CONFERENCE OF INGOs
OF THE COUNCIL OF EUROPE

CONFERENCE DES OING DU
CONSEIL DE L'EUROPE

Recommandation CONF/PLE(2017)REC1 adoptée par la Conférence des OING le 27 janvier 2017

« Surveillance des avocats : la nécessité de normes garantissant le secret professionnel »

La Conférence des organisations internationales non gouvernementales (OING) du Conseil de l'Europe :

Considérant les préoccupations exprimées par plusieurs organisations internationales gouvernementales et non gouvernementales[1] liées aux pouvoirs d'enquête secrets ou insuffisamment contrôlés dont disposent les organismes publics, ainsi qu'à leur usage de technologies d'interception et de traçage hautement sophistiquées et de grande portée pour accéder aux données de communication des citoyens de manière indiscriminée, à grande échelle et en l'absence de tout soupçon ;

Soulignant que même si certaines technologies d'interception et de traçage peuvent parfois être utiles dans la lutte contre le terrorisme et le crime organisé, elles soulèvent aussi un certain nombre de problèmes, en particulier concernant la compatibilité de cette ingérence avec les principes du secret professionnel et du *legal professional privilege*[2] ;

Considérant que les activités de surveillance des « gouvernements » peuvent impliquer le gouvernement national en soi, mais aussi les différents niveaux de gouvernement (fédéral, central ou local), les organismes gouvernementaux, les autorités fiscales, les organismes indépendants chargés de la fonction publique, la police, les procureurs, les services de renseignements, etc., et peuvent inclure l'externalisation de ces activités par le gouvernement ;

[1] Se reporter par exemple aux rapports – cités dans les notes de bas de page 9 à 13 – de l'Assemblée parlementaire du Conseil de l'Europe, de la Commission de Venise du Conseil de l'Europe, du Commissaire aux droits de l'homme du Conseil de l'Europe et du Parlement européen. Par ailleurs, 10 organisations de défense des droits de l'homme ont intenté une action en justice (en avril 2015) contre le Royaume-Uni devant la Cour européenne des droits de l'homme au sujet de la surveillance de masse.

[2] 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. Pour de plus amples informations, voir Conseil des barreaux européens, Recommandations du CCBE sur la protection du secret professionnel dans le cadre des activités de surveillance, 28 avril 2016, pages 9-10.

Mettant l'accent sur le fait que la surveillance de masse porte gravement atteinte au droit à la confidentialité des communications avec leur avocat des personnes demandant à bénéficier de conseils et d'une représentation juridiques et à l'obligation de préserver cette confidentialité faite aux avocats, alors que ces droits et obligations en matière de secret professionnel sont des composantes essentielles de droits fondamentaux plus larges comme le droit à un procès équitable (article 6 CEDH), le droit au respect de la vie privée (article 8 CEDH), ou le droit à la liberté d'information et d'expression (article 10 CEDH) ;

Rappelant que ces droits sont les piliers de la démocratie, et que ne pas les respecter porte également atteinte à l'état de droit ;

Soulignant que les activités de surveillance ciblée des gouvernements doivent être rigoureusement réglementées et contrôlées par des autorités judiciaires indépendantes et satisfaire aux principes de légalité, de nécessité et de proportionnalité[3] ;

Considérant que la confidentialité des communications avocat-client[4] est considérée non seulement comme étant le devoir de l'avocat, mais encore comme un droit fondamental du client, et que 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 ;

Mettant l'accent sur le fait que l'obligation de confidentialité de l'avocat sert les intérêts de l'administration de la justice comme ceux du client, et qu'elle doit par conséquent bénéficier d'une protection spéciale de l'État ;

Soulignant que la confidentialité des communications avocat-client est protégée en vertu de la Convention européenne des droits de l'homme et du droit de l'Union européenne, et qu'elle revêt une grande importance aux yeux de la Cour européenne des droits de l'homme[5], de la Cour de justice de l'Union européenne[6] et d'autres organes européens concernés ;

---

[3] Voir le document (2015) de la Commission de Venise du Conseil de l'Europe intitulé « 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 ».

[4] Aux fins de la présente recommandation, on entend par « communications avocat-client » toutes communications avec ou entre les avocats dans l'exercice de leurs activités professionnelles, y compris toutes les données couvertes par le secret professionnel ou par le *legal professional privilege*.

[5] Comme par exemple dans les affaires suivantes : *S. c. Suisse* (12629/87, 1991) (*« 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 »)* ; *Pruteanu c. Roumanie* (30181/05, 2015) (« (…) *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* ») ; *Niemietz c. Allemagne* (13710/88, 1992) (*« (…) il convient de 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 [de la Convention] (…) »*) ; *Kopp c. Suisse* (23224/94, 1998) (*« 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. »*). Plus spécifiquement, la Cour s'est prononcée sur la compatibilité avec l'article 8 de perquisitions et saisies effectuées dans le cabinet d'un avocat ou à son domicile *(*voir *Niemietz c. Allemagne ; Roemen et Schmit c. Luxembourg, requête nº 51772/99 ; Sallinen et autres c. Finlande, requête nº 50882/99, 27 septembre 2005 ; André et autre c. France, 24 juillet 2008 ; Xavier Da Silveira c. France, 21 janvier 2010),* de la fouille et saisie de données électroniques dans un cabinet d'avocat (voir *Sallinen et autres, Wieser et Bicos Beteiligungen GmbH c. Autriche, 16 octobre 2007,* et *Robathin c. Autriche, requête nº 30457/06, 3 juillet 2012),* de l'interception de la correspondance entre un avocat et son client *(*voir *Schönenberger et Durmaz c. Suisse, 20 juin 1988, Série A nº 137),* de la mise sur écoute des lignes téléphoniques d'un avocat (voir *Kopp c. Suisse*, 25 mars 1998), de l'obligation faite aux avocats de déclarer leurs « soupçons » relatifs aux activités de blanchiment d'argent de leurs clients *(Michaud c. France)*, des

Se référant en particulier à l'affaire *Michaud*[7], dans laquelle il est affirmé que *« si l'article 8 [CEDH] 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. […] 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 » ;*

Rappelant que selon la recommandation du Conseil de l'Europe adoptée le 25 octobre 2000[8], *« toutes les mesures nécessaires devraient être prises pour veiller au respect du secret professionnel des relations entre avocats et clients »*, et que *« des exceptions à ce principe devraient être permises seulement si elles sont compatibles avec l'état de droit »* ;

Rappelant que selon la Résolution 2045 du 21 avril 2015[9] de l'Assemblée parlementaire du Conseil de l'Europe, *« les opérations de surveillance révélées jusqu'ici mettent en danger les droits de l'homme fondamentaux »*, surtout *« lorsque les communications confidentielles des avocats »* sont interceptées ;

Rappelant que, selon le rapport 2015[10] de la Commission de Venise intitulé « 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 », les avocats sont des *« communicants privilégiés »* qui requièrent un seuil très élevé de protection ;

Rappelant que selon le document thématique publié en 2015[11] par le Commissaire aux droits de l'homme du Conseil de l'Europe sur la surveillance démocratique et effective des services de sécurité nationale, *« l'interception des communications entre les avocats et leurs clients […] peut porter atteinte à l'égalité des armes et au droit à un procès équitable, notamment lorsque les services de sécurité sont parties au litige »* [traduction non officielle] ;

---

perquisitions et saisies de la correspondance entre les avocats et leurs clients opérées dans les locaux d'une société par l'autorité nationale de la concurrence (*Vinci Construction et GTM génie civil et services c. France*, requêtes nos 63629/10 et 60567/10, 2 avril 2015) et de l'accès aux comptes bancaires d'une avocate *(Brito Ferrinho Bexiga Villa-Nova c. Portugal, requête no 69436/10, 1er décembre 2015).*

[6] Dans l'affaire *AM & S c. Commission* (155/79, 1982), la CJCE a admis que le respect de la confidentialité à l'égard de certaines communications entre les avocats et leurs clients constitue un principe général de droit commun au droit de tous les États membres et, en tant que tel, un droit fondamental protégé par le droit communautaire. La Cour a estimé 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. Voir aussi CJCE, Conclusions de l'avocat général Léger, *J.C.J. Wouters, J.W. Savelbergh, Price Waterhouse Belastingadviseurs BV c. Algemene Raad van de Nederlandse Orde van Advocaten,* dans l'affaire C-309/99, 10 juillet 2001, par. 182, et CJCE, Conclusions de l'avocat général Poiares Maduro, *Ordre des barreaux francophones et germanophone et autres c. Conseil des ministres,* dans l'affaire C-305/05, par. 42-44, 14 décembre 2006.

[7] Cour européenne des droits de l'homme, *Michaud c. France* (12323/11), 2012, par. 118.

[8] Conseil de l'Europe, Recommandation no R(2000)21 du Comité des Ministres aux États membres sur la liberté d'exercice de la profession d'avocat, 25 octobre 2000, par. 6.

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

[10] Rapport 2015 de la 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 », par. 18.

[11] Commissaire aux droits de l'homme du Conseil de l'Europe, document thématique, *Democratic and effective oversight of national security services*, 2015, p. 27.

Rappelant que la résolution du Parlement européen[12] du 12 mars 2014 sur la surveillance souligne 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 »*[13] *;*

Considérant les Recommandations[14] adoptées par le Conseil des barreaux européens sur la protection du secret professionnel dans le cadre des activités de surveillance ;

Notant les appels lancés par plusieurs organisations[15] en faveur d'une charte des droits numériques mondiale et d'un habeas corpus numérique européen, qui devraient aussi fournir une protection supplémentaire aux communications avocat-client ;

Insistant sur la nécessité de normes, la Conférence des OING du Conseil de l'Europe :

1. **demande instamment** au Comité des Ministres du Conseil de l'Europe d'adopter et de mettre en œuvre les recommandations énumérées ci-après pour s'assurer que les principes du secret professionnel et du *legal professional privilege* ne soient pas remis en cause par les pratiques des États à des fins de surveillance impliquant l'interception des communications entre les avocats et leurs clients et d'autres données protégées par le *legal professional privilege* ou par les obligations de secret professionnel :

   a) 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 *legal professional privilege* et par le secret professionnel sont inviolables et ne peuvent être sujettes à des interceptions ou à une surveillance ;
   b) 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 ;
   c) seules les communications sortant du champ d'application du secret professionnel ou du *legal professional privilege* 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

---

[12] Parlement européen, Résolution sur le programme de surveillance de la NSA, les organismes de surveillance dans divers États membres et les incidences sur les droits fondamentaux des citoyens européens et sur la coopération transatlantique en matière de justice et d'affaires intérieures, 12 mars 2014, par. 11.

[13] Voir aussi Parlement européen, Résolution sur le suivi de la résolution du Parlement européen du 12 mars 2014 sur la surveillance électronique de masse des citoyens de l'Union européenne, qui fait valoir que *« la surveillance de masse remet sérieusement en question […] les droits des citoyens de l'Union à être protégés contre toute surveillance de communications confidentielles avec leurs avocats »*, 29 octobre 2015, par. 43.

[14] Conseil des barreaux européens, Recommandations sur la protection du secret professionnel dans le cadre des activités de surveillance, 28 avril 2016.

[15] Dont le Parlement européen (Résolution sur le programme de surveillance de la NSA, les organismes de surveillance dans divers États membres et les incidences sur les droits fondamentaux des citoyens européens et sur la coopération transatlantique en matière de justice et d'affaires intérieures, 12 mars 2014, par. 132), European Digital Rights (EDRi) et la Fédération des Barreaux d'Europe (résolution relative à la protection des données et au secret professionnel adoptée par le Congrès de la FBE à Bilbao en mai 2015).

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 *legal professional privilege* ou du secret professionnel. Les organismes publics et forces de l'ordre doivent être tenus d'utiliser tous les moyens technologiques disponibles afin de maintenir les informations relevant du secret professionnel et du *legal professional privilege* hors du champ d'application des opérations de surveillance[16] ;

d) une autorisation judiciaire préalable et, si nécessaire, assortie de conditions est indispensable avant toute interception des communications avocat-client. Un contrôle juridictionnel *a posteriori* ne peut lui être substitué que dans des circonstances exceptionnelles (le cas échéant). Une fois l'autorisation judiciaire accordée, il est nécessaire de veiller à ce qu'un organe judiciaire indépendant, ayant le pouvoir de mettre fin à l'interception, mais aussi de détruire les informations interceptées, contrôle toutes les étapes de la procédure de surveillance. La loi doit à cette fin accorder des pouvoirs suffisants à cet organe pour qu'il puisse prendre des décisions exécutoires et être financièrement et politiquement indépendent ;

e) toute information interceptée sans autorisation judiciaire et au mépris du 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 et communiquée à toutes les parties ;

f) les avocats et leurs clients victimes de surveillance illégale doivent disposer de voies de recours et un système de sanctions doit être instauré. 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 l'existence des mesures de surveillance révélée, et doivent pouvoir contester la légalité de ces mesures devant un juge. Toute autorité gouvernementale reconnue coupable d'activités de surveillance illégale doit être passible de sanctions ;

2. **demande instamment** l'élaboration et l'adoption de recommandations du Comité des Ministres du Conseil de l'Europe sur la protection du secret professionnel dans le cadre des activités de surveillance en s'inspirant des normes exposées ci-dessus ;

3. **invite** le Comité des Ministres du Conseil de l'Europe à élaborer une définition de la « securité » dont la « sécurité nationale » suffisamment précise pour permettre un contrôle juridictionnel effectif des activités des gouvernements et assurer qu'elles satisfont rigoureusement à un double test de nécessité et de proportionalité.

---

[16] L'usage des services de communications électroniques ou d'autres services dématérialisés par les avocats devrait être protégé de la même façon, que les données soient stockées dans un centre de données, dans un ordinateur de leur cabinet ou dans leur ordinateur personnel. Les données contenant des informations protégées par le secret professionnel ou revêtant le caractère d'une information juridiquement privilégiée et traitées par un service de communications électroniques ou par un prestataire de services d'informatique en nuage (y compris les fournisseurs d'accès Internet) ne devraient pas être accessibles aux organismes publics. Les services de communications électroniques et les prestataires de services d'informatique en nuage devraient être tenus d'offrir aux avocats la possibilité d'indiquer quelles sont les informations concernées – après avoir dûment vérifié, bien évidemment, que cet utilisateur est réellement un avocat comme il le prétend. Aux Pays-Bas, par exemple, il existe un système de reconnaissance du numéro de téléphone capable d'identifier les numéros des avocats et de faire cesser toute surveillance.