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 – F. : +32 (0)2 234 65 11
Email : ccbe@ccbe.eu – www.ccbe.eu

Déclaration du CCBE sur la surveillance électronique de masse par des organismes gouvernementaux (notamment les données des avocats européens)

14/10/2013

Historique

Le Conseil des barreaux européens (CCBE) représente les barreaux de 32 pays membres et 11 pays associés et observateurs, soit plus d'un million d'avocats européens.

Le 1er juillet 2013, le CCBE a publié une déclaration (voir en annexe) concernant les pratiques gouvernementales impliquant l'exploration massive de données à des fins de surveillance, dans laquelle il exprime sa préoccupation profonde vis-à-vis de la menace sérieuse que subit la valeur fondamentale de la profession qu'est le secret professionnel, dont l'érosion portera atteinte à la confiance en l'État de droit.

La déclaration du CCBE suit les rapports concernant la violation massive des droits de l'homme à la protection de la vie privée et des données à caractère personnel qu'ont mené de manière systématique les agences gouvernementales de grandes puissances occidentales, parmi lesquelles certains États membres de l'Union européenne. Ces allégations dévoilent des violations manifestes de la Charte des droits fondamentaux de l'Union européenne par certains organismes gouvernementaux au sein de l'Union européenne, principalement les articles 7[1] et 8[2], mais également l'article 47[3] en raison de l'absence de mécanisme de contrôle judiciaire approprié. L'accès généralisé présumé à la plupart des communications entre personnes non ressortissantes des États-Unis et leur surveillance à grande échelle comprenait également les communications entre les avocats et leurs clients. Le CCBE estime que ce type de surveillance de masse va au-delà d'une atteinte à des droits de l'homme spécifiques entre particuliers : il s'agit d'une menace envers l'État de droit tel que les démocraties modernes le reconnaissent.

---

1 **Article 7 - Respect de la vie privée et familiale**

Toute personne a droit au respect de sa vie privée et familiale, de son domicile et de ses communications.

2 **Article 8 - Protection des données à caractère personnel**

1. Toute personne a droit à la protection des données à caractère personnel la concernant.

2. Ces données doivent être traitées loyalement, à des fins déterminées et sur la base du consentement de la personne concernée ou en vertu d'un autre fondement légitime prévu par la loi. Toute personne a le droit d'accéder aux données collectées la concernant et d'en obtenir la rectification.

3. Le respect de ces règles est soumis au contrôle d'une autorité indépendante.

3 **Article 47 – Droit à un recours effectif et à accéder à un tribunal impartial**

Toute personne dont les droits et libertés garantis par le droit de l'Union ont été violés a droit à un recours effectif devant un tribunal dans le respect des conditions prévues au présent article.

Toute personne a droit à ce que sa cause soit entendue équitablement, publiquement et dans un délai raisonnable par un tribunal indépendant et impartial, établi préalablement par la loi. Toute personne a la possibilité de se faire conseiller, défendre et représenter.

Une aide juridictionnelle est accordée à ceux qui ne disposent pas de ressources suffisantes, dans la mesure où cette aide serait nécessaire pour assurer l'effectivité de l'accès à la justice.

Jusqu'à présent, ni l'Union européenne ni ses États membres n'ont publié de rapports répondant de manière satisfaisante aux allégations susmentionnées. En l'absence de fondement juridique solide, il demeure impossible de savoir s'il y a eu violation des droits fondamentaux, tels qu'à l'alinéa 2 de l'article 8 de la Charte des droits fondamentaux de l'Union européenne, ou à l'article 12 de la directive relative à la protection des données (95/46/CE), qui rend également toute tentative de faire valoir ces droits impossible. Tout citoyen de l'Union européenne a le droit d'accéder aux données le concernant, qui comporte tout aussi expressément le droit de savoir si un État-nation a commis une intrusion frauduleuse dans sa vie privée sur Internet. Le problème réside également dans le fait que les négociations bilatérales avec les États-Unis d'Amérique sur la question ne sont pour l'instant absolument pas transparentes.

À la suite des articles de presse et des récentes audiences de la commission LIBE du Parlement européen, le CCBE est d'avis que les plus grandes menaces à la confiance des clients envers le secret professionnel ont deux origines : a) le manque de confiance dans les organismes publics disposant de pouvoirs secrets de surveillance (la crainte étant qu'ils utilisent ces pouvoirs au-delà du cadre de leur mandat démocratique) et b) un manque objectif de moyens techniques à la disposition des cabinets d'avocats pour protéger de manière effective le secret professionnel.

Le secret professionnel des avocats est rigoureusement protégé dans tous les États membres de l'Union européenne, même si les limites et les moyens de cette protection juridique sont différents. La jurisprudence de la Cour européenne de justice tout comme celle de la Cour européenne des droits de l'homme reconnaissent ce droit. Toujours est-il que les révélations récentes sur les pratiques d'agences de surveillance gouvernementales de premier plan ont suscité la crainte que la protection au secret professionnel offerte par les mesures juridiques des États membres de l'Union européenne ne fonctionne pas en pratique.

Sans secret professionnel, pas de confiance : les répercussions sur la stratégie numérique pour l'Europe

Le rôle de l'avocat, qu'il agisse pour le compte d'un particulier, d'une entreprise ou de l'État, est d'être le conseiller et le représentant de confiance du client, un professionnel respecté par les tiers et un acteur incontournable de l'administration équitable de la justice et de la démocratie. Il relève de la quintessence de sa fonction de savoir quels sont les sujets que le client ne veut pas dévoiler (les détails personnels les plus intimes ou les secrets commerciaux les plus précieux) et d'être le destinataire d'autres informations en toute confiance. Sans la certitude de bénéficier du secret, la confiance est inexistante. Par conséquent, si les citoyens et les entreprises de l'Union européenne sont privés de leur droit à être protégés contre le dévoilement de leurs communications avec leur avocat, ils peuvent être privés d'accès à des conseils juridiques et à la justice.

Compte tenu des moyens techniques dont disposent les cabinets d'avocats, y compris les très grands cabinets, le CCBE constate que les avocats ont actuellement recours à des systèmes de communication électronique et de services en nuage non sécurisés, car nous savons désormais que ces systèmes comportent des portes dérobées auxquelles les agences gouvernementales ont accès. Le CCBE a encore appris récemment que même la plus grande de ces agences gouvernementales éprouve parfois des difficultés à contrôler les informations secrètes auxquelles elle a accès. De toute évidence, plus les portes dérobées seront nombreuses, moins l'infrastructure en ligne sera sécurisée.

S'ils utilisent ces systèmes de communication électronique ou services en nuage, les avocats transgressent *de facto* leurs obligations de responsabilité des données et violent leurs règles déontologiques. Les communications non sécurisées ne sont pas simplement une question de formation ou de culture, mais plutôt une question concernant toutes les entreprises européennes, à l'exception des plus grandes et de celles du secteur de la défense.

Dans de telles circonstances, les avocats sont donc contraints à opérer un choix entre les solutions suivantes :

a) Continuer à utiliser les mêmes systèmes de communication électronique et services d'informatique en nuage que le grand public, en sachant qu'ils enfreignent leur devoir envers le client de maintenir la confidentialité de leurs informations, et demander le consentement éclairé des clients après leur avoir exposé les risques encourus ; ou

b) Utiliser les services de communication électronique rendus possibles par de nouveaux investissements dans un internet totalement distinct, destiné uniquement à l'Union européenne et disposant de passerelles strictes exécutant toutes les politiques rigoureuses,

etc., rétablissant ainsi la confiance à l'échelle de l'Union, tout en acceptant l'inefficacité de ce type de solution, dont les coûts de redéveloppement, etc. ; ou

c) N'utiliser ni courriels, ni services de communication électronique ni services d'informatique en nuage dans les communications avec les clients en échangeant uniquement les données par le biais de supports de données physiques tels que les clés USB, ou en utilisant des machines à écrire, les services postaux et des services de livraison express.

Aucune des solutions ci-dessus ne semble réaliste en pratique et il est clair que la situation est totalement inacceptable dans une société démocratique fondée sur l'État de droit.

Ce phénomène aura à son tour des répercussions sur l'évolution de la stratégie numérique pour l'Europe, qui a pour objectif principal d'aider les citoyens et les entreprises en Europe à tirer le meilleur parti des technologies numériques. La stratégie numérique pour l'Europe précise pourtant bien : « Les Européens n'adopteront pas de technologie dont ils se méfient. L'ère numérique n'est synonyme ni de cyberespionnage ni de cyberjungle »[4]. Comme indiqué précédemment, ce fait est particulièrement important dans le cas des avocats. La prestation effective des services juridiques restera gravement menacée tant que le secret professionnel des communications des avocats et de leurs clients ne sera pas garanti. En raison du lien étroit entre les services juridiques et les résultats économiques, dû au rôle que les services juridiques jouent en facilitant et en soutenant les marchés, la situation aura des répercussions négatives sur l'économie européenne.[5]

Rétablir la confiance

Les révélations récentes concernant la pratique de certains organismes de surveillance ont suscité la crainte que la protection au secret professionnel offerte par les mesures juridiques des États membres de l'Union européenne ne fonctionne pas en pratique, et il se pourrait que dans certains cas des États membres aient procédé à la surveillance électronique à l'encontre de leurs propres ressortissants en violation de leur propre réglementation nationale.

En outre, si dans un État membre de l'UE donné une ordonnance judiciaire est nécessaire pour obtenir l'accès à des informations confidentielles détenues par des avocats dans un autre État, il s'avère impossible de remplir cette condition si le tribunal qui délivre l'ordonnance se situe par définition dans un autre État, sans aucun contrôle possible de la part d'un juge dans l'État de résidence de l'avocat. De même, les motifs liés à la sécurité nationale d'un autre État, qu'il soit membre de l'Union ou non, ne constitueront pas forcément des motifs de sécurité nationale dans un autre, et les organismes de sécurité nationale d'un État membre ne devraient pas coopérer à cette surveillance sans respecter la réglementation nationale concernant le secret professionnel.

Si les forces de l'ordre et les services de sécurité nationaux ont besoin de surveiller électroniquement les citoyens dans certaines circonstances particulières, la perte de confiance créée n'est soluble qu'en prenant des mesures politiques , par exemple en déterminant soigneusement quels domaines des activités secrètes de surveillance secrète ne doivent pas être rendues publics et, par conséquent, ceux ou la participation des citoyens (par l'intermédiaire de représentants de la profession d'avocats notamment) permettrait de rétablir et de maintenir la confiance du public.

Recommandations

1. Se référant à la prise de position du CCBE (adoptée le 7 septembre 2012) concernant le paquet de réformes de la protection des données, le CCBE estime que les obligations des forces de l'ordre en matière de protection des données à caractère personnel et de toute autre donnée relevant du secret professionnel doivent être pour le moins aussi élevées que

[4] Communication de la Commission sur une stratégie numérique pour l'Europe, page 18 : http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0245:FIN:FR:PDF.

[5] Voir l'étude du professeur George Yarrow et du docteur Christopher Decker du *Regulatory Policy Institute*, Assessing the economic significance of the professional legal services sector in the European Union (août 2012). À la page 3, il est indiqué qu'un lien particulièrement étroit entre les services juridiques et les résultats économiques découle du rôle que jouent les services juridiques en facilitant et en soutenant les marchés : l'activité principale du secteur des services juridiques professionnels tend à développer l'activité des marchés à travers toute l'économie, d'où le lien étroit aux résultats et à la croissance économique.

la protection attendue des entités de contrôle des données dans la sphère privée. Cet aspect renforce la nécessité d'un régime de protection global et unique.

2. Des mesures sont par ailleurs nécessaires à l'échelle de l'Union européenne pour établir un seuil minimal de protection du secret professionnel face à la surveillance électronique des gouvernements, y compris dans l'utilisation des services de communication électronique ou autres services d'informatique en nuage dans les communications entre avocats et clients. Le recours à ces outils entre avocats et clients doit être protégé de la même manière, quel que soit le l'emplacement de conservation des données, qu'il s'agisse d'un centre de données, d'un ordinateur de bureau ou portable. Le contenu relevant du secret professionnel et traité par l'intermédiaire d'un service de communication électronique ou d'informatique en nuage (y compris un fournisseur de service de messagerie) ne devrait pas être accessible aux services gouvernementaux. Les fournisseurs de services de communication électronique et d'informatique en nuage devraient être tenus de proposer aux avocats la possibilité de signaler ces informations, bien entendu après avoir vérifié soigneusement que l'utilisateur est effectivement avocat.

3. Il convient d'instaurer des normes minimales européennes en matière de surveillance électronique, notamment le besoin de poser des limites raisonnables aux arguments de sécurité nationale comme motifs de restriction du droit à la protection de la vie privée. Ces travaux de réglementation devraient reposer sur des rapports et des propositions régionales et internationales en la matière, comme le rapport de Frank La Rue, rapporteur spécial du Conseil des droits de l'homme des Nations unies (voir ici en anglais) ou le projet de rapport d'une des commissions de l'Assemblée parlementaire du Conseil de l'Europe, *Compilation of good practices on legal and institutional frameworks and measures that ensure respect for human rights by intelligence agencies while countering terrorism, including on their oversight* (voir ici en anglais).

4. L'Union doit travailler au renforcement du droit à la vie privée à l'échelle internationale à partir des protocoles facultatifs de l'article 17 du Pacte international relatif aux droits civils et politiques et en renforçant le niveau de protection garanti en pratique selon les principes de la « sphère de sécurité ». En ce qui concerne les pays européens en dehors de l'Espace économique européen, dans le cadre du processus de modernisation de la convention, l'Union européenne devrait soutenir l'adoption d'exceptions plus précises et plus détaillées à l'article 9 de la Convention 108 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel.

5. Au-delà de toutes les mesures de protection nécessaires pouvant être mises en place grâce à des moyens politiques et législatifs, des mesures techniques doivent également être prises pour reconstruire la confiance dans les services de communication électronique et d'informatique en nuage. Les mesures techniques visant à rendre Internet et l'informatique en nuage plus sûrs et à soumettre davantage leur accès par les gouvernements à un examen juridique doivent également prendre en compte les exigences spécifiques à respecter en matière d'informations soumises aux obligations et aux règles du secret professionnel telles que celles qui régissent les communications entre l'avocat et son client. En d'autres termes, il est nécessaire de construire des infrastructures de communication électronique et d'informatique en nuage là où même des fonctionnalités techniques garantissent que les gouvernements ou des tiers n'empruntent pas abusivement les portes dérobées.

Conclusion

Le CCBE exhorte donc les institutions européennes à créer le cadre juridique et technologique nécessaire afin de résoudre la situation en matière de surveillance électronique de masse et de protéger le secret professionnel qui est un droit de tous les citoyens de l'Union européenne et une des valeurs fondamentales de la profession d'avocat.

ANNEXE : Déclaration du CCBE concernant les pratiques gouvernementales impliquant l'exploration massive de données à des fins de surveillance (1er juillet 2013)

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 – F. : +32 (0)2 234 65 11
Email : ccbe@ccbe.eu – www.ccbe.eu

Déclaration du CCBE concernant les pratiques gouvernementales impliquant l'exploration massive de données à des fins de surveillance

01/07/2013

Le Conseil des barreaux européens (CCBE) représente les barreaux de 32 pays membres et 11 pays associés et observateurs, soit plus d'un million d'avocats européens.

C'est avec la plus grande inquiétude que le CCBE a constaté la révélation récente de pratiques gouvernementales impliquant l'exploration massive de données à des fins de surveillance.

Le CCBE a souligné à maintes reprises l'importance du secret professionnel et rappelle que la Cour européenne de justice elle-même a expressément déclaré dans sa décision dans l'affaire AM&S (affaire C-155/79) : « cette confidentialité répond en effet à l'exigence, dont l'importance est reconnue dans l'ensemble des États membres, 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 « la protection de la confidentialité de la correspondance entre avocats et clients se fonde principalement sur la reconnaissance de la nature même de la profession d'avocat, en tant qu'elle coopère au maintien de la légalité, dans l'exigence plus spécifique du respect des droits de la défense ».

Cette valeur fondamentale de la profession d'avocat se trouve néanmoins sous la menace d'organisations aux moyens techniques et financiers extrêmement développés, y compris des services d'État disposant de pouvoirs secrets de surveillance.

Les avocats n'ont d'autre choix que d'avoir recours aux technologies modernes dans leurs communications avec les clients, les tribunaux, leurs confrères, etc. Or, il apparaît désormais que l'emploi de ces technologies n'est pas sûr.

L'érosion de la confidentialité des communications entre l'avocat et son client affaiblit également la confiance du citoyen en l'État de droit.

Le CCBE appelle donc les institutions européennes à prendre des mesures de protection et de renforcement de la confidentialité des communications entre l'avocat et son client dans le cadre de l'usage des nouvelles technologies. Il serait bon que ces mesures comportent des travaux dans le domaine de l'harmonisation des normes techniques (par exemple la possibilité de définir un compte d'avocat qui serait soumis à une protection accrue contre l'exploration de données) ou dans le domaine des instruments du droit international.