Conseil des barreaux européens
Council of Bars and Law Societies of Europe
Association internationale sans but lucratif
Rue Joseph II, 40 /8 – 1000 Bruxelles
T. : +32 (0)2 234 65 10
Email : ccbe@ccbe.eu – www.ccbe.eu

Recommandations du CCBE sur la protection du secret professionnel dans le cadre des activités de surveillance

28/04/2016

RÉSUMÉ

« L'obligation de l'avocat relative au secret professionnel sert les intérêts de l'administration de la justice comme ceux du client. Elle doit par conséquent bénéficier d'une protection spéciale de l'État »

– Article 2.3 du Code de déontologie du CCBE

Le but du présent document est d'informer les législateurs et décideurs européens concernant les normes à respecter pour s'assurer que les principes essentiels du secret professionnel ne soient pas remis en cause par les pratiques des États à des fins de surveillance ou d'application de la loi et impliquant l'interception des communications et l'accès aux données protégées par le secret professionnel des avocats.

La première partie expose la signification et la portée du principe de confidentialité des clients dans le contexte des droits consacrés par la législation européenne et la Convention européenne des droits de l'homme, ainsi que l'approche adoptée par les tribunaux européens. Le document démontre que la confidentialité des communications entre les avocats et leurs clients est protégée en vertu de la Convention et du droit de l'UE, et qu'elle revêt une importance particulière aux yeux des juridictions européennes et d'autres organes européens concernés. La confidentialité est considérée non seulement comme étant le devoir de l'avocat, mais également comme un droit de l'homme fondamental du client. Sans la certitude de la confidentialité, il ne peut y avoir de confiance, élément essentiel du bon fonctionnement de l'administration de la justice et de l'état de droit.

Les recommandations qui suivent dans la deuxième partie visent à garantir le respect de ce principe en énonçant les conditions principales suivantes :

1. Principe fondamental : Tout recours, direct ou indirect, de l'État à la surveillance s'inscrit dans les limites de l'état de droit et doit respecter le principe selon lequel les données et les communications couvertes par le secret professionnel sont inviolables et ne peuvent être sujettes à des interceptions ou à une surveillance.

2. Besoin de contrôle législatif : Toutes les activités de surveillance doivent être réglementées avec un degré de précision suffisant par la législation primaire prévoyant une protection explicite des communications avocat-client. Dans les cas où les activités de surveillance seraient confiées à des sociétés privées, le gouvernement doit toujours garder le contrôle complet de l'ensemble du processus de surveillance. Le décryptage des données sécurisées ne peut être autorisé que s'il est juridiquement défini et qu'il suit une procédure régulière à la suite d'une autorisation judiciaire.

3. Champ d'application des exceptions tolérées : Seules les communications sortant du champ d'application du secret professionnel peuvent être interceptées. Aucun système ne protège les communications lorsque l'avocat est impliqué dans la poursuite d'activités criminelles. L'objectif devrait être d'assurer l'inviolabilité des informations relevant du secret professionnel. Par conséquent, tout mandat d'interception des communications avec un avocat ne doit être accordé que s'il existe des preuves convaincantes que les informations recherchées ne relèvent pas du secret professionnel.

4. Contrôle juridictionnel indépendant : Dans le cas de communications avec des avocats, une autorisation judiciaire est indispensable avant la mise en place de toute mesure d'interception. En outre, un organe judiciaire indépendant pouvant mettre fin à l'interception, mais aussi détruire les informations interceptées, doit contrôler tous les stades de la mise en place des mesures de surveillance. La loi doit à cette fin accorder des pouvoirs appropriés à cet organe pour qu'il puisse prendre des décisions exécutoires.

5. Utilisation des informations interceptées : Toute information interceptée sans autorisation judiciaire (préalable) et portant atteinte au principe du secret professionnel doit être jugée irrecevable devant un tribunal et sa destruction doit être exigée. Toute information obtenue légalement doit être recevable comme élément de preuve.

6. Voies de recours et sanctions : Les voies de recours sont indispensables pour les avocats et leurs clients victimes de surveillance illégale, tout comme l'instauration d'un système de sanctions. Les avocats et leurs clients ont le droit d'être informés quant aux données recueillies lors d'activités de surveillance directe ou indirecte une fois que la prise de ces mesures a été divulguée.

Table des matières

INTRODUCTION

Ces dernières années, le CCBE a plusieurs fois exprimé sa profonde inquiétude[1] à la suite des révélations relatives aux méthodes employées par les services de renseignements nationaux. Ces préoccupations sont principalement liées aux pouvoirs d'enquête secrets ou insuffisamment contrôlés dont disposent les organismes publics, ainsi qu'à l'exercice de ces pouvoirs au moyen de technologies de pointe et de grande envergure en matière de surveillance et d'interception. Ces moyens permettent d'accéder massivement en continu et de manière indiscriminée aux données de communication des citoyens. Bien qu'elles puissent contribuer à lutter contre le terrorisme et le crime organisé, ces technologies sont à l'origine de nombreux problèmes nouveaux, en particulier concernant la légalité lorsqu'il y a atteinte aux droits de l'homme fondamentaux.

Cette atteinte devient d'autant plus dangereuse lorsque les gouvernements consultent les données et les communications qui bénéficient d'une protection spéciale accordée par la loi, ce qui est clairement le cas dans le cadre des communications entre les avocats et leurs clients. Dans tous les États membres de l'Union européenne, la législation prévoit une protection contre la divulgation de renseignements communiqués entre un avocat et son client en toute confidentialité. Sans cette protection, le fonctionnement même de l'Etat de droit serait compromis.

L'accès à la justice, le droit à un procès équitable, le droit au respect de la vie privée peuvent, entre autres, être touchés. Ces droits sont protégés par de nombreux instruments juridiques nationaux et internationaux, comme la Convention européenne des droits de l'homme (CEDH) et la Charte des droits fondamentaux de l'Union européenne. Porter atteinte à la confidentialité des communications avocat-client, qu'elle repose ou non sur le concept du secret professionnel ou celui du *legal professional privilege* dans certaines juridictions, signifie violer les obligations internationales, renier les droits des accusés et compromettre intégralement la nature démocratique de l'État.

De nombreux organismes internationaux le reconnaissent. En octobre 2015, par exemple, le parlement européen a adopté une résolution[2] de suivi sur la surveillance électronique de masse des citoyens de l'Union européenne. Celle-ci souligne que les droits des citoyens européens doivent être protégés de toute surveillance des communications avec leur avocat. En outre, le parlement a explicitement invité la Commission européenne à adopter une communication à cet égard[3]. En 2015, le Conseil de l'Europe a adopté et publié plusieurs documents consacrés à cette question. Son assemblée parlementaire a adopté une résolution[4] mettant en exergue le fait qu'intercepter les communications confidentielles des avocats compromettait les droits fondamentaux et, en particulier, le droit au respect de la vie privée et à un procès équitable. La commission de Venise a, quant à elle, publié une mise à jour[5] d'un précédent rapport sur le contrôle démocratique des agences de collecte de renseignements d'origine électromagnétique dans lequel elle reconnaît que les communications avocat-client doivent bénéficier d'une protection élevée, notamment grâce à des garanties procédurales et d'un contrôle externe strict. Enfin, le commissaire aux droits de l'homme a élaboré un document thématique[6] dans lequel il souligne que l'interception des communications entre les avocats et leurs clients peut compromettre le principe d'égalité des armes et le droit à un procès équitable.

Par conséquent, l'importance de ce principe ne peut être sous-estimée. Pourtant, il est aujourd'hui grandement menacé. L'évolution récente que connaissent de nombreux pays européens compromet la

---

[1] Déclaration du CCBE sur la surveillance électronique de masse par des organismes gouvernementaux (notamment les données des avocats européens), 2013 ; Étude comparative du CCBE sur la surveillance gouvernementale des données des avocats hébergées dans le nuage, 2014 ; Les avocats européens saluent les mesures du Parlement européen à l'encontre de la surveillance électronique de masse, 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 ; Une cour néerlandaise soutient la décision de l'instance inférieure interdisant la surveillance des communications des avocats après l'intervention réussie du CCBE, 2015 ; Le CCBE intervient auprès du Conseil constitutionnel pour défendre la confidentialité des échanges avocat-client, 2015.

[2] Résolution du Parlement européen, « Suivi de la résolution du Parlement européen du 12 mars 2014 sur la surveillance électronique de masse des citoyens de l'Union européenne », 29 octobre 2015.

[3] Ibid, §43.

[4] Assemblée parlementaire du Conseil de l'Europe, Résolution 2045, 21 avril 2015, §4.

[5] Commission de Venise du Conseil de l'Europe, « Mise à jour du rapport de 2007 sur le contrôle démocratique des services de sécurité et rapport sur le contrôle démocratique des agences de collecte de renseignements d'origine électromagnétique », 2015, §18 et 106.

[6] Commissaire aux droits de l'homme du Conseil de l'Europe, « La surveillance démocratique et effective des services de sécurité nationale », document thématique, Conseil de l'Europe, 2015, 27.

protection traditionnellement accordée au secret professionnel et au *legal professional privilege* par les États démocratiques[7].

Ce document a pour but d'informer les législateurs et décideurs concernant les normes à respecter pour s'assurer que les principes essentiels du secret professionnel ne soient pas remis en cause par les pratiques des États impliquant l'interception des communications et l'accès aux données des avocats à des fins de surveillance ou d'application de la loi.

Ce document ne souhaite pas définir une approche européenne commune en tant que telle, car il reconnaît qu'il existe des différences importantes entre le *legal professional privilege* et le secret professionnel. Il prend également en compte le fait que la compréhension de la nature et du champ d'application exacts du secret professionnel varie selon les juridictions. Néanmoins, quelle que soit l'approche des différentes juridictions, chaque État membre du Conseil de l'Europe est lié par la Convention européenne des droits de l'homme (CEDH), tandis que les États membres de l'Union européenne sont liés par les dispositions de la législation européenne. Le présent document entreprend donc une analyse de l'approche de la Cour européenne des droits de l'homme (CEDH) et de la Cour de justice de l'Union européenne (CJUE) de façon à dégager les normes minimales en vigueur en Europe. Le document reconnaît, bien sûr, l'existence de normes plus élevées dans certaines juridictions.

Aux fins du présent document, les termes « États » et « gouvernement » sont délibérément utilisés dans un sens large et peu précis puisqu'ils se réfèrent tous deux au gouvernement national en soi, mais aussi aux différents niveaux de gouvernement (fédéral, central, ou local), aux organismes gouvernementaux, aux autorités fiscales, aux organismes indépendants chargés de la fonction publique, à la police, aux procureurs, aux services de renseignement, etc. Ces recommandations concernent surtout l'accès de l'État, sous toutes ses formes et manifestations, aux données et aux communications entre les clients et leurs avocats.

[7] Par exemple, en France, la loi sur le renseignement, récemment adoptée, autorise les agences de renseignement à avoir recours à des techniques d'espionnage plus élargies que jamais, mais aussi à accéder aux métadonnées de toutes les communications (dont celles entre clients et avocats). Aux Pays-Bas, après un recours formulé par un cabinet soutenu par le CCBE contre l'État néerlandais, en juin 2015, le tribunal a ordonné au gouvernement de cesser toute interception des communications entre les clients et les avocats jusqu'à ce qu'il puisse fournir assez de garanties, dont un contrôle indépendant, jusqu'alors largement insuffisant. La Diète (le parlement polonais) a récemment amendé la loi sur la police ainsi que d'autres lois relatives aux services secrets nationaux et plus particulièrement la réglementation de la surveillance et de la conservation des données. Ces amendements sont entrés en vigueur le 7 février 2016 et prévoient des dispositions accordant un accès sans réserve aux informations relevant du secret professionnel. Comme dernier exemple, au Royaume-Uni, la première version du projet de loi à venir sur les pouvoirs d'enquête a été qualifié de menace pour le secret professionnel par les barreaux britanniques, car il donnerait un large accès à des informations confidentielles sur le client sans donner de protection réglementaire au secret professionnel en se cantonnant à un « code de bonnes pratiques » non législatif. Les versions suivantes, qui ont prévu des protections dans le projet de loi lui-même, ont été critiquées comme offrant des protections inadaptées.

PARTIE I : SECRET PROFESSIONNEL– IMPORTANCE ET CHAMP D'APPLICATION

Le secret professionnel et le legal professional privilege

L'efficacité des avocats dans leur travail de défense des droits de leurs clients dépend de la certitude que la confidentialité des communications entre les avocats et leurs clients est garantie. Ce principe est reconnu à travers l'Europe entière depuis des siècles. En substance, sans cette garantie, il y a un risque que le client soit dépourvu de la confiance[8] nécessaire à une divulgation entière et franche à son avocat et l'avocat, à son tour, serait dépourvu des informations nécessaires (et qui peuvent s'avérer importantes) pour prodiguer des conseils exhaustifs à son client ou le représenter efficacement. Sans cette confiance, le client n'est pas assuré de pouvoir être exhaustif et franc dans ses communications avec son avocat ; un principe essentiel afin d'offrir des conseils juridiques et un soutien complets et précis, ce qui constitue une garantie déterminante d'un procès équitable.

En raison de cet impératif, des dispositions existent dans tous les pays européens de manière à assurer la protection du droit et du devoir de l'avocat de maintenir la confidentialité des affaires des clients. Dans certaines juridictions européennes, cette confidentialité est préservée en attribuant à ces communications la protection du secret professionnel (*legal professional privilege*), dans d'autres juridictions en les considérant comme des secrets professionnels. Les deux approches servent néanmoins le même objectif : la protection des informations créées dans le cadre de la relation avocat-client dans le but de donner ou de recevoir des conseils ou une représentation juridique (qu'il y ait litige ou non) dans tout type de procédure judiciaire, à caractère civil ou pénal.

Bien qu'une analyse détaillée du *legal professional privilege* et du secret professionnel ne relève pas de la portée du présent document, il est utile de comprendre l'approche générale large de chacune de ces deux notions[9].

La notion de *legal professional privilege* attribue aux communications avocat-client un privilège de confidentialité, qui appartient au client. L'avocat est tenu à l'obligation découlant de la relation avocat-client de maintenir la confidentialité de toutes les communications, entre le client et lui-même, relevant de sa fonction d'avocat mandaté par le client, à moins que le client ne renonce à cette confidentialité. Cette obligation civile se traduit en une obligation déontologique. Il est toutefois important de comprendre que le privilège ne concerne pas les communications qui sortent du cadre de la relation entre le client, en tant que client, et l'avocat, en tant qu'avocat dudit client. Il ne concerne par exemple pas les communications entre un individu et un avocat, qui pourrait éventuellement agir en tant qu'avocat du client dans certains domaines, à propos d'un sujet qui ne se situerait pas dans le cadre de la relation professionnelle. Voici un exemple clair : si l'avocat communique, non pas en tant qu'avocat chargé de la défense pénale d'un client soupçonné du cambriolage d'une banque ou d'un acte terroriste, mais comme complice, pour planifier avec le client le cambriolage d'une banque ou un acte terroriste, il est évident que cette communication ne relève pas du *legal professional privilege*. Dans les juridictions de *common law*, cette exception porte généralement le nom de *iniquity exception*, bien qu'il soit important de noter qu'il ne s'agit pas réellement d'une « exception » : il s'agit plutôt d'une question qui ne relève pas, en premier lieu, du champ d'application du *legal professional privilege*.

Lorsque le fondement est le secret professionnel, l'obligation de maintenir la confidentialité des communications est absolue. Cette obligation repose directement sur les épaules de l'avocat et le client ne peut même pas y renoncer, dans la plupart des juridictions. Dans certaines juridictions, le secret professionnel a un statut constitutionnel visant à garantir les droits fondamentaux tels que le droit à l'intimité de la vie privée, le droit au secret des communications, le droit à la défense et à un procès équitable. Dans certaines juridictions, la violation du secret professionnel par un avocat constitue une infraction pénale définie dans le code pénal et la divulgation de renseignements relevant du secret professionnel est passible d'une peine d'emprisonnement. En dépit de ces différences majeures, la notion de secret professionnel partage avec celle de *legal professional privilege* le principe que son champ d'application exclut le cas de l'avocat engagé avec le client dans la poursuite d'activités criminelles.

---

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

[9] Une discussion complète est disponible dans les rapports suivants : 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.

Toute référence au « secret professionnel » dans le présent document doit être considérée, sauf indication contraire, comme comprenant à la fois le secret professionnel et le *legal professional privilege*.

Pas de procès équitable sans secret professionnel

La plupart des systèmes juridiques partagent le principe commun qu'un refus du droit du justiciable à la confidentialité, à savoir le droit du citoyen d'être protégé de toute divulgation de ses communications avec son avocat, pourrait priver les justiciables de l'accès effectif à des conseils juridiques et à la justice. Le secret professionnel est donc considéré comme un instrument qui conditionne l'accès à la justice et le maintien de l'état de droit. En effet, la CEDH a maintes fois lié le respect du secret professionnel au respect des articles 6 et 8 de la CEDH. Tout d'abord, la Cour a estimé que « *le droit, pour l'accusé, de communiquer avec son avocat hors de portée d'ouïe d'un tiers figure parmi les exigences élémentaires du procès équitable dans une société démocratique et découle de l'article 6 par. 3 c) (art. 6-3-c) de la Convention*[10] ». En outre, la Cour a déclaré que « *le droit du respect du justiciable à un procès équitable*[11] » dépend de la « *relation de confiance entre [l'avocat et le client]* ». En second lieu, la Cour a souligné à plusieurs reprises que saper le secret professionnel peut constituer une violation de l'article 8, qui protège le droit au respect de la vie privée et familiale. En effet, l'article « *accorde une protection renforcée aux échanges entre les avocats et leurs clients*[12] ». La Cour poursuit : « *Cela se justifie par le fait que les avocats se voient confier une mission fondamentale dans une société démocratique : la défense des justiciables. Or un avocat ne peut mener à bien cette mission fondamentale s'il n'est pas à même de garantir à ceux dont il assure la défense que leurs échanges demeureront confidentiels* ».

Ailleurs dans la législation européenne, l'article 4 de la directive relative au droit d'accès à un avocat (directive 2013/48/UE) prévoit que :

> *« Les États membres respectent la confidentialité des communications entre les suspects ou les personnes poursuivies et leur avocat dans l'exercice du droit d'accès à un avocat prévu par la présente directive. Ces communications comprennent les rencontres, la correspondance, les conversations téléphoniques et toute autre forme de communication autorisée par le droit national. »*

Il convient de noter que l'obligation des États membres de respecter le secret professionnel est absolue. Même si le champ d'application de la directive est limité au droit pénal, l'article 4 reflète le principe d'inviolabilité du secret professionnel.

À cet égard, le considérant 34 de la directive 2013/48/UE n'est pas cohérent vis-à-vis des termes précis de l'article 4 cité ci-dessous :

Le considérant 34 indique en particulier que : « *La présente directive devrait s'entendre sans préjudice du non-respect du principe de confidentialité lié à une opération de surveillance licite effectuée par les autorités compétentes. Elle devrait également s'entendre sans préjudice des activités qui sont menées, par exemple, par les services de renseignement nationaux, pour sauvegarder la sécurité nationale conformément à l'article 4, paragraphe 2, du traité sur l'Union européenne ou qui relèvent de l'article 72 du traité sur le fonctionnement de l'Union européenne, en vertu duquel le titre V relatif à l'espace de liberté, de sécurité et de justice ne doit pas porter atteinte à l'exercice des responsabilités qui incombent aux États membres pour le maintien de l'ordre public et la sauvegarde de la sécurité intérieure*. »

En revanche, les dispositions de fond de la directive 2013/48/UE permettent une dérogation temporaire uniquement en vertu des articles 3 (5) et (6) et de l'article 5 (3). Ces dérogations temporaires sont soumises aux obligations prévues à l'article 8 de la directive. Dans le cas où un motif de « sécurité nationale » serait en soi avancé à titre d'exception ou de justification, cette « exception » (en particulier en l'absence totale de définition claire de « sécurité nationale ») rendrait impossible pour des personnes

[10] CEDH, *S. c. Suisse* (12629/87), 1991, §48. Voir également CEDH, *Domenichini c. Italie* (15943/90), 1996, §39; CEDH, *Öcalan c. Turquie* (46221/99), 2005, §1333; CEDH, *Moiseyev c. Russie* (62936/00), 2008, §209; CEDH, *Campbell c. Royaume-Uni* (13590/88), 1992, §§ 44-48.
[11] CEDH, *Michaud c. France* (12323/11), 2012, §117-8.
[12] Ibid ; voir également CEDH, *Kopp c. Suisse* (23224/94), 1998.

suspectes ou accusées d'invoquer correctement le droit au secret professionnel ou à la communication avec leur avocat.

Par conséquent, en cas de conflit, la CJUE devrait préférer les termes clairs repris dans la disposition de fond de l'article 4 de la directive 2013/48/UE.

La jurisprudence

La jurisprudence des cours européennes de Luxembourg et Strasbourg traitant du secret professionnel et soulignant l'importance de ce principe est abondante. Les instruments juridiques européens ont également consacré le secret professionnel. En outre, tous les États membres de l'UE reconnaissent le secret professionnel comme l'un des principaux objectifs et principes de la réglementation de la profession d'avocat, dont la violation constitue dans certains États membres de l'UE non seulement une violation professionnelle, mais également une infraction pénale. En outre, le CCBE, dans sa propre Charte des principes essentiels de l'avocat européen, son Code de déontologie des avocats européens, et de nombreux autres documents, consacre le secret professionnel comme comptant parmi les valeurs fondamentales de la profession d'avocat européenne. Les principales décisions des tribunaux européens, les instruments juridiques européens ainsi que les documents du CCBE qui s'y rapportent sont repris plus en détail ci-dessous.

Cour de justice de l'Union européenne : l'affaire AM&S

Dans l'affaire *AM & S c. Commission*, la Cour de justice de l'Union européenne (CJUE) a reconnu que le maintien de la confidentialité de certaines communications entre avocat et client constitue un principe général du droit qui est commun aux droits de tous les États membres et, à ce titre, un droit fondamental protégé par le droit de l'UE[13]. La Cour a jugé que *« tout justiciable doit avoir la possibilité de s'adresser en toute liberté à son avocat, dont la profession même comporte la tâche de donner, de façon indépendante, des avis juridiques à tous ceux qui en ont besoin »*, et que, par conséquent, la confidentialité de certaines communications avocat-client doit être protégée[14]. Le secret professionnel peut être invoqué tout aussi bien par des personnes physiques que par des entreprises pouvant faire l'objet d'une enquête de la Commission, quelle que soit leur forme juridique. Cette confidentialité couvre tous les documents dont dispose l'avocat ou le client et s'applique aux communications provenant de l'un ou de l'autre.

La décision de la CJUE était d'une importance particulière, et l'est toujours, étant donné qu'elle a confirmé la protection des communications confidentielles (qui a été contestée jusqu'en 1978) et défini la portée du secret professionnel et ses implications pratiques. La CJUE a noté que le secret professionnel est étroitement lié à la notion du rôle de l'avocat, qui participe à l'administration de la justice par les tribunaux[15]. Le CCBE est intervenu dans l'affaire à l'appui du requérant.

Dans l'arrêt *AM&S*, la CJUE a défini la portée du secret professionnel dans le système de l'Union européenne sur la base des traditions juridiques communes aux États membres. Elle a interprété le règlement 17 comme protégeant la confidentialité des communications écrites entre un avocat et ses clients, sous réserve de deux conditions, l'incorporation des éléments de cette protection qui se sont révélés être communs aux lois des États membres en 1982, à savoir que de telles communications : (i) sont réalisées pour les besoins et dans les intérêts des droits de la défense du client et (ii) émanent d'avocats indépendants qui sont qualifiés pour exercer dans un pays de l'EEE.

---

[13] CJUE, *AM & S c. Commission* (155/79), 1982, §16 et 18.

[14] Ibid. Bien qu'AM&S ait fait l'objet d'inspections, il est généralement reconnu que les principes établis dans cette affaire sont également applicables aux demandes de renseignements de la Commission. L'affaire AM&S est née d'un différend au sujet de la confidentialité d'une série de documents trouvés dans les locaux d'AM&S, une société britannique, au cours d'une enquête relative à une entente. La société a refusé de divulguer certains des documents au motif qu'il s'agissait de communications écrites confidentielles entre un avocat et son client. La Commission européenne a publié une décision exigeant d'AM&S de produire ces documents.

[15] Ibid, §24 : *Quant à la deuxième condition, il y a lieu de préciser que l'exigence relative à la position et à la qualité d'avocat indépendant, que doit revêtir le conseil dont émane la correspondance susceptible d'être protégée, procède d'une conception du rôle de l'avocat, considéré comme collaborateur de la justice et appelé à fournir, en toute indépendance et dans l'intérêt supérieur de celle-ci, l'assistance légale dont le client a besoin. Cette protection a pour contrepartie la discipline professionnelle, imposée et contrôlée dans l'intérêt général par les institutions habilitées à cette fin. Une telle conception répond aux traditions juridiques communes aux États membres et se retrouve également dans l'ordre juridique communautaire, ainsi qu'il résulte de l'article 17 du statut de la cour CEE et CEEA ainsi que de l'article 20 du statut de la cour CECA.*

En ce qui concerne la première exigence, la CJUE a souligné qu'il faut veiller à ce que les droits de la défense puissent être exercés en totalité dans le cadre des procédures d'enquête de la Commission, et que la protection de la confidentialité des communications écrites avocat-client est un corollaire essentiel des droits de la défense. Elle a donc reconnu que toutes les communications écrites échangées après l'ouverture de la procédure doivent être protégées. Toutefois, étant donné que la Commission peut ouvrir une enquête avant l'ouverture formelle de la procédure, la Cour a jugé, afin de ne pas décourager les sociétés de prendre des conseils juridiques le plus tôt possible, que la protection du secret professionnel s'étend à toute communication écrite antérieure ayant un lien avec l'objet de la procédure. Les conseils juridiques sont considérés comme constituant une étape « préparatoire » dans la défense de la société[16].

Conformément à la deuxième exigence établie dans l'arrêt *AM&S*, le secret professionnel s'applique uniquement aux communications écrites émanant d'avocats indépendants qui ont le droit d'exercer leur profession dans l'un des États membres, qu'il s'agisse ou non de l'État membre dans lequel réside le client[17]. Cela signifie que, par définition, les communications concernant des avocats qualifiés dans des pays tiers tels que les États-Unis ne seront pas considérées comme confidentielles aux fins du régime juridique de l'UE, quand bien même ces avocats seraient établis dans l'UE.

En outre, la notion « d'avocat indépendant » n'englobe, selon la Cour, aucun expert juridique lié à son client par un rapport d'emploi. La Cour a estimé que cette exigence concernant la position et le statut d'un conseiller juridique repose sur la « *conception du rôle de l'avocat, considéré comme collaborateur de la justice et appelé à fournir, en toute indépendance et dans l'intérêt supérieur de celle-ci, l'assistance légale dont le client a besoin* »[18]. Malgré sa référence à « *la discipline professionnelle, imposée et contrôlée dans l'intérêt général par les institutions habilitées à cette fin* » comme étant la contrepartie de la protection du secret professionnel, la Cour a jugé dans l'affaire *AM&S*, d'après les critères communs trouvés dans les législations nationales des États membres, qu'un document contenant des conseils juridiques et échangé entre un avocat et son client est protégé de toute divulgation uniquement si l'avocat est « indépendant », « *c'est-à-dire non lié au client par un rapport d'emploi* »[19].

Néanmoins, certains pays européens permettent aux avocats inscrits à un barreau de travailler au sein d'une société. Dans beaucoup de ces juridictions, ces avocats sont soumis aux mêmes règles professionnelles et déontologiques que les avocats externes ou à des règles similaires. Ils jouissent alors de la protection du secret professionnel en vertu du droit national applicable.

Cour européenne des droits de l'homme

Les arrêts de la CEDH ont également reconnu le droit à la confidentialité des communications entre avocat et client en vertu de l'article 8 (« droit au respect de la vie privée et familiale ») ou de l'article 6 (« droit à un procès équitable ») de la CEDH.

L'article 8 établit clairement le droit de chacun au respect de sa correspondance. Il protège la confidentialité des communications quel que soit le contenu de la correspondance en question et quelle qu'en soit la forme. Toute limitation de ce droit doit être conforme à la loi, poursuivre un but légitime et être nécessaire dans une société démocratique pour atteindre l'objectif concerné. Ce dernier aspect a été examiné par la Cour dans de nombreuses décisions. Il convient toutefois de noter que, si une limitation du droit prévu à l'article 8 est possible de la manière expliquée ci-dessus, ce n'est pas le cas du droit prévu à l'article 6.

La jurisprudence de la CEDH est particulièrement riche en ce qui concerne la confidentialité des communications avocat-client et se développe de plus en plus au fil des ans. Voici quelques décisions importantes fixant des principes généraux à observer au sujet de la relation avocat-client :

[16] Fordham International Law Journal, Volume 28, Issue 4, page 1009, 2004.
[17] CJUE, *AM & S c. Commission* (155/79), §25. Les limites de cette protection doivent être déterminées en se référant aux règles sur l'exercice de la profession d'avocat en vertu la directive 77/249/CEE du Conseil du 22 mars 1977 tendant à faciliter l'exercice effectif de la libre prestation de services par les avocats (JO L 78/17) et de la directive 98/5/CE du Parlement européen et du Conseil du 16 février 1998 tendant à faciliter l'exercice permanent de la profession d'avocat dans un État membre autre que celui où la qualification a été acquise (JO L 77/36).
[18] CJUE, *AM & S c. Commission* (155/79), §24 et 27.
[19] Ibid.

- *« (…) Si un avocat ne pouvait s'entretenir avec son client sans une telle surveillance et en recevoir des instructions confidentielles, son assistance perdrait beaucoup de son utilité, alors que le but de la Convention consiste à protéger des droits concrets et effectifs (…)*[20]*. »*

- *« (…) l'interception des conversations d'un avocat avec son client porte incontestablement atteinte au secret professionnel, qui est la base de la relation de confiance qui existe entre ces deux personnes*[21]*. »*

- *« (…) il convient de se rappeler à cet égard que dans le cas d'un avocat, pareille intrusion peut se répercuter sur la bonne administration de la justice et, partant, sur les droits garantis par l'article 6 (art. 6). (…) ».*[22]

- *« Surtout, en pratique, il est pour le moins étonnant de confier cette tâche à un fonctionnaire du service juridique des PTT, appartenant à l'administration, sans contrôle par un magistrat indépendant. Cela d'autant plus que l'on se situe dans le domaine délicat de la confidentialité des relations entre un avocat et ses clients, lesquelles touchent directement les droits de la défense. »*[23]

Dans l'affaire *Foxley c. Royaume-Uni*[24], qui est particulièrement intéressante au sujet des communications entre avocats et clients, la Cour a jugé que l'article 8 avait été violé par l'interception de la correspondance du requérant avec ses avocats. La Cour a souligné dans l'affaire la nécessité de garanties efficaces[25] pour assurer une atteinte minimale au droit au respect de la correspondance et a également rappelé que la relation avocat-client est par principe confidentielle et que la correspondance dans ce contexte, quel qu'en soit l'objet, porte sur des questions à caractère privé et confidentiel.

> *"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)".*

Dans l'affaire *Michaud c. France (2012),* la Cour a déclaré :

> *118. Il en résulte que si l'article 8 protège la confidentialité de toute « correspondance » entre individus, il accorde une protection renforcée aux échanges entre les avocats et leurs clients. Cela se justifie par le fait que les avocats se voient confier une mission fondamentale dans une société démocratique : la défense des justiciables. Or un avocat ne peut mener à bien cette mission fondamentale s'il n'est pas à même de garantir à ceux dont il assure la défense que leurs échanges demeureront confidentiels. C'est la relation de confiance entre eux, indispensable à l'accomplissement de cette mission, qui est en jeu. En dépend en outre, indirectement, mais nécessairement, le respect du droit du justiciable à un procès équitable, notamment en ce qu'il comprend le droit de tout « accusé » de ne pas contribuer à sa propre incrimination.*
>
> *119. Cette protection renforcée que l'article 8 confère à la confidentialité des échanges entre les avocats et leurs clients et les raisons qui la fondent conduisent la Cour à constater que, pris sous cet angle, le secret professionnel des avocats – qui toutefois se décline avant tout en obligations à leur charge – est spécifiquement protégé par cette disposition.*

[20] CEDH, *S. c. Suisse* (12629/87), 1991, §48.
[21] CEDH, *Pruteanu c. Roumanie* (30181/05), 2015, §49
[22] CEDH, *Niemietz c. Allemagne* (13710/88), 1992, §37.
[23] CEDH, *Kopp c. Suisse* (23224/94), 1998, §74.
[24] CEDH, *Foxley c. Royaume-Uni* (33274/96), 2000.
[25] Voir également CEDH, *Niemietz c. Allemagne* (13710/88), 1992, §37, CEDH, *Matheron c. France* (57752/00), 2005, §36-43 et CEDH, *Pruteanu c. Roumanie* (30181/05), 2015, §49

Dans l'affaire *R.E. c. Royaume-Uni*[26], la CEDH a conclu à une violation de l'article 8 de la convention découlant de la surveillance d'un entretien entre un avocat et son client dans un commissariat de police et a estimé ce qui suit (au paragraphe 131) :

> *"The Court therefore considers that the surveillance of a legal consultation constitutes an extremely high degree of intrusion into a person's right to respect for his or her private life and correspondence; higher than the degree of intrusion in Uzun*[27] *and even in Bykov*[28]*. 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."*

La tendance de la CEDH a été d'aborder la question de l'interception des communications avocat-client en regardant à travers le prisme du droit de l'article 8 à la confidentialité des communications, en accordant aux communications avocat-client un degré de protection plus élevé que celui accordé aux autres communications privées. Bien que cela ait conduit à une reconnaissance cohérente par la Cour du besoin d'une protection renforcée des communications entre les avocats et leurs clients, certains commentaires occasionnels de la Cour ont indiqué que des exceptions pouvaient être autorisées, sans que la nature et la portée de ces exceptions n'aient véritablement fait l'objet d'un examen par la Cour.

Une question demeure néanmoins sans réponse ;

> Quelles contributions l'article 6 et l'article 8 de la CEDH peuvent-ils apporter pour garantir la protection du secret professionnel ?

Il convient tout d'abord d'identifier les éléments couverts par le secret professionnel. Tel que susmentionné, aucune forme de secret professionnel ne couvre les communications dans lesquelles l'avocat est impliqué dans la poursuite d'activités criminelles (« *iniquity exception* »). Le véritable objectif de la protection juridique devrait être de garantir l'inviolabilité des informations relevant du secret professionnel.

À cet égard, l'article 6 prévoit un mécanisme de filtrage utile, même s'il ne permet pas de protéger toutes les communications relevant du secret professionnel. La raison en est que, bien que le champ d'application de l'article 6 soit vaste (il concerne le droit à un procès équitable tant dans les affaires pénales que civiles, la protection prévue par l'article 6 s'étend jusqu'au moment de la première consultation), il n'est pas général, puisque le domaine des communications protégées par le secret professionnel est plus vaste que le champ d'application de l'article. C'est le cas notamment des communications relatives aux négociations de contrats ou à d'autres affaires n'impliquant pas de litiges. Cependant, si une communication couverte par le secret professionnel relève de l'article 6, alors, en raison du caractère absolu garanti par l'article 6, aucune forme d'interception ne peut être autorisée.

Tel que susmentionné, toutes les communications relevant du secret professionnel ne sont pas protégées par l'article 6, c'est pourquoi la protection accordée par l'article 8 est essentielle. L'article 8 est limité, car il exige de trouver un équilibre entre la confidentialité et la poursuite des intérêts de l'État dont l'objectif, dans une société démocratique, est de protéger ses citoyens. Néanmoins, la jurisprudence de la CEDH a clairement démontré la protection accrue garantie par l'article 8 aux communications couvertes par le secret professionnel. Il est difficile de comprendre pourquoi la protection accrue accordée par l'article 8 aux communications protégées par le secret professionnel ne devrait pas être, en principe, équivalente à la protection garantie à ces communications par l'article 6.

Par conséquent, pour répondre à la question posée ci-dessus, lors de l'examen d'une demande d'autorisation pour intercepter des communications avocat-client, il convient en premier lieu de déterminer si celles-ci relèvent du champ d'application du secret professionnel.

[26] CEDH, *R.E. c. Royaume-Uni* (62498/11), 2015.
[27] CEDH, *Uzun c. Royaume-Uni* (35623/05), 2010.
[28] CEDH, *Bykov c. Russie* (4378/02), 2009.

Le cas échéant[29], l'étape suivante consiste à déterminer si ces communications relèvent de l'article 6. Si tel est le cas, ces communications ne peuvent en aucune manière être interceptées ou faire l'objet d'une surveillance.

Les communications ne relevant pas de l'article 6 demeurant des communications privées, il serait alors approprié de trouver un équilibre en vertu de l'article 8. Ces communications pourraient alors encore bénéficier de la protection accrue accordée en vertu de l'article 8, et les principes de la jurisprudence *Michaud* seraient dès lors applicables. L'application de ces principes devrait avoir des effets similaires à la protection prévue par l'article 6.

La Recommandation No. R(2000)21 du 25 octobre 2000 du Conseil de l'Europe

Outre la jurisprudence abondante des cours européennes sur les communications confidentielles, il est important d'évoquer la Recommandation Rec (2000) 21 du 25 octobre 2000 du Conseil de l'Europe sur la liberté d'exercice de la profession d'avocat en Europe qui prévoit que *« toutes les mesures nécessaires devraient être prises pour veiller au respect du secret professionnel des relations entre avocats et clients. Des exceptions à ce principe devraient être permises seulement si elles sont compatibles avec l'État de droit. »* (Principe I, paragraphe 6) et que *« les avocats devraient respecter le secret professionnel conformément à la législation interne, aux règlements et à la déontologie de leur profession. Toute violation de ce secret, sans le consentement du client, devrait faire l'objet de sanctions appropriées. »* (Principe III, paragraphe 2.)

Les documents du CCBE

Le CCBE accorde une grande importance aux valeurs fondamentales de la profession d'avocat en Europe, notamment le secret professionnel. C'est pourquoi il travaille à l'heure actuelle sur un autre document, « Vers un modèle de code de déontologie » qui servira de guide aux barreaux nationaux dans l'examen de leurs propres règles nationales. Le code modèle traitera, entre autres, du secret professionnel et de la prise en compte de la jurisprudence des tribunaux européens.

Actuellement, deux documents clés du CCBE concernent le secret professionnel.

- Premièrement, la Charte des principes essentiels de l'avocat européen du CCBE, adoptée le 24 novembre 2006, énonce dix principes essentiels qui sont l'expression de la base commune à toutes les règles nationales et internationales qui régissent la profession d'avocat Les principes de la Charte prévoient :

  « Principe (b) - le respect du secret professionnel et de la confidentialité des affaires dont il a la charge :

  Il est de l'essence de la profession d'avocat que celui-ci se voie confier par son client des informations confidentielles, qu'il ne dirait à personne d'autre – informations les plus intimes ou secrets commerciaux d'une très grande valeur – et que l'avocat doit recevoir ces informations et toutes autres sur base de la confiance. Sans certitude de confidentialité, la confiance ne peut exister. La Charte souligne la nature duale de ce principe – respecter la confidentialité n'est pas uniquement un devoir de l'avocat, c'est aussi un droit fondamental du client. Les règles relatives au secret professionnel interdisent l'utilisation contre le client des communications entre un avocat et son client. Dans certains systèmes juridiques, le droit au secret est vu comme bénéficiant uniquement au client, alors que dans d'autres, le secret professionnel peut aussi nécessiter que l'avocat garde secrètes à l'égard de son client les communications confidentielles de l'avocat de l'autre partie. Ce principe (b) comprend tous les concepts qui y ont trait, à savoir le secret professionnel, la confidentialité et le legal professional privilege. L'obligation au secret à l'égard du client subsiste après que l'avocat a cessé d'agir en son nom. »

Il est important de noter la Charte du CCBE n'est pas conçue comme un code de déontologie. Elle a néanmoins vocation à s'appliquer à l'Europe tout entière, au-delà des territoires des États membres, associés et observateurs du CCBE. La Charte a notamment pour objet de venir en aide aux barreaux qui luttent pour faire reconnaître leur indépendance ; elle vise également à accroître la compréhension

[29] Comme indiqué plus haut, les communications effectuées dans la poursuite d'activités criminelles ne sont pas concernées par le secret professionnel.

de l'importance du rôle de l'avocat dans la société ; elle s'adresse tant aux avocats eux-mêmes qu'aux décideurs et au public en général.

- Deuxièmement, le Code de déontologie des avocats européens du CCBE, qui date du 28 octobre 1988 et a été révisé pour la dernière fois en 2006, contient également une disposition sur le secret professionnel :

  « 2.3. Secret professionnel

  2.3.1. Il est de la nature même de la mission de l'avocat qu'il soit dépositaire des secrets de son client et destinataire de communications confidentielles. Sans la garantie de confidentialité, il ne peut y avoir de confiance. Le secret professionnel est donc reconnu comme droit et devoir fondamental et primordial de l'avocat.

  L'obligation de l'avocat relative au secret professionnel sert les intérêts de l'administration de la justice comme ceux du client. Elle doit par conséquent bénéficier d'une protection spéciale de l'État.

  2.3.2. L'avocat doit respecter le secret de toute information confidentielle dont il a connaissance dans le cadre de son activité professionnelle.

  1.3.3. Cette obligation au secret n'est pas limitée dans le temps.

  2.3.4. L'avocat fait respecter le secret professionnel par les membres de son personnel et par toute personne qui coopère avec lui dans son activité professionnelle. »

Contrairement à la Charte, le Code est un texte contraignant dans tous les États membres du CCBE : tous les avocats membres des barreaux de ces pays (que ces barreaux soient des membres effectifs, associés ou observateurs du CCBE) sont tenus au respect du Code dans leurs activités transfrontalières à l'intérieur de l'Union européenne, de l'Espace économique européen, de la Confédération helvétique comme des pays associés et observateurs.

Les précédents débats démontrent que la confidentialité des communications entre clients et avocats fait l'objet d'une attention particulièrement élevée de la part des tribunaux européens et des autres organismes européens concernés. Le secret professionnel n'est pas seulement considéré comme étant le devoir de l'avocat, il est également considéré comme étant un droit de l'homme fondamental du client. Sans certitude de confidentialité, la confiance ne peut exister. Cette confiance est essentielle au bon fonctionnement de l'administration de la justice et à l'État de droit.

PARTIE II : RECOMMANDATIONS DU CCBE

L'analyse préalable du droit confirme la position du CCBE selon laquelle les données et les communications couvertes par le secret professionnel sont inviolables et ne peuvent être sujettes à des interceptions ou à une surveillance. Les recommandations suivantes ont pour but de garantir le respect de ce principe.

1. Principe fondamental

Tout recours, direct ou indirect, de l'État à la surveillance s'inscrit dans les limites de l'état de droit, et cette surveillance doit respecter la protection garantie par le secret professionnel. Dans le cadre de litiges, cette protection est une composante essentielle du respect du droit à un procès équitable et demeure, dans tous les cas, un principe fondateur de l'état de droit.

2. Besoin de contrôle législatif

2.1 Toutes les activités de surveillance doivent être réglementées de manière transparente et avec les précisions nécessaires (en définissant clairement la « sécurité nationale », par exemple).

Dans une société démocratique, les services de sécurité ne peuvent ni manquer de transparence, ni omettre de rendre des comptes, ni agir au-delà d'un véritable cadre légal contraignant. Sans de tels contrôles, il existe un risque de manquement arbitraire aux droits de l'homme en général et au secret professionnel en particulier. L'inscription de la fonction des agences de renseignement dans la législation primaire est une exigence posée par la CEDH[30].

Dans les États où il existe un cadre réglementaire, d'importantes protections ont parfois été inscrites non pas dans la législation primaire, mais dans des codes de bonnes pratiques non contraignants, des lignes directrices et autres textes semblables (au Royaume-Uni, par exemple, en vertu du *Regulation of Investigatory Powers Act 2000,* d'importants domaines de régulation et de contrôle ne sont repris que dans des codes de bonnes pratiques non contraignants). Bien que ces codes et principes aient leur place, une protection concrète du secret professionnel doit être consacrée par la législation primaire, obligeant ainsi les services secrets à rendre des comptes devant les tribunaux quant à la manière d'exécuter leurs fonctions.

2.2 La législation régissant les activités de surveillance doit prévoir une protection explicite du secret professionnel et doit mettre la surveillance ciblée et délibérée des communications client-avocat hors de portée du pouvoir des agences de renseignement.

En tant que tel, le niveau de protection du secret professionnel prévu par la loi doit toujours être le plus élevé, que les mesures de surveillance soient entreprises à des fins répressives (par exemple, par la police ou les services judiciaires) ou pour la protection de la sécurité nationale (par les agences de renseignement nationales). La nature intrusive et les effets potentiels des deux types d'activité sur les droits des individus à un procès équitable sont identiques et nécessitent par conséquent un niveau de protection juridique tout aussi élevé.

L'affaire *Re McE*[31], au Royaume-Uni, constitue une bonne mise en garde. Dans cette affaire, la Chambre des Lords a interprété l'absence de protections spécifiques du secret professionnel comme permettant tacitement et légalement d'intercepter des informations confidentielles. Par conséquent (à l'occasion de l'interprétation du texte législatif), il a été jugé que le Parlement avait porté atteinte au secret professionnel. Cette décision a été sévèrement critiquée, mais il est significatif que le texte de la

[30] Conseil de l'Europe, Commission de Venise, Mise à jour du rapport de 2007 sur le contrôle démocratique des services de sécurité et rapport sur le contrôle démocratique des agences de collecte de renseignements d'origine électromagnétique, 2015, page 18 : *« La plupart des États démocratiques, conscients de l'impact de la surveillance stratégique sur les droits individuels, ont défini au moins une partie de la fonction de ROEM dans la législation primaire. […] Cet énoncé du mandat du service compétent correspond également à une exigence posée par la CEDH. »*

[31] Chambre des Lords, *Re McE*, UKHL, 2009.

législation proposée et débattue au Parlement reproduise, à cet égard, la formulation du *2000 Act* et, avec elle, la volonté d'intercepter des informations couvertes par le *legal professional privilege*.

2.3 La législation doit prévoir des garanties suffisantes dans les cas où les activités de surveillance seraient partiellement ou entièrement confiées à des sociétés privées de façon à garantir que le gouvernement garde toujours le contrôle complet et que l'Etat soit toujours pleinement responsable de l'ensemble du processus de surveillance, des données, et de leur utilisation.

Confier les activités de surveillance à des sociétés privées peut libérer la police, les services judiciaires ou de la sécurité nationale de leur responsabilité et les décharger sur des petites sociétés qui ne peuvent être tenues responsables des interdictions constitutionnelles. Par conséquent, les sociétés privées impliquées dans le processus de surveillance doivent être soumises à des règles déontologiques et des exigences de confidentialité strictes ainsi qu'à des obligations contractuelles de transparence et d'octroi au gouvernement de l'accès aux techniques et modalités d'organisation régissant les activités de surveillance. Les organismes publics doivent avoir accès aux connaissances et aux ressources suffisantes pour pouvoir conserver le contrôle intégral de toutes les activités de surveillance sous-traitées par des sociétés privées.

2.4 La législation ne doit pas empêcher les avocats de protéger correctement la confidentialité des communications avec leurs clients (par des méthodes de cryptage, par exemple) et ne doit donner ni aux organismes publics ni aux forces de l'ordre un quelconque accès privilégié aux données cryptées.

Les avocats détiennent des informations sensibles confiées par leurs clients en toute confidentialité (allant du secret commercial aux détails de la vie privée) et qui ne peuvent être divulguées. Les avocats sont dès lors particulièrement vulnérables aux attaques illégales perpétrées par le gouvernement ou les pirates informatiques. Des moyens de protection cryptographiques leur sont dès lors nécessaires. Le droit à la protection des données concerne également la sécurité des données, garantie par l'article 8 de la CEDH[32] ainsi que par la Convention de 1981 du Conseil de l'Europe pour la protection des données et la décision-cadre relative à la protection des données en 2008. Néanmoins, l'absence de sécurité des données peut toucher une multitude d'autres droits tels que les droits économiques, le respect de la vie privée et la bonne administration de la justice[33]. Le décryptage des communications entre avocats et clients ne peut, par conséquent, être autorisé à moins d'être défini légalement et d'être précédé d'une décision émanant d'un juge indépendant, au cas par cas, et selon une procédure régulière[34].

3. Champ d'application des interceptions tolérées

3.1 Seules les communications sortant du champ d'application du secret peuvent être interceptées.

Tel que susmentionné, la première question à se poser en cas d'interception de communications relevant du secret professionnel est : la communication entre-t-elle dans le champ d'application de ces protections ? Le cas échéant, relève-t-elle de l'article 6 de la CEDH ? Si oui, conformément à l'article 6 de la CEDH, aucune forme d'interception ne peut être tolérée. Dans le cas contraire, il convient alors d'examiner l'affaire à la lumière de l'article 8 qui prévoit une protection accrue pour les communications avocat-client. Cette protection accrue doit conduire au même résultat que l'application de l'article 6.

3.2 Les organismes publics et forces de l'ordre doivent être tenus d'utiliser tous les moyens technologiques possibles afin de maintenir les informations relevant du secret hors du champ d'application des opérations de surveillance.

Il convient de distinguer la surveillance ciblée de la surveillance non ciblée. Dans le cas de cette dernière, il peut y avoir un risque d'interception accidentelle de communications soumises au secret professionnel. Aux Pays-Bas, par exemple, il existe un système de reconnaissance du numéro de

[32] Ibid.
[33] Ibid.
[34] Ibid.

téléphone capable d'identifier les numéros des avocats et ainsi cesser toute surveillance. Dans l'affaire *Prakken d'Oliveira*[35], l'utilisation de ce système par les services de sécurité a été longuement débattue.

3.3 L'interception des données ne doit être autorisée que lorsque l'organe souhaitant mettre en place la surveillance peut démontrer qu'il y a des raisons impérieuses donnant lieu à un degré de suspicion suffisant pour justifier cette interception.

Le processus d'interception ne doit pas être utilisé de manière à collecter des informations sur la base de seuls indices ou soupçons. La surveillance ne doit pas cibler des informations relevant du secret professionnel. Aucun mandat d'interception ne peut donc être accordé dans le but d'intercepter des communications auxquelles participe un avocat à moins qu'il y ait des preuves suffisantes que les données ne seront pas protégées par le secret professionnel.

3.4 La loi doit strictement régir la procédure d'examen des informations susceptibles d'être protégées par le secret professionnel dans le but de réduire les risques qu'elles soient utilisées ultérieurement.

Nonobstant les garanties susmentionnées, les communications protégées par le secret professionnel peuvent être interceptées par accident. Par conséquent, les agences de collecte de renseignements doivent être transparentes quant aux informations qu'elles collectent, y compris la manière et la mesure dans laquelle elles ont accidentellement intercepté des communications potentiellement protégées par le secret professionnel. Elles doivent également être transparentes quant aux risques que comporte l'interception de ces communications couvertes par le secret professionnel, aux garanties mises en œuvre pour empêcher que cela se produise et, si cela se produit accidentellement, indiquer quelles mesures seront prises pour empêcher ces informations d'être utilisées.

Toute interception accidentelle de communications relevant du secret professionnel doit être signalée à l'avocat dans les meilleurs délais dès que l'organisme réalisant la surveillance en prend conscience.

4. Contrôle juridictionnel indépendant

Nature des contrôles

4.1 Dans le cas où il est sollicité ou requis d'intercepter des communications entre avocats et clients, des contrôles au cas par cas sont exigés à toutes les étapes de la procédure de surveillance.

Dans une société démocratique, un contrôle externe est indispensable. En effet, compter uniquement sur un contrôle interne et gouvernemental (comme une autorisation ministérielle) des activités de surveillance ne suffit pas[36]. Cela est d'autant plus vrai dans le cas où les activités de surveillance sont nécessairement menées sans connaître l'individu ciblé (comme le soulignait la CEDH en 1978[37]). Par conséquent, l'objet de la surveillance se verra dépourvu de recours effectif et tenu à l'écart de toute procédure de recours. Il est dès lors essentiel que les procédures en place garantissent les droits des individus.

4.2 Le contrôle doit être confié à une entité judiciaire.

Le contrôle juridictionnel constitue une protection efficace contre l'arbitraire : seul un juge peut offrir la garantie de l'indépendance, de l'impartialité et de la procédure adéquate nécessaires. De fait, la CEDH considérait en 1978[38] que, dans un domaine où les abus sont relativement fréquents dans les affaires individuelles et où les conséquences peuvent être si dévastatrices pour la société démocratique dans son ensemble, il est souhaitable, en principe, de confier le contrôle à un juge. La Cour a lié ce principe

[35] Cour d'appel de La Haye, *Prakken d'Oliveira et autres c. Pays-Bas*, n. 200 174 280/01, 2015.
[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. Voir aussi : Commission de Venise, Mise à jour du rapport de 2007 sur le contrôle démocratique des services de sécurité et rapport sur le contrôle démocratique des agences de collecte de renseignements d'origine électromagnétique, 2015, p.31
[37] CEDH, *Klass et autres c. Allemagne* (5029/71), 1978, §55.
[38] Ibid, §56.

à celui de l'état de droit. En outre, la séparation des pouvoirs doit être suffisamment garantie. Ce rôle de contrôle quasi judiciaire[39] ne doit donc pas être confié à un organe parlementaire ou administratif.

4.3 Le juge chargé du contrôle des activités de surveillance doit être inamovible[40], et indépendant à la fois financièrement et politiquement du pouvoir exécutif. Le juge qui approuvera une demande d'interception ne devra pas être le même que le juge contrôlant l'exécution de toute interception autorisée.

Il est primordial que le contrôle juridictionnel soit exercé non seulement de manière indépendante, sans craindre ni favoriser qui que ce soit, mais aussi que cette indépendance soit visible. Il est donc capital que le juge ou l'organe judiciaire de contrôle ne soit en aucun cas subordonné au contrôle effectif ou à l'influence du pouvoir exécutif, qu'il s'agisse du gouvernement, du service à l'origine de la demande d'autorisation, ou toute autre personne ou organe similaire.

Par exemple, dans l'affaire *Kopp c. Suisse*, la CEDH[41] a jugé « étonnant » qu'une tâche consistant à déterminer si les conversations entre clients et avocats étaient liées à des activités autres que rendre des avis juridiques ait été assignée à un membre du pouvoir exécutif sans aucun contrôle d'un juge indépendant. Le seul organe autorisé à prendre la décision de porter atteinte à la confidentialité des communications entre les avocats et leurs clients doit être indépendant[42].

4.4 Une autorisation externe et, si nécessaire, assortie de conditions est indispensable avant la mise en place de toute mesure d'interception.

Pour protéger pleinement le secret professionnel et la confidentialité des informations sensibles, il est indispensable d'établir l'autorisation judiciaire préalable (*a priori*) comme étant la norme. Les contrôles juridictionnels *a posteriori* ne peuvent lui être substituée que dans des circonstances exceptionnelles. Le contrôle doit être mené avant la mise en place des mesures de surveillance de manière à interdire une surveillance non autorisée et donc illégale. La nécessité d'obtenir une autorisation préalable a clairement été établie par la CEDH dans le cadre de la confidentialité des sources journalistiques. Il est clair que le même raisonnement s'applique aux communications entre clients et avocats[43]. En outre, cette autorisation judiciaire préalable doit être valide durant une période de temps définie et raisonnable afin de permettre une évaluation régulière de la situation et de la légalité des mesures imposées.

Dans certaines juridictions, un rôle spécial est accordé au bâtonnier ou à une autre autorité du barreau. Dans un grand nombre d'entre elles, l'autorité du barreau est impliquée dans le contrôle de l'exécution de la réquisition à l'encontre d'un avocat et, dans certaines de ces juridictions, l'autorité du barreau est également amenée à déterminer si, dans la durée de la réquisition, des documents peuvent relever du secret professionnel et, ainsi, être exclus de sa portée. L'importance du rôle du bâtonnier ou de toute autre autorité du barreau a été confirmée par la CEDH dans l'affaire *Michaud c. France*[44] (confirmant ainsi la jurisprudence de la Cour).

Par conséquent, dans les juridictions où un tel rôle est attribué au bâtonnier ou à une autre autorité du barreau, les règles spécifiques régissant la délivrance ou l'exécution de la réquisition doivent être maintenues.

Dans tous les cas, l'autorisation judiciaire préalable ne doit être valide que durant un délai raisonnable et défini de manière à assurer une évaluation régulière de la situation et la légalité des mesures imposées.

Tel que susmentionné, un contrôle *a posteriori* ne peut lui être substitué que dans certaines circonstances, comme en cas de menace grave et imminente et qu'aucun juge n'est disponible dans l'immédiat pour délivrer une autorisation. Cette mesure devrait néanmoins être appliquée uniquement en dernier ressort : pour anticiper le besoin d'un contrôle postérieur, il est préférable que l'État soit

---

[39] Commission de Venise, « mise à jour du rapport de 2007 sur le contrôle démocratique des services de sécurité et rapport sur le contrôle démocratique des agences de collecte de renseignements d'origine électromagnétique », 2015, p. 32 ; voir également § 85 de la CEDH *Szabó et Vissy c. Hongrie* (37 138/14), 2015.
[40] En fonction des règles et modalités prévues, telles qu'une faute grave ou des problèmes de santé.
[41] CEDH, *Kopp c. Suisse* (23 224/94), 1998.
[42] Cour d'appel de La Haye, *Prakken d'Oliveira et autres c. Pays-Bas*, n. 200 174 280/01, 2015.
[43] Voir Telegraaf c. Pays-Bas (39 315/06), 2012 : « *post factum, whether by the Supervisory Board, [...], cannot restore the confidentiality of journalistic sources once it is destroyed.* » § 101
[44] CEDH, *Michaud c. France* (12323/11), 2012 et jurisprudence précitée.

soumis à une véritable obligation de prendre toutes les mesures nécessaires dans le but de s'assurer que l'organe judiciaire soit, autant que possible, disponible à tout moment.

4.5 Une fois l'autorisation accordée, un organe juridictionnel distinct, répondant aux mêmes exigences que celui qui délivre les autorisations, doit à son tour contrôler la mise en place des mesures d'interception autorisées. Cet organe doit pouvoir mettre fin à l'interception, mais aussi détruire les informations interceptées s'il s'avère que les mesures de surveillances ont été mises en place illégalement.

De manière à prévenir d'éventuels abus de la part des autorités de surveillance et des forces de l'ordre, il est important qu'un organe judiciaire indépendant veille à la mise en place des mesures. Pour être inclusive et efficace, la mise en place doit respecter l'autorisation telle qu'elle a été accordée et, le cas échéant, les conditions assorties ou inhérentes, dont les suivantes : (I) la détention d'informations interceptées ; (II) le partage de ces informations (que ce soit avec d'autres organismes ou des gouvernements étrangers) ; (III) la sélection et l'analyse des données recueillies ; (IV) les circonstances dans lesquelles il devient obligatoire de notifier la personne concernée par l'interception et (V) la divulgation (complète ou partielle) des informations interceptées et collectées.

Bien qu'il faille un contrôle juridictionnel à la fois préalable à l'exercice de la surveillance (par l'imposition d'obligations légales de disposer d'un mandat judiciaire pour exercer ce pouvoir) et postérieur (par exemple, en traitant une plainte déposée contre les agences de sécurité pour acte illicite dans une affaire donnée), ces contrôles ne doivent pas pour autant être exercés par le même organe (un juge unique peut délivrer un mandat et un tribunal spécial peut exercer le contrôle postérieur), à condition que chacun remplisse les conditions énoncées plus haut.

Compétence de l'organe de contrôle

4.6 Le ou les organes de contrôle doivent s'assurer que les mesures de surveillance ne portent atteinte au secret professionnel.

À cette fin, lorsqu'il y a lieu d'autoriser une interception, l'organe de contrôle doit s'efforcer de vérifier la légalité et l'efficacité de la mesure de surveillance : dans le cas de communications impliquant des avocats, il doit exiger des preuves irréfutables que la communication n'entre pas dans le champ d'application des informations protégées par le secret. Tout contrôle doit veiller au respect des garanties procédurales en lien avec l'avocat (par exemple, la participation du bâtonnier ou d'une autre autorité du barreau).

L'organe doit être certain que des mesures appropriées sont mises en place afin de minimiser le risque de récupération accidentelle de communications protégées par le secret, d'évaluer objectivement si les informations récupérées accidentellement entrent ou non dans le champ d'application de ces protections et limiter et contrôler toute éventualité que des informations confidentielles et obtenues par accident soient utilisées.

L'organe auquel incombe le contrôle *a posteriori* est également tenu de s'assurer que l'agence de sécurité n'a violé aucun des principes qui précèdent.

Pouvoirs des organes de contrôle

4.7 La loi doit accorder des pouvoirs contraignants, appropriés, et proportionnels à l'organe de contrôle pour qu'il s'acquitte de son rôle. Il doit pouvoir prendre des décisions exécutoires en tout état de cause.

Pour prendre des décisions en tout état de cause, l'organe doit avoir accès à :

- Toutes les preuves nécessaires pour établir que les communications en question ne sont pas couvertes par le secret professionnel. Ces communications doivent, en outre, être la seule manière d'obtenir des preuves. En cas de contrôle *a posteriori*, toutes les informations interceptées sont concernées[45].

[45] CEDH, *Zakharov c. Russie* (47 143/06), 2015, §280 ; voir aussi CEDH, *Kennedy c. Royaume-Uni* (26 839/05), 2010, §160.

- Toute politique, tout code de bonnes pratiques et toutes instructions, circulaires, etc… conçues par l'État dans le but de contrôler et superviser la surveillance d'affaires qui relèvent, ou peuvent relever, du secret professionnel.
- Aux ordres donnés par le gouvernement aux organismes privés afin d'obtenir des informations.

Il est important de souligner que si les organes de contrôle n'ont aucunement le pouvoir de mettre fin à la surveillance des communications entre clients et avocats, ils ne seront pas en mesure de remplir leur mission[46]. Par conséquent, pour pouvoir prendre des décisions exécutoires, les organes de contrôle doivent pouvoir :

- Délivrer des autorisations de mise en place des mesures de surveillance (si réputées légales et efficaces).
- Annuler toute ordonnance d'interception jugée illégale[47].
- Ordonner aux autorités de cesser ou de suspendre la mise sur écoute, la réception, l'enregistrement, le contrôle, ou la transcription directs ou indirects de toute forme de communication des avocats, ou auxquelles des avocats participent, en cas d'illégalité.
- Ordonner la destruction permanente[48] de l'écoute, la réception, l'enregistrement, le contrôle ou la transcription directs ou indirects de toute forme de communication des avocats, ou auxquelles des avocats participent, en cas d'illégalité. Et plus particulièrement, dans le cas du contrôle *a posteriori*, l'organe doit pouvoir interdire la transmission d'informations obtenues illégalement au parquet, au Juge d'instruction ou à tout autre juridiction, organe ou organisme gouvernemental engagés dans les poursuites ou représentant ou conseillant le gouvernement en matière civile.

5. Utilisation des informations interceptées

5.1 Toute information interceptée sans autorisation judiciaire (préalable) et portant atteinte au principe du secret professionnel doit être jugée irrecevable devant un tribunal.

Comme l'a maintes fois répété la CEDH[49], le secret professionnel est inextricablement lié au droit à un procès équitable. La section II de ce document fait référence à la jurisprudence. Il en ressort que toute preuve obtenue en portant atteinte au principe du secret professionnel ne devrait être recevable devant un tribunal qu'à la condition que la mesure de surveillance ait été dûment autorisée par un organe de contrôle juridictionnel indépendant tel qu'établi à la section IV. En outre, pour éviter tout risque qu'un État utilise des informations interceptées légalement dans le but d'orienter et de nourrir sa stratégie à l'occasion des procédures judiciaires, tout en maintenant la défense dans l'ignorance de cette situation (et ne puisse faire jouer le contrôle juridictionnel), les informations collectées légalement doivent, d'une part être communiquées aux avocats agissant au nom de la partie dont les données ou communications confidentielles ont été surveillées, et d'autre part être recevables comme preuve devant un tribunal.

5.2 Toute information obtenue légalement doit être utilisée uniquement aux fins autorisées par l'organe de contrôle.

Toute autre utilisation constituerait une violation du principe du secret professionnel et doit, en ce sens, être jugée irrecevable devant un tribunal.

5.3 Lorsque les informations interceptées sont jugées illégales, leur destruction doit être exigée.

Ceci inclut toutes les informations liées aux communications en question, à savoir les participants, l'heure, le lieu, ainsi que toute autre information.

[46] Cour d'appel de La Haye, *Prakken d'Oliveira et autres c. Pays-Bas*, n. 200 174 280/01, 2015.
[47] CEDH, *Zakharov c. Russie* (47 143/06), 2015 ; voir aussi CEDH, *Kennedy c. Royaume-Uni* (26 839/05), 2010.
[48] CEDH, *Kennedy c. Royaume-Uni* (26 839/05), 2010, §168.
[49] CEDH, *S. c. Suisse* (12629/87), 1991, §48. Voir également CEDH, *Domenichini c. Italie* (15943/90), 1996, §39; CEDH, *Öcalan c. Turquie* (46221/99), 2005, §1333; CEDH, *Moiseyev c. Russie* (62936/00), 2008, §209; CEDH, *Campbell c. Royaume-Uni* (13590/88), 1992, §§ 44-48.

6. Voies de recours et sanctions

6.1 Afin de fournir une protection juridique efficace contre la surveillance illégale, les voies de recours sont indispensables pour les avocats et leurs clients victimes de surveillance illégale. Les auteurs d'actes de surveillance illégale doivent si nécessaire se voir infliger des sanctions.

Ce principe a été établi, en 2006, dans un jugement rendu par la CEDH et exigeant l'ouverture effective de voies de recours pour les victimes[50] une fois que l'existence des mesures de surveillance a été révélée. Ces voies de recours doivent être ouvertes aussi bien pour la surveillance illégale en raison de l'absence d'autorisation que pour la surveillance autorisée en premier lieu mais exécutée ensuite de manière illégale (ou dont l'autorisation aurait été retirée).

6.2 Une fois l'existence de mesures de surveillance révélée, les avocats et leurs clients ont notamment le droit d'être informés quant aux données recueillies à leur insu lors d'activités de surveillance directe ou indirecte.

Ce droit est absolu (il ne peut dès lors être limité par les allégations de sûreté de l'État) et opposable à toute autorité nationale ou européenne. La CEDH a précisé[51] que ce droit à l'information était limité dans la mesure où le gouvernement a le droit de trouver un juste équilibre entre la protection de la sécurité nationale et la gravité de l'atteinte au droit au respect de la vie privée des citoyens en vertu de l'article 8. Néanmoins, comme expliqué précédemment, si les informations obtenues lors des activités de surveillance sont protégées en vertu de l'article 6, un tel exercice d'équilibre ne devrait pas être possible conformément à l'article 8. Contrairement à l'article 8, l'article 6 n'autorise aucune exception. Dans les cas où les mesures de surveillance visent des informations couvertes par le secret professionnel et relevant de l'article 6, un exercice d'équilibre ne peut en aucun cas être permis. De plus, au vu de la protection accrue accordée aux communications avocat-client par l'article 8, le résultat d'un exercice d'équilibre ne devrait, en principe, pas être différent de l'application de l'article 6.

6.3 Une fois l'existence des mesures de surveillance révélée, les avocats et leurs clients qui en ont été victimes doivent pouvoir en contester la légalité devant un juge.

Doivent au moins être ouvertes les voies de recours suivantes :

Mesures préventives

Les avocats et leurs clients doivent pouvoir exiger des mesures préventives. Celles-ci doivent être applicables à la fois aux surveillances directe et indirecte. En réalité, les avocats et leurs clients peuvent avoir été victimes de surveillance à leur insu. Ils ne devraient dès lors pas avoir à prouver qu'ils en ont été victimes, en particulier dans le cas de surveillance de masse. La Commission de Venise[52] a suggéré de mettre en place une procédure générale de dépôt de plaintes en raison de la méconnaissance probable de la part des personnes concernées des activités de surveillance.

Cette approche a été adoptée par la CEDH dans de nombreuses affaires de surveillance gouvernementale. Dans les affaires *Roman Zakharov c. Russie*[53] et *Szabó et Vissy c. Hongrie*[54], la Cour a clairement établi que si les requérants ont, du moins vraisemblablement, été touchés par la surveillance et qu'ils ne sont pas suffisamment protégés par la législation nationale, alors ils n'ont aucune obligation de prouver qu'ils ont personnellement été victimes de cette surveillance. Même si une protection juridique nationale est disponible, la CEDH ne retient pas le fait d'être personnellement concerné comme condition préalable. Le requérant doit néanmoins prouver que, en raison de sa situation personnelle, il est susceptible d'être l'objet de mesures de surveillance.

Demande de suppression

[50] CEDH, *Segerstedt-Wiberg et autres c. Suède* (62 332/00), 2006, §117.
[51] Ibid.
[52] Commissaire aux droits de l'homme du Conseil de l'Europe, 'Democratic and effective oversight of national security services', 2015, page 51.
[53] CEDH, *Zhakarov c. Russie* (47 143/06), 2015.
[54] CEDH, *Szabó et Vissy c. Hongrie* (37 138/14), 2016.

Les avocats et leurs clients doivent pouvoir exiger la destruction ou la suppression de toute information obtenue illégalement. Cette approche a d'ailleurs reçu le soutien du Commissaire aux droits de l'homme du Conseil de l'Europe[55] dans un communiqué.

Dédommagement pour préjudices pécuniaires et non pécuniaires

Les avocats et leurs clients doivent être dédommagés pour tout dommage financier résultant d'une surveillance illégale. En outre, ils doivent bénéficier d'un dédommagement pour tous les préjudices non pécuniaires qu'ils peuvent établir conformément à la jurisprudence de la CEDH. En 2015[56], la CEDH a accordé la somme de 4 500 euros au titre de la satisfaction équitable (pour *« préjudice moral »*) à un avocat pénaliste bulgare dont les communications avec son client avaient été interceptées.

6.4 Toute autorité gouvernementale reconnue coupable d'activités de surveillance illégale doit être passible de sanctions.

Un système de sanctions complet et efficace doit être mis en place de façon à prévenir d'éventuelles violations.

Au regard de la décision-cadre 2005/222/JAI du 24 février 2005 du Conseil de l'Union européenne, et en rapport avec la surveillance numérique en particulier, chaque État membre doit avoir mis en place un système d'infractions pénales multiples couvrant les nombreuses méthodes de surveillance illégales. La décision-cadre du Conseil permettait certaines exceptions aux réglementations nationales, en particulier pour les infractions mineures. Le CCBE estime qu'aucune exception ne peut être appliquée à la surveillance des communications des avocats étant donné qu'elles ne peuvent, par définition, constituer une infraction mineure.

Par conséquent, toute mesure de surveillance illégale portant atteinte au secret professionnel doit être passible de sanctions pénales ou d'autres sanctions appropriées.

CONCLUSION

Le CCBE salue l'obligation des États d'assurer la sécurité et la protection des citoyens, mais souligne que le secret professionnel est un pilier essentiel de l'état de droit. Lorsqu'un État cherche à nier ou à porter atteinte au principe du secret professionnel, même au nom de la sécurité nationale, il porte atteinte à l'état de droit.

De plus, le soi-disant conflit opposant, d'une part, l'impératif de la protection de la sécurité nationale et, d'autre part, la protection du secret professionnel, est illusoire. Comme l'explique le présent document, ces deux aspects peuvent coexister en composant des éléments essentiels d'une société démocratique mature et parfaitement fonctionnelle qui fonctionne conformément à l'Etat de droit.

[55] Commissaire aux droits de l'homme du Conseil de l'Europe, 'Democratic and effective oversight of national security services', 2015, page 51.
[56] CEDH, *Pruteanu c. Roumanie* (30181/05), 2015, §64.

Historique des actions du CCBE en matière de surveillance

Depuis les révélations Snowden de 2013, le CCBE a publié des déclarations, des études et des lettres dénonçant les violations du secret professionnel par les États et les organismes gouvernementaux qui exercent des activités de surveillance illégales.

Au début du mois de juillet 2013, le CCBE a publié une première déclaration dénonçant la menace que représentent les organismes d'État disposant de pouvoirs d'enquête secrets et technologies d'interception sophistiquées.

En octobre 2013, le CCBE a présenté ses premières recommandations visant à protéger le secret professionnel de la surveillance des gouvernements.

En décembre 2013, le CCBE a participé à l'enquête de la commission LIBE sur la surveillance électronique de masse des citoyens de l'UE. Après six mois d'enquête, le Parlement européen a approuvé en mars 2014 une résolution qui conclut notamment qu'il est « *capital de protéger le secret professionnel des avocats […] contre les activités de surveillance de masse* » et « *que toute incertitude concernant la confidentialité des communications entre les avocats et leurs clients pourrait avoir des incidences négatives sur le droit d'accès des citoyens de l'Union européenne à l'assistance juridique et à la justice, ainsi que le droit à un procès équitable* ». Cette même résolution propose également d'instaurer un habeas corpus numérique pour protéger les droits fondamentaux, y compris l'état de droit et la confidentialité des communications entre l'avocat et son client. Le CCBE a salué cette résolution.

En avril 2014, le CCBE a publié une étude comparative sur la surveillance gouvernementale des données des avocats hébergées dans le nuage, qui expose de quelle manière, dans les diverses juridictions européennes, les gouvernements sont susceptibles d'avoir accès aux données électroniques sont susceptibles d'être examinées, ainsi que les règles et les conditions d'un tel accès.

À la suite des évolutions importantes en matière de surveillance par les gouvernements et de leurs répercussions sur les avocats et leurs clients, le CCBE a décidé de créer en mars 2015 un groupe de travail spécialement consacré à la surveillance.

En mars 2015, le CCBE a adressé une lettre au ministre britannique de l'Immigration ainsi qu'au secrétaire d'État britannique des affaires étrangères et du Commonwealth. Les courriers exprimaient des craintes concernant des politiques permettant l'accès du personnel des services de sécurité du Royaume-Uni à des communications confidentielles entre des avocats et leurs clients et demandaient des précisions sur la question. Enfin, le CCBE a exprimé par écrit en janvier 2016 au président du Parlement polonais ses préoccupations au sujet d'un projet de loi sur des modifications à la loi sur la police et à d'autres lois liées aux services secrets de l'État, en particulier concernant la réglementation sur la surveillance des données et sur la conservation des données.

Le CCBE a en outre été impliqué dans deux affaires en 2015. Il est tout d'abord intervenu auprès du Conseil constitutionnel français pour défendre la confidentialité des échanges avocat-client. Il a soumis des commentaires au regard de la loi relative au renseignement et a formulé plusieurs suggestions afin que la loi soit conforme au droit au respect de la vie privée et au droit à l'assistance d'un avocat. En mai 2015, il est ensuite intervenu avec succès dans l'affaire que le cabinet d'avocats amstellodamois Prakken d'Oliveira et l'Association néerlandaise des avocats pénalistes (NVSA) ont portée contre l'État néerlandais devant le tribunal d'arrondissement de La Haye. Le tribunal a été saisi quant à la légalité des écoutes des appels et des communications des avocats par les agences de renseignements nationales. Dans son verdict du 1er juillet, le tribunal a reconnu la possibilité de communiquer en toute confidentialité avec un avocat comme constituant un droit fondamental violé par la politique de surveillance néerlandaise. Le tribunal a ordonné au gouvernement néerlandais de cesser toute interception des communications entre les clients et les avocats sous le régime actuel dans les six mois à venir. L'État néerlandais a rapidement interjeté appel de la décision. Le 25 août 2015, le CCBE a, à son tour, contesté les motifs d'appel et, le 27 octobre 2015, la Cour d'appel néerlandaise a rejeté tous les motifs d'appels avancés par l'État néerlandais et a confirmé la décision de l'instance inférieure interdisant la surveillance des communications des avocats protégés par le secret professionnel.

Bibliographie

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, *Sakhnovskiy 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.