LA CONSERVATION DES DONNÉES ET LE SECRET PROFESSIONNEL DE L'AVOCAT
Commission des droits de l'homme de la FBE Barcelone 30 janvier 2015

Sommaire :

Introduction.

La Commission des droits de l'homme (CDH) de la FBE s'intéresse à la question de la préservation du secret professionnel de l'avocat et de la confiance qui fonde toute relation professionnelle entre un avocat et son client, et plus précisément de la confiance liée au devoir de confidentialité de l'avocat à l'égard de ses clients. Notre préoccupation résulte des évolutions de l'internet qui ont érodé la protection des données et compromis la communication confidentielle entre un avocat et son client, entre un avocat et les tribunaux et entre avocats.

La CDH reconnait qu'il existe différentes normes de protection dans les pays d'Europe. Harmoniser ces normes sera bénéfique aux citoyens et résidents des États membres. L'Union européenne permet aux États membres de collaborer entre eux afin de protéger la confidentialité et la confiance basées sur le secret professionnel de l'avocat. La protection et la préservation de la relation de confiance avocat-client est précisément le sujet de préoccupation des avocats européens, que nous considérons comme un sujet important dans le cadre des directives et des règlements européens.

Première partie : La conservation des données et l'Union européenne.

En 2006, l'UE a promulgué la directive 2006/24 sur la conservation des données. La directive visait à garantir que les données de communication[1] soient disponibles, pour une durée limitée, en vue de la prévention, de la recherche, de la détection et de la poursuite d'infractions graves telles que celles liées, en particulier, à la criminalité organisée et au terrorisme. À cette fin, les fournisseurs de services de communications électroniques accessibles au public ou de réseaux publics de communications devaient conserver les données relatives au trafic et les données de localisation ainsi que certaines données connexes nécessaires pour identifier l'utilisateur. La directive n'autorisait pas l'enregistrement et la conservation du contenu de la communication.[2]

L'article 6 de la directive 95/46/CE antérieure contient des obligations concernant des mesures visant à garantir la confidentialité et la sécurité du traitement des données. Les objectifs de la directive 2006/24/CE étaient d'harmoniser les obligations incombant aux fournisseurs de conserver certaines données et de garantir que ces données soient disponibles aux fins de la recherche, de la détection et de la poursuite d'infractions graves telles qu'elles sont définies par chaque État membre dans son droit interne. Ces objectifs ne pouvant pas être réalisés de manière suffisante par chaque

[1] L'article 2 de la directive 2006/24/CE prévoit qu'aux fins de la directive, on entend par « données », les données relatives au trafic et les données de localisation, ainsi que les données connexes nécessaires pour identifier l'abonné ou l'utilisateur. C'est ce que l'on appelle les données sur le « qui », « où » et « quand ». Ce n'est pas le contenu des communications qui est en cause, mais le contexte.

[2] Newsletter d'avril de Baker & McKenzie, avril 2014

État membre agissant isolément, ils peuvent être mieux réalisés au niveau communautaire en vertu de cette directive. Conformément au principe de proportionnalité, la directive n'excède pas ce qui est nécessaire pour atteindre ces objectifs.

La directive 2006/24/CE vise[3] à veiller à ce que les droits fondamentaux liés au respect de la vie privée et des communications des citoyens et à la protection des données à caractère personnel, tels que consacrés aux articles 7 et 8 de la Charte des droits fondamentaux de l'Union européenne, soient pleinement respectés.

Deuxième partie : La décision de la Cour de justice de l'Union européenne et la contestation de la directive d'avril 2014

La directive 2006/24 a été invalidée par la CJUE dans l'arrêt qu'elle a rendu dans l'affaire « Digital Rights Ireland »[4].

Deux États membres, l'Irlande et l'Autriche, ont demandé une décision préjudicielle, en joignant à leur demande des observations transmises par les gouvernements de l'Irlande, de l'Autriche, de l'Espagne, de la France, de l'Italie, de la Pologne, du Portugal, du Royaume-Uni, ainsi que par le Parlement européen, le Conseil de l'Union européenne et la Commission européenne.

L'arrêt cite l'article 5 de la directive 2006/24/CE qui énumère les catégories de données à conserver[5] et qui prévoit au paragraphe 2 qu'**« aucune donnée révélant le contenu de la communication ne peut être conservée au titre de la présente directive. »**

Dans son arrêt, la Cour a déclaré que :

> *« même si la directive sur la conservation des données n'autorise pas la conservation du contenu de la communication et des informations consultées en utilisant un réseau de communications électroniques, la Cour « n'exclut pas » que la conservation des données en cause puisse avoir une incidence sur l'utilisation, par les abonnés ou les utilisateurs inscrits, des moyens de communication visés par cette directive et, en conséquence, sur l'exercice par ces derniers de leur liberté d'expression, garantie par l'article 11 de la Charte des droits fondamentaux de l'Union européenne. »* [6]

La directive interfère sérieusement avec les droits au respect de la vie privée et des communications et à la protection des données à caractère personnel, consacrés aux articles 7 et 8 de la Charte.

En résumé, la décision de la CJUE a été rendue au motif qu'«en adoptant la directive 2006/24, le législateur de l'Union européenne avait excédé les limites qu'impose le respect du principe de proportionnalité au regard des articles 7 [respect de la vie privée et familiale], 8 [protection des données à caractère personnel] et 52(1) [limitation des droits], de la Charte [des droits fondamentaux de l'Union européenne].»

---

[3] Ainsi que la directive 2002/58/CE

[4] Arrêt du 8 avril 2014 rendu dans les affaires jointes C-293/12 Digital Rights Ireland et C-594/12 Seitlinger http://curia.europa.eu/juris/document/document.jsf?docid=150642&doclang=FR

[5] (a) les données nécessaires pour retrouver et identifier la source d'une communication ; (b) les données nécessaires pour identifier la destination d'une communication ; (c) les données nécessaires pour déterminer la date, l'heure et la durée d'une communication ; (d) les données nécessaires pour déterminer le type de communication ; (e) les données nécessaires pour identifier le matériel de communication des utilisateurs ou ce qui est censé être leur matériel ; (f) les données nécessaires pour localiser le matériel de communication mobile.

[6] Je remercie Baker & McKenzie qui nous a fourni des informations utiles en avril 2014 http://www.bakermckenzie.com/files/Publication/fcf2ef80-c7f6-4361-a782-660857c40248/Presentation/PublicationAttachment/cac82cb1-74a4-4451-bef6-6829c1ecf1c5/ALGermanyPublicLawApril2014.pdf

La Cour a estimé que la conservation des données n'était pas « *de nature à porter atteinte au contenu essentiel du droit fondamental à la protection des données à caractère personnel* » et était, en principe, justifiée par un objectif d'intérêt général, à savoir la poursuite d'infractions graves, afin de garantir la sécurité publique. [7]

L'importance de cet arrêt réside dans le fait que la Cour a considéré que la directive violait le principe de proportionnalité qui requiert *« que les actes des institutions de l'Union soient aptes à réaliser les objectifs légitimes poursuivis par la réglementation en cause et ne dépassent pas les limites de ce qui est approprié et nécessaire à la réalisation de ces objectifs. »*

La Cour a estimé que, bien que la conservation des données puisse être considérée comme *« apte à réaliser l'objectif poursuivi »* par la directive, les mesures de conservation prévues par la directive ne pouvaient pas être considérées comme « nécessaires » à la réalisation de l'objectif légitime (para. 46, 51 sq.). Selon la Cour, le législateur de l'UE a dépassé les limites imposées par le principe de proportionnalité et la directive était donc invalide.

> *La directive sur la conservation des données couvre toute personne et tous les moyens de communication électronique ainsi que l'ensemble des données relatives au trafic sans qu'aucune différenciation, limitation ni exception ne soient opérées en fonction de l'objectif de lutte contre les infractions graves. En particulier, la directive s'applique même à des personnes pour lesquelles il n'existe aucun indice de nature à laisser croire que leur comportement puisse avoir un lien, même indirect ou lointain, avec des infractions graves.*[8]
>
> *De même, elle ne requiert aucune relation entre les données dont la conservation est prévue et une menace pour la sécurité publique et, notamment, elle n'est pas limitée à une conservation portant soit sur des données afférentes à une période temporelle, à une zone géographique déterminée ou à un cercle de personnes données susceptibles d'être mêlées d'une manière ou d'une autre à une infraction grave, soit sur des personnes qui pourraient, pour d'autres motifs, contribuer, par la conservation de leurs données, à la prévention, à la détection ou à la poursuite d'infractions graves.*

Même les personnes dont la communication devrait être soumise au secret professionnel, y compris au secret professionnel de l'avocat, serait couvertes par cette protection générale. En outre, la Cour a reproché à la directive de ne fixer aucun critère objectif permettant de délimiter l'accès des autorités nationales compétentes aux données et leur utilisation ultérieure.

Selon la Cour, il conviendrait de subordonner l'accès aux données et leur conservation par une autorité nationale compétente à un contrôle préalable effectué soit par une juridiction, soit par une entité administrative indépendante.[9] La Cour a également estimé que la conservation des données pendant une période d'au moins six mois sans que soit opérée une quelconque distinction entre les catégories de données ne se justifiait pas au regard du principe de proportionnalité. La direction n'offrait pas non plus les garanties suffisantes pour assurer une protection efficace des données pendant la période de conservation.

Troisième partie : Les États membres de l'UE

La décision préjudicielle a été demandée par l'Irlande et l'Autriche, et la décision couvre désormais leur jurisprudence nationale.

[7] Arrêt de la Cour (grande chambre) du 8 avril 2014. Paragraphe 39
[8] Arrêt de la Cour (grande chambre) du 8 avril 2014. Paragraphe 58 **« En outre, elle ne prévoit aucune exception, de sorte qu'elle s'applique même à des personnes dont les communications sont soumises, selon les règles du droit national, au secret professionnel. »**
[9] Arrêt de la Cour (grande chambre) du 8 avril 2014. Paragraphe 62

Dans tous les autres États membres de l'UE, les dispositions de droit national transposant la directive sur la conservation des données resteront en vigueur jusqu'à ce qu'elles soient contestées, conformément aux règles de procédure nationales, devant les juridictions nationales. Certaines des informations ci-dessous sont tirées du site internet de Baker & McKenzie.[10]

En **France,** par exemple, les dispositions de droit national qui transposent la directive sur la conservation des données peuvent être contestées devant le Conseil constitutionnel au moyen d'une question prioritaire de constitutionnalité résultant d'une instance en cours.

En **Allemagne,** la Cour constitutionnelle fédérale avait considéré, dans un arrêt daté du 2 mars 2010, que les dispositions de la loi allemande transposant la directive sur la conservation des données violaient le droit fondamental à la confidentialité des communications électroniques garanti par la loi fondamentale allemande. À la suite de l'arrêt de la Cour constitutionnelle, le gouvernement fédéral allemand n'a pas tenté de faire adopter une nouvelle loi de transposition de la directive sur la conservation des données conforme aux exigences exposées dans l'arrêt de la Cour constitutionnelle fédérale, et ce, en dépit de la procédure d'infraction que la Commission européenne avait engagée contre la République fédérale d'Allemagne.

En **Italie**, la section concernée du Code italien de protection des données peut être contestée devant la Cour constitutionnelle italienne (*Corte Costituzionale*).

En **Pologne**, le tribunal constitutionnel doit statuer sur plusieurs demandes d'annulation des dispositions de droit national qui transposent la directive de l'UE sur la conservation des données et il faut s'attendre à ce que le tribunal déclare la réglementation nationale nulle et non avenue.

En **Roumanie**, les droits en matière de communications sont protégés par l'article 28 de la Constitution, et un Avocat du Peuple indépendant est chargé d'entendre les plaintes, mais il est critiqué car il ne donne aux citoyens que peu accès à la justice.

En **Espagne**, la législation nationale peut être contestée devant la Cour constitutionnelle qui évaluerait les dispositions par rapport aux principes nationaux en matière de protection des données et les droits fondamentaux, probablement avec une issue identique à l'arrêt de la CJUE.

Au **Royaume-Uni**, trois mois après l'arrêt de la CJUE, le gouvernement britannique a fait adopter en urgence la loi relative à la conservation des données et aux pouvoirs d'investigation (*Data Retention and Investigatory Powers Act* (DRIPA) 2014). Il propose à présent d'amender la DRIPA[11] afin de conserver des données supplémentaires relatives aux adresses IP. Par ailleurs, le ministère de l'Intérieur a mené des consultations sur la révision des codes de bonnes pratiques en matière de collecte et de divulgation des données de communication et en matière de conservation des données de communication, dans le cadre de la loi relative à la régulation des pouvoirs d'investigation (*Regulation of Investigatory Powers Act* (RIPA)) adoptée en 2000. La consultation sur les codes de bonnes pratiques entend prendre en compte les remarques de la CJUE disant que toute personne, même celles dont les communications devraient être couvertes par le secret professionnel, peut voir ses données de communication interceptées et conservées. L'absence de contrôle judiciaire ou indépendant de même que la proposition d'accroître les pouvoirs en matière de conservation des données ont suscité de vives inquiétudes.

De manière générale, les fournisseurs de services publics de communication ou de réseaux publics de communication resteront soumis aux obligations nationales en matière de conservation des

[10] http://www.bakermckenzie.com/files/Publication/fcf2ef80-c7f6-4361-a782-
[11] Par le biais de l'article 17 de son projet de loi sur la sécurité et la lutte contre le terrorisme (*Counter-Terrorism and Security Bill*)

données tant que les dispositions de droit national les concernant ne seront pas invalidées au niveau de l'État membre. Baker & McKenzie fait remarquer qu'il est probable que la Commission européenne relance ses efforts pour établir un cadre juridique en harmonisant les dispositions des État membres en matière de conservation des données aux fins de la recherche, de la détection et de la poursuite d'infractions graves, en prenant en compte les considérations détaillées sur le principe de proportionnalité formulées par la CJUE.

À l'avenir, il faut s'attendre à ce que de la législation européenne fixe des obligations nouvelles (et « améliorées ») en matière de conservation des données qui exigeront des entreprises de télécommunications qu'elles conservent les données soumises à des exigences de sécurité strictes dans des installations de stockage des données « à l'intérieur de l'Union européenne ». Ces centres de données devront faire l'objet de « contrôles » réalisés en conformité avec la législation européenne par « une autorité indépendante ».

Il reste à savoir si la Commission européenne optera pour l'harmonisation des règles européennes sur la conservation des données sur la base d'une nouvelle directive ou pour le recours à l'instrument juridique qu'est le « règlement ». Vu le temps que prendrait la transposition d'une directive en droit national et le patchwork de règles nationales différentes qui en résulterait probablement, il est possible que la Commission européenne opte pour un règlement sur la conservation des données qui produirait un effet juridique direct dans les États membres et éviterait la longue procédure de transposition en droit national.[12]

Quatrième partie : Rapport des Nations Unies sur les Droits de l'Homme et le Terrorisme

Le 23 septembre 2014, le rapport du Rapporteur spécial[13] sur la promotion et la protection des droits de l'homme et des libertés fondamentales dans la lutte antiterroriste a été présenté à l'Assemblée générale.[14]

Le Rapporteur spécial décrit le rythme du changement technologique comme « dynamique », « ce qui a permis à certains États d'obtenir un accès global aux données de communication et à leur contenu sans soupçon préalable. Les [autorités compétentes de ces] États sont maintenant en mesure d'appliquer des algorithmes "d'exploration de données" automatique pour traquer l'univers potentiellement illimité du trafic des communications. »[15] L'article 17 du Pacte international relatif aux droits civils et politiques prévoit que toute immixtion dans les communications privées doit être prévue par la loi et doit être un moyen nécessaire et proportionné d'atteindre un objectif de stratégie publique légitime.[16] Selon le Rapporteur spécial, l'existence de programmes de surveillance de masse constitue une immixtion potentiellement disproportionnée dans le droit à la vie privée.[17]

Dans son rapport rendu le 30 juin 2014[18], le Haut Commissaire aux droits de l'homme a conclu que les pratiques suivies par de nombreux États ont fait apparaître l'absence de législation nationale et/ou de mesures d'application des lois adéquates, la faiblesse des garanties procédurales et l'inefficacité du contrôle, lesquels ont tous contribué à ce qu'il n'y ait pas d'obligation de rendre des comptes pour les atteintes arbitraires ou illégales au droit à la vie privée.

[12] Newsletter d'avril de Baker & McKenzie, avril 2014
[13] Ben Emmerson
[14] http://s3.documentcloud.org/documents/1312939/un-report-on-human-rights-and-terrorism.pdf
[15] Paragraphe 8 du rapport des Nations Unies sur la promotion et la protection des droits de l'homme et des libertés fondamentales dans la lutte antiterroriste
[16] Paragraphe 11 du rapport des Nations Unies sur la promotion et la protection des droits de l'homme et des libertés fondamentales dans la lutte antiterroriste
[17] Paragraphe 18 du rapport des Nations Unies sur la promotion et la protection des droits de l'homme et des libertés fondamentales dans la lutte antiterroriste
[18] A/HRC/27/37

Cinquième partie : La FBE et la conservation des données

En vue de soumettre des recommandations à l'Union européenne, la Commission des droits de l'homme de la FBE propose à la discussion les points suivants :

1. Les communications soumises au secret professionnel de l'avocat doivent être exemptées de toute mesure de conservation des données, à moins qu'une ordonnance judiciaire ait été délivrée pour accéder aux données aux fins de la recherche, de la détection et de la poursuite d'infractions graves ;
2. Les communications exigeant le secret professionnel de l'avocat devraient être identifiées à la source ;
3. Les États devraient définir des critères clairs et transparents pour la conservation des données, conformément aux fins de recherche, de détection et de poursuite d'infractions graves ;
4. Les données conservées par les gouvernements doivent l'être dans des conditions sûres ;
5. Il conviendrait de prévoir des dispositions visant à la destruction irréversible des données à l'issue de la période de conservation ;
6. Les États devraient mettre en place des organismes de contrôle forts etindépendants, disposant de ressources suffisantes ;[19]
7. Les États devraient mettre en place des tribunaux où chacun pourrait rechercher une réparation effective pour toute violation en ligne alléguée de ses droits à la vie privée ; [20]
8. Les États devraient mettre en place une instance indépendante capable de procéder à un examen approfondi et impartial ;[21]
9. Tous les États membres devraient posséder une législation qui protège le stockage et la divulgation des données à des tiers ;
10. Les fonctionnaires travaillant dans les gouvernements nationaux, régionaux et locaux doivent être liés par les mêmes dispositions en matière de protection des données que celles s'appliquant aux gouvernements ;
11. La divulgation devrait entraîner des sanctions pénales ;
12. L'UE doit mettre en place des règles afin de prévenir l'interception de données par des acteurs non étatiques ;
13. Les avocats doivent faire connaître leurs préoccupations quant à l'impact de la rupture de la relation client-avocat sur la société, sur l'accès à la justice et sur l'État de droit ;
14. Il conviendrait de prévoir une législation nationale dans les États membres visant à consacrer les droits numériques ;
15. Il conviendrait de créer une charte européenne des droits numériques ;
16. Il conviendrait de créer une charte mondiale des droits numériques ;

La Commission des droits de l'homme de la FBE présentera cet article à Barcelone et le soumettra à la Présidence pour discussion et adoption.

Sixième partie : Des solutions de protection pratiques pour les avocats - quelques suggestions :

Tor (réseau anonyme) T O R : The Onion Router (le routeur oignon)

Il s'agit d'un logiciel gratuit permettant de rendre anonymes les échanges en ligne. Tor fait passer les flux internet par un réseau mondial constitué de 5 000 nœuds bénévoles afin de cacher la situation

[19] Paragraphe 61 du rapport du Rapporteur spécial des Nations Unies sur la promotion et la protection des droits de l'homme et des libertés fondamentales dans la lutte antiterroriste
[20] Paragraphe 61 du rapport du Rapporteur spécial des Nations Unies sur la promotion et la protection des droits de l'homme et des libertés fondamentales dans la lutte antiterroriste
[21] Paragraphe 61 du rapport du Rapporteur spécial des Nations Unies sur la promotion et la protection des droits de l'homme et des libertés fondamentales dans la lutte antiterroriste

géographique et l'activité de navigation de l'utilisateur. Il est conçu pour protéger la vie privée des utilisateurs ainsi que leur capacité à communiquer de manière confidentielle en empêchant la surveillance de leurs activités sur l'internet.

L'expression « routage en oignon » fait référence aux couches de chiffrement qui rappellent celles d'un oignon. Tor chiffre les données originales, y compris l'adresse IP de destination, à de multiples reprises et les envoie dans un circuit virtuel comprenant des nœuds Tor successifs choisis de manière aléatoire. Chaque nœud déchiffre une couche qui ne révèle que le nœud suivant du circuit afin de lui transmettre les données chiffrées restantes. Le nœud final déchiffre la toute dernière couche et envoie les données originales à sa destination sans révéler, ni même d'ailleurs connaître, l'adresse IP d'origine. Le routage de la communication étant partiellement caché à chaque étape du circuit Tor, cette méthode élimine tout point au niveau duquel la surveillance du réseau pourrait lever l'anonymat de la communication en ayant connaissance de sa source et de sa destination. Tor se distingue par son indépendance de la plupart des autres réseaux permettant l'anonymat : il fonctionne au niveau du flux TCP (*Transmission Control Protocol*).

Pretty Good Privacy (PGP) (Assez Bonne Confidentialité)

PGP est un logiciel de chiffrement et de déchiffrement de données qui garantit la confidentialité et l'authentification de la communication de données. PGP sert à signer, chiffrer et déchiffrer des textes, des e-mails, des fichiers, des répertoires et à accroître la sécurité des communications par e-mail. PGP peut être utilisé pour envoyer des messages confidentiels. PGP associe le chiffrement à clé symétrique et le chiffrement à clé publique. Le message est chiffré à l'aide d'un algorithme de chiffrement symétrique qui requiert une clé symétrique. Chaque clé symétrique n'est utilisée qu'une seule fois (et est ainsi également appelée clé de session). Le message et sa clé de session sont envoyés au destinataire. La clé de session doit être envoyée au destinataire afin que le message puisse être déchiffré. Pour protéger le message durant la transmission, il est chiffré à l'aide de la clé publique du destinataire. Seule la clé privée appartenant au destinataire peut déchiffrer la clé de session.

La Commission des droits de l'homme recommande aux membres de la FBE d'encourager les associations d'avocats dans leurs pays à rechercher et à utiliser des moyens de communication numérique sécurisés.

Professeur Sara Chandler, présidente de la Commission des droits de l'homme, avec mes remerciements à Timothy Hill, Law Society of England & Wales