECtHR, Matheron v. France (57752/00), 2005.
- ECtHR, Lanz v. Austria (24430/94), 2002.
- ECtHR, Brennan v. United Kingdom (39846/98), 2001.
- ECtHR, Foxley v. UK (33274/96), 2000.
- ECtHR, Domenichini v. Italy (15943/90), 1996.
- ECtHR, Kopp v. Switzerland (23224/94), 1998.
- ECtHR, Campbell v. United Kingdom (13590/88), 1992.
- ECtHR, Niemietz v. Germany (13710/88), 1992.
- ECtHR, S. v. Switzerland (12629/87), 1991.
- ECtHR, Bonzi v. Switzerland (7854/77), 1978.
- ECtHR, Klass and Others v. Germany (5029/71), 1978.

#### Court of Justice of the European Union

- CJEU, European Commission v Italian Republic (387/05), 2009.
- CJEU, Ordre des barreaux francophones et germanophone and others v. Conseil des ministres (305/05), 2007.
- CJEU, AM & S v Commission (155/79), 1982.

#### Domestic case-law

- Hague Court of Appeal, Prakken D'Oliveira and others v. The State of The Netherlands, n. 200 174 280/01, 2015.
- House of Lords, Re McE, UKHL 15, 2009.
- Czech Constitutional Court, Pl. ÚS 24/10, 2011.