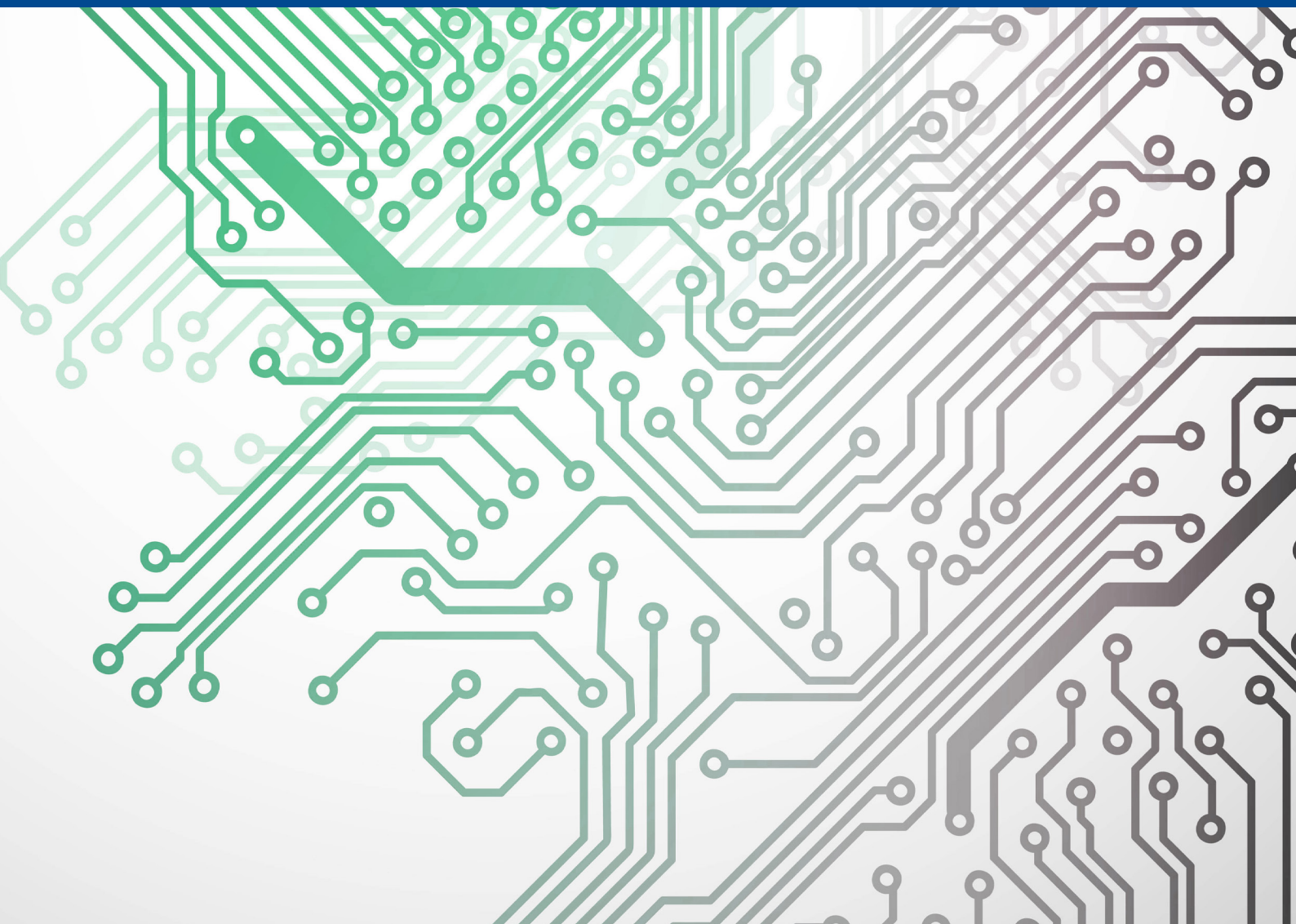
EUROPEAN LAWYERS
EUROPEAN BARS
CCBE
BARREAUX EUROPÉENS
AVOCATS EUROPÉENS

CONSEILS DU CCBE

pour le renforcement de la sécurité informatique des avocats contre la surveillance illégale



CONTACT:

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

Suivez-nous sur
www.ccbe.eu
ccbe@ccbe.eu

AVERTISSEMENT:

Cover illustration / *illustration de la couverture*:
© littlestocker - Fotolia.com

SOMMAIRE

INTRODUCTION

1

L'obligation qu'a l'avocat de garder secrètes ses communications avec le client, ainsi que les informations reçues de son client et les conseils qu'il lui prodigue est une composante essentielle de l'état de droit dans une société libre et démocratique. Il s'agit toutefois d'une valeur de plus en plus menacée, que ce soit par des moyens d'intervention illicite de la part de tiers ou, dans certains cas, la surveillance effectuée par les gouvernements, qui n'est pas suffisamment réglementée.

En ce qui concerne la surveillance de la part des gouvernements, les Recommandations du CCBE sur la protection du secret professionnel dans le cadre des activités de surveillance ont été publiées en mai 2016 afin 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 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[1].

Le danger est toutefois reconnu que, dans certaines juridictions, les contrôles prévus dans la réglementation sur la surveillance par le gouvernement peuvent ne pas être tout à fait adaptés et partout plane le risque d'une interception non autorisée ou illégale par des tiers. Ces conseils sont dès lors destinés à offrir des conseils pratiques aux barreaux européens quant aux mesures que les avocats et les cabinets d'avocats peuvent prendre pour assurer la protection nécessaire des informations relevant du secret professionnel et des obligations en matière de protection des données.

Ces conseils sont destinés aux barreaux membres du CCBE, qui sont invités à examiner l'idée de les incorporer (dans la mesure où ils s'appliquent à leur juridiction) dans leurs lignes directrices à l'attention de leurs propres membres.

Ils sont divisés en deux parties : un aperçu approfondi de la manière dont les avocats pourraient approcher les questions de sécurité informatique, puis des conseils spécifiques concernant le type de mesures techniques que les avocats peuvent prendre pour se protéger de la surveillance illégale ou toute autre ingérence dans leur système informatique.

1 http://www.ccbe.eu/fileadmin/speciality_distribution/public/documents/SURVEILLANCE/SVL_Position_papers/FR_SVL_20160428_CCBE_recommendations_on_the_protection_of_client_confidentiality_within_the_context_of_surveillance_activities.pdf

APERÇU DES POSSIBILITÉS D'AMÉLIORATION DU NIVEAU DE SÉCURITÉ INFORMATIQUE DES AVOCATS

2

1. Garantir le secret professionnel comme principe essentiel de la profession d'avocat

La *Charte des principes essentiels de l'avocat européen*[2] précise qu'il est du devoir de l'avocat de respecter le secret professionnel et la confidentialité des affaires dont il a la charge. Le respect du secret professionnel est à la fois une obligation de l'avocat et un droit de l'homme fondamental du client, qui doit être respecté par tous.

Les cadres réglementaires que les États ont adoptés individuellement et qui garantissent ce principe connaissent des variations et, dans un certain nombre de juridictions, la surveillance gouvernementale peut constituer une menace potentielle à ce principe.

Dans son rapport de 2014 « Paysage des menaces », l'Agence de l'Union européenne chargée de la sécurité des réseaux et de l'information (ENISA) a souligné que « *les violations de la vie privée que les médias ont révélées quant aux pratiques de surveillance ont affaibli la confiance des utilisateurs vis-à-vis d'Internet* »[3]. En outre, la résolution du Parlement européen du 12 mars 2014, 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* indique dans ses conclusions qu'il « juge capital de protéger le secret professionnel des avocats […] contre les activités de surveillance de masse ; souligne en particulier que toute incertitude concernant la confidentialité des communications entres 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 »[4].

Le CCBE a, pour les mêmes raisons, exprimé de manière répétée depuis 2013 sa profonde préoccupation du fait que de telles pratiques compromettent non seulement la valeur essentielle de la profession d'avocat, mais aussi la confiance envers l'état de droit, ce qui a abouti à la publication en mai 2016 des *Recommandations du CCBE sur la protection du secret professionnel dans le cadre des activités de surveillance*. Malgré la présence du risque à la fois de surveillance gouvernementale et d'accès illégal par des tiers aux systèmes et données informatiques, il est impossible pour les avocats d'exercer sans avoir recours à des systèmes informatiques, notamment pour envoyer et recevoir des courriels et utiliser Internet. En effet, l'utilisation d'Internet et l'adoption de solutions informatiques en nuage étant de plus en plus courante chez les clients, les avocats peuvent être fortement empressés par leurs clients d'utiliser ces systèmes eux-mêmes.

Le Code de déontologie des avocats européens établit l'obligation pour les avocats de respecter le secret de toute information confidentielle, tout en exigeant qu'ils maintiennent et développent leurs connaissances et leurs compétences professionnelles[5].

De ces exigences découle un impératif de plus en plus présent pour les avocats d'acquérir les compétences pouvant s'avérer nécessaires pour garantir la protection des informations confidentielles des clients dans le monde virtuel.

Ces conseils ont donc pour objet d'aborder les possibilités qu'ont les barreaux pour améliorer la sécurité informatique des avocats en informant leurs membres (y compris, en particulier, les avocats exerçant seuls et les petits cabinets d'avocats, qui peuvent ne pas avoir accès à la même expertise technique que les grands cabinets) de certaines des solutions possibles. Les conseils ne sont pas là pour aborder l'utilisation technique d'outils spécifiques, ni donner des

2 http://www.ccbe.eu/fileadmin/speciality_distribution/public/documents/DEONTOLOGY/DEON_CoC/FR_DEON_CoC.pdf
3 https://www.enisa.europa.eu/activities/risk-management/evolving-threat-environment/enisa-threat-landscape/enisa-threat-landscape-2014
4 http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P7-TA-2014-0230+0+DOC+XML+V0//FR
5 Voir les articles 2.3.2, 2.3.4 et 5.8 du Code de déontologie des avocats européens.

recommandations détaillées quant à l'infrastructure ou aux produits informatiques particuliers dans lesquels les barreaux et les avocats devraient investir.

2. Connaître les bases de la sécurité informatique

Il peut s'avérer nécessaire aux avocats d'investir dans des systèmes de sécurité informatiques, des outils de protection et des outils de chiffrement, mais il est également nécessaire pour y parvenir que l'avocat ait une bonne connaissance de l'environnement dans lequel ces outils évoluent. Par exemple, il est inutile d'utiliser des outils de chiffrement si un pirate a pris le contrôle à un point de terminaison où a lieu le déchiffrement et l'enregistrement d'informations de manière non chiffrée.

Un certain degré de connaissance minimum en sécurité informatique est une compétence de base importante pour tout avocat travaillant avec des systèmes informatiques. Même si l'avocat choisit de déléguer ou de sous-traiter auprès d'experts techniques la prise de mesures spécifiques pour assurer la sécurité informatique en général ou la confidentialité en particulier, un niveau minimum de connaissances et de compétences doit encore entrer dans la gestion des cabinets d'avocats. Dans le cas contraire, les avocats du cabinet seront personnellement responsables de l'absence de contrôles de sécurité informatique, tout comme ils le seraient en cas d'absence de contrôles internes pour la gestion des fonds ou des documents des clients.

Par conséquent, avant d'envisager des mesures techniques, il est nécessaire d'insister sur la nécessité d'assurer un niveau de connaissance minimum commun à tous les avocats en matière de sécurité informatique.

3. S'appuyer sur l'expérience commune

Les obligations imposées aux avocats en matière de sécurité informatique par la loi de l'Union européenne sont exprimées de manière générale et tendent à s'inscrire dans le contexte précis de la protection des données, par exemple, les exigences de l'article 17 de la directive sur la protection des données 95/46/CE. Ni le nouveau règlement général sur la protection des données, ni le projet de directive sur la sécurité des réseaux et de l'information ne devraient changer cette approche législative dans un avenir proche. En conséquence, la réalisation technique des normes exigées par la loi en matière de protection des données ne se trouvent pas dans les exigences juridiques formelles mais ailleurs, comme dans les pratiques reconnues et les normes officielles du secteur.

Ces conseils n'ont néanmoins pas pour objet de se confondre en détails sur des solutions informatiques particulières. En raison de la grande variété de systèmes informatiques et d'outils utilisés, il serait de toute évidence inutile de discuter des détails techniques ici.

Au contraire, ce document part du principe plus large qu'un bon point de départ serait l'approche générale en matière de sécurité informatique que d'autres professions et secteurs ont déjà prise, à savoir d'appliquer, le cas échéant, les normes reconnues déjà utilisées dans la sécurité informatique. En plus d'être en soi raisonnable, elle présente l'avantage accessoire du fait que la capacité d'un avocat à démontrer qu'il respecte les normes déjà appliquées dans d'autres secteurs tend à renforcer la confiance des clients dans la garantie que leurs données et leurs communications sont protégés.

En outre, elle a) aide les avocats à comparer leur propre niveau de sécurité informatique à celui des autres professions et secteurs et b) facilite la réutilisation des expériences, des politiques et des détails (contrôles) techniques applicables déjà utilisés dans d'autres secteurs.

En conséquence, les barreaux devraient aider les avocats à acquérir une bonne compréhension de l'utilité des normes de sécurité informatique concernées, sans nécessairement obliger tous les cabinets d'avocat à obtenir la certification de ces normes. En effet, étant donné que les normes de sécurité informatique sont formulées de manière tellement générique que seuls les spécialistes de la sécurité informatique peuvent les appliquer directement (et dans de nombreux cas, le personnel informatique des cabinets d'avocats peut ne pas avoir l'expertise appropriée) le but de mieux faire connaître les normes aux avocats est de ne pas leur imposer de disposer d'une certification de ces normes, mais plutôt de leur offrir un aperçu du type d'approche systématique et structurée qu'ils peuvent suivre.

En outre, selon les exigences minimales formulées dans la deuxième partie de ce guide, il est recommandé aux barreaux de :

- examiner de manière suffisamment approfondie l'état d'avancement de la préparation de la sécurité informatique des avocats dans leur juridiction ;
- le cas échéant, émettre des recommandations à leurs membres, qui traduisent, communiquent et si nécessaire localisent les exigences énoncées dans les présents conseils et dans les normes de sécurité informatique pertinentes ;
- faire connaître les normes pertinentes et les expliquer à leurs membres ;
- s'assurer que toute recommandations ou ligne directrice qu'ils émettent est conforme aux normes de sécurité informatique pertinentes ;
- garantir la conformité de leurs membres à ces recommandations ou lignes directrices.

Certains barreaux ont déjà répondu à l'une ou plusieurs des questions énoncées ci-dessus[6], organisé une formation spécifique, ou publié des documents à ce sujet[7]. Ce type de matériel constitue un point de départ ou une référence pratique pour d'autres barreaux en Europe.

Les mesures prises dans ce domaine sont bénéfiques non seulement aux avocats exerçant seuls, mais plus encore à leurs clients. Les barreaux devraient par conséquent envisager, au moment de publier ces lignes directrices à leurs membres, d'informer également le grand public et les clients des lignes directrices ou des recommandations pour en faire la promotion. Les barreaux peuvent ainsi sensibiliser les clients au fait que les avocats continuent de prendre au sérieux, indépendamment du canal de communication employé, la protection des renseignements confidentiels de ces derniers.

6 Ex. Conseil National des Barreaux http://cnb.avocat.fr/Securite-de-l-information-au-sein-des-cabinets-deux-guides-mis-a-disposition-de-la-Profession_a1191.html, notes de *la Law Society of England and Wales*, par ex. http://www.lawsociety.org.uk/support-services/advice/practice-notes/information-security/, ou le barreau hongrois : http://www.magyarugyvedikamara.hu/common/file-servlet/document/898/default/doc_url/160113_Utmutato_IT_biztonsaghoz_kamarai1096398_1.pdf

7 Ex. *Cyber Security Toolkit* de Peter Wright, publié par Law Society Publishing, ou l'*ABA Cybersecurity Handbook: A Resource for Attorneys, Law Firms and Business Professionals*.

MESURES TECHNIQUES DE LUTTE CONTRE LA SURVEILLANCE ILLÉGALE

3

1. Aperçu des normes applicables en matière de sécurité informatique

Il existe de nombreuses normes mondiales différentes en matière de sécurité informatique. Certaines de ces normes sont connues, mais n'offrent pas de cadre adéquat pour régir la manière dont chaque profession, dont les avocats, pourrait effectivement assurer un niveau élevé de sécurité informatique. Par exemple, la norme des « critères communs » (CC), bien connue, définit des profils de protection pour des catégories spécifiques d'utilisation, par exemple pour le chiffrement des lecteurs flash USB, pour les distributeurs de billets ou des applications de création de signatures électroniques. Au-delà des profils de protection, les CC permettent d'évaluer si certains produits et systèmes spécifiques (« objectifs de sécurité ») sont conformes à ces profils ou non. Il s'agit donc davantage de faire en sorte qu'un produit ou un système spécifique soit conforme à des exigences spécifiques prédéfinies, telles que la sécurité informatique commerciale générique. Dès lors, même si cette norme revêt un certain intérêt pour les avocats en ce qui concerne le matériel et les produits liés à la sécurité (clés USB, cartes à puce, pare-feu, etc.) qu'ils peuvent utiliser, elle ne constitue pas l'objet des questions abordées ici.

Une autre norme mondiale largement utilisée est CobiT (*Control Objectives for Information and related Technology*, en français Objectifs de contrôle de l'information et des technologies associées). Cette norme dispose actuellement d'une portée très vaste, et se définit comme un cadre pour la gouvernance et la gestion des technologies au sein des entreprises, y compris la gestion de la sécurité informatique. Compte tenu de sa portée, cette norme ne semble concerner que les organisations dont l'infrastructure informatique est complexe et qui sont en mesure de l'adopter en tant qu'approche globale de l'informatique et de traduire les exigences opérationnelles en exigences informatiques, ou de manière à garantir le maintien du contrôle de gestion sur les fonctions informatiques. Cette norme se concentre clairement sur d'autres aspects que ceux qui posent problème actuellement à la majorité des avocats et des petits cabinets d'avocats.

En effet, sur le petit nombre de familles de normes de sécurité informatique à l'échelle mondiale, seules deux sont applicables à la gestion des risques de sécurité informatique des avocats, à savoir :

(a) FIPS 800-53 et *FIPS Cybersecurity* Framework *(and related standards)* du NIST[8]

(b) Les normes basées sur la norme ISO 27000.

La deuxième partie de ces conseils a pour objet d'offrir, en partant de ces normes, des recommandations plus détaillées. Le point 7 en particulier constitue un exemple plus détaillé de la manière d'aborder un aspect spécifique des risques, à savoir la confidentialité des communications entre le client et l'avocat.

a) Normes du NIST

Les normes publiées par le *National Institute of Standards and Technologies of the United States of America* (NIST) sont plus accessibles et peuvent servir de point de départ aux discussions sur les cadres de sécurité informatique des avocats. La norme *NIST Special Publication 800-53 (Security and Privacy Controls for Federal Information Systems and Organizations)* concerne les contrôles de sécurité génériques pour les systèmes informatiques fédéraux. Cette norme fortement utilisée et connue est très détaillée. Elle comporte cependant peut-être trop de détails

8 FIPS Cybersecurity Framework. FIPS 800-53: NIST Special Publication 800-53 Revision 4, April 2013, Security and Privacy Controls for Federal Information Systems and Organizations.

pour la taille moyenne d'un cabinet d'avocat en Europe. En outre, l'évaluation de la conformité à cette norme peut constituer un exercice difficile pour les cabinets d'avocats dans le contexte européen. Le *FIPS*[9] *Cybersecurity Framework (and related standards)* [10] (également publié par le NIST) est un autre cadre plus générique et concis qui correspond mieux à l'utilisation des organisations plus petites telles que le cabinet d'avocat moyen. En outre, le fait qu'un projet de conseils pratiques pour les petits cabinets a déjà été publié[11] constitue un avantage certain.

b) Normes ISO

Enfin, il existe un équivalent ISO pour la mise en œuvre des normes de gestion de la sécurité informatique, les normes fondées sur ISO 27000, qui comprend des normes pour lesquelles les organisations peuvent recevoir des certifications, comme ISO 9001. Des lignes directrices techniques suffisamment détaillées telles que ISO 27002 ont été publiées, ainsi qu'un certain nombre de lignes directrices pour les petites entreprises[12].

Les familles de normes évoquées ci-dessus suivent le même principe, mais elles présentent de légères différences dans les niveaux de détail, le public visé et la manière dont la conformité à ces normes est prouvée.

Bien sûr, le nombre de normes de sécurité informatique est beaucoup plus grand et leur portée va au-delà que ce qui a été expliqué ci-dessus. Cependant, la plupart de ces normes de sécurité informatique entre dans un ou plusieurs des cadres abordés ci-dessus étant donné qu'elles concernent un aspect particulier du cadre informatique plus générique.

2. Mesures minimales essentielles pour un système de gestion de sécurité efficace

Afin de développer un système basique de sécurité de l'information, un cabinet d'avocats ou un avocat exerçant seul devrait, en tenant compte du domaine du droit du cabinet, de sa clientèle habituelle, et des compétences de son personnel, commencer par les étapes suivantes :

- identifier ses ressources principales d'information, en particulier les informations et les documents des clients, les principaux services et registres qui sont essentiels à son fonctionnement ;
- une fois ces ressources principales identifiées, le cabinet d'avocats devrait également identifier les failles de sécurité qui auraient les pires conséquences possibles sur les activités du cabinet d'avocats (en tenant également compte de la probabilité que ces failles de sécurité se produisent et des conséquences éventuelles) et identifier les solutions permettant de réduire ces risques.

L'avantage de laisser l'évaluation reposer sur les normes de sécurité informatique devient évident au moment où l'on envisage les solutions pour traiter les risques, la manière d'aborder ces solutions et les catégories de solutions. Ces solutions devraient comprendre au moins les aspects suivants :

- contrôler l'accès aux ressources principales d'information (y compris l'identification des utilisateurs des systèmes informatiques en ne leur octroyant que les droits d'accès nécessaires) ;
- définir des zones de sécurité physique avec des contrôles ;

9 FIPS : *Federal Information Processing Standards.*
10 http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf
11 NIST Small Business Information Security: The Fundamentals, http://csrc.nist.gov/publications/drafts/nistir7621-r1/nistir_7621_r1_draft.pdf
12 Voir par ex. *ISO/IEC 27001 for Small Businesses: Practical Advice* d'Edward Humphreys, publié par ISO en 2010.

- sécuriser le recyclage et l'enlèvement du matériel (y compris les appareils mobiles et les supports de données non mobiles) et la sécurité du matériel hors site ;
- sécuriser le réseau (en particulier l'utilisation d'infrastructures partagées comme les réseaux câblés et sans fil) ;
- établir des procédures opérationnelles pour assurer une protection contre les codes malveillants ;
- gérer les mots de passe, les sauvegardes et les rapports des failles de sécurité, etc.[13]

Les mesures exposées au point 7 ci-après constituent un exemple plus détaillé de la manière d'aborder un aspect spécifique des risques, à savoir la confidentialité des communications entre le client et l'avocat.

3. Contrôles de sécurité informatique des appareils mobiles (voir le contrôle 6.2.1 ISO 27001)

Un aspect particulier de l'analyse des risques défendue ci-dessus est le risque particulier qui découle de l'utilisation des appareils mobiles.

Les appareils mobiles, à savoir les ordinateurs portables, les tablettes et les téléphones portables, sont exposés à divers risques, qui correspondent tous à la perte du contrôle des ressources en soi. Ces outils étant utilisés en dehors de l'environnement bien contrôlé que constitue le cabinet, il existe un risque accru de perdre, d'endommager ou de compromettre l'appareil ou les informations qui s'y trouvent. Si une personne malveillante met la main sur l'un de ces appareils, elle sera en mesure de lancer une grande variété d'attaques de sécurité.

Les appareils mobiles nécessitent davantage de contrôles de sécurité que les dispositifs qui demeurent au sein du cabinet. Il n'est pas absolument nécessaire de chiffrer le stockage de masse dans un environnement de bureau, mais cela est indispensable pour un ordinateur portable. En l'absence de mesures de protection adéquates et efficaces, le support de données de l'appareil mobile peut être obtenu facilement grâce à l'utilisation d'outils simples, quelle que soit la fiabilité du mot de passe de l'utilisateur. Alors qu'un mot de passe sécurisé peut protéger les ressources accessibles par le biais d'un réseau, les données disponibles sur des supports amovibles ne peuvent être efficacement protégées que si elles sont également chiffrées. Cela vaut également pour tous les appareils mobiles, y compris les téléphones portables, les clés USB ainsi que, bien entendu, les ordinateurs portables. Le chiffrement à accès contrôlé est facilement disponible et abordable pour tous ces appareils.

En outre, étant donné le risque de vol des appareils, des mesures de protection physique supplémentaires peuvent s'avérer nécessaires : par exemple l'utilisation d'un cadenas de poche permet d'empêcher les ordinateurs portables d'être subtilisés, tout comme des précautions élémentaires telles que le fait de placer les appareils mobiles avec les bagages à main à bord de l'avion plutôt que dans les bagages enregistrés en soute.

Outre la protection physique de ces appareils, les avocats doivent faire attention aux ressources du réseau qui sont utilisées pour se connecter à leurs services à distance ou des emplacements de stockage. Les smartphones et les tablettes peuvent comporter un risque particulier car les utilisateurs ont tendance à mettre en œuvre moins de contrôles de sécurité que pour les ordinateurs portables, alors que les risques sont similaires. Il est important de savoir qu'il est possible d'installer un logiciel antivirus, un pare-feu et une protection contre les sites malveillants sur les appareils mobiles (et, comme indiqué ci-dessus, de chiffrer les données qui

13 La manière de traiter ces risques peut se trouver dans le *Guide de sécurité de l'information pour les avocats* ou le document du NIST *Small Business Information Security: The Fundamentals* http://csrc.nist.gov/publications/drafts/nistir7621-r1/nistir_7621_r1_draft.pdf et, évidemment, les listes plus longues d'ISO 27002 et du NIST FIPS 800-53.

s'y trouvent). Ces logiciels ne sont cependant généralement pas inclus à l'achat d'un appareil mobile et l'utilisateur doit donc prévoir le budget nécessaire, l'acquisition de la licence, ainsi que l'installation et la configuration de ces logiciels.

4. Contrôle de sécurité informatique de protection contre les logiciels malveillants (contrôle 12.2.1 ISO 27001)

Les logiciels malveillants (malware) existent sous nombreuses formes : virus, vers, chevaux de Troie, portes dérobées et logiciels malveillants furtifs, mais la catégorisation exacte des logiciels malveillants ne présente pas d'intérêt aux fins des présents conseils[14].

Les logiciels malveillants peuvent gravement endommager voire détruire les ressources informatiques, donner l'accès (non autorisé) aux données enregistrées, qui peuvent alors être utilisées à des fins malveillantes, ou envoyer aux clients des messages embarrassants provenant du cabinet d'avocats.

Ces codes peuvent infecter les ordinateurs de nombreuses manières, appelées vecteurs d'attaque. Une infection peut encore survenir à l'utilisation de supports amovibles infectés (par exemple de clés USB), mais de nos jours ces codes nocifs viennent généralement de plus loin, en recherche constante d'une nouvelle « victime ». Ils peuvent infecter des ressources en utilisant des adresses électroniques recueillies[15] ou d'autres connexions informatiques (services réseau). Très souvent, les pirates attirent les utilisateurs peu méfiants vers des sites apparemment attrayants ou utiles. Bien entendu, ces codes malveillants peuvent fonctionner par reconnaissance active, par exemple en tentant d'analyser les adresses réseau.

Après avoir obtenu ces adresses, le pirate, à force d'essais répétés, peut efficacement identifier, sur l'appareil ciblé, une vulnérabilité informatique quelconque permettant alors d'exécuter le code non autorisé sur l'appareil[16]. Il n'existe malheureusement aucune plateforme libre de virus disponible aux consommateurs et aux utilisateurs professionnels ayant un niveau de connaissances informatiques similaire[17].

La meilleure ligne de défense d'un cabinet d'avocats consiste à avoir recours à un logiciel adéquat de protection contre les logiciels malveillants. Afin de choisir le bon produit, il convient aussi bien de prendre en compte le budget disponible et les besoins que les résultats publiés par des laboratoires de contrôle européens indépendants concernant l'efficacité prouvée de ces logiciels contre les logiciels malveillants[18]. Cette remarque peut sembler anodine, mais il est surprenant de voir que ce ne sont pas toujours les logiciels les plus connus ni les plus faciles à utiliser qui offriront la meilleure protection.

Les logiciels de protection contre les logiciels malveillants doivent être installés non seulement sur les ordinateurs de bureau et autres types d'appareils fixes, mais également sur les appareils mobiles, tels que les tablettes et les smartphones, si les données des clients ou d'autres informations juridiques importantes se trouvent sur ces appareils[19].

14 Pour davantage de contexte, voir le point 2 du guide suivant : http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-83r1.pdf.

15 En envoyant des codes malveillants en pièce jointe ou en renvoyant l'utilisateur vers des adresses web comprenant des logiciels malveillants.

16 Les points vulnérables des logiciels pouvant servir à recueillir des informations ou à exécuter des codes de manière non autorisée est une « exploitation ».

17 La différence dans le taux de piratages réussis provient souvent du fait que les codes malveillants doivent être programmées pour un certain type d'appareil, ce qui fait que les systèmes moins courants seront moins la cible des attaques des logiciels malveillants.

18 https://www.av-test.org/fr/antivirus/, http://www.av-comparatives.org/dynamic-tests/, https://www.virusbtn.com/vb100/latest_comparative/index

19 Voir l'un des rapports concernant les appareils Android : http://www.av-comparatives.org/wp-content/uploads/2015/09/avc_mob_2015_en.pdf

Les logiciels antivirus n'offrent pas de protection contre toutes les attaques. Selon les laboratoires mentionnés ci-dessus, un taux de détection de plus de 99 % est possible contre les logiciels malveillants déjà identifiés et analysés par les sociétés éditrices de logiciels antivirus. Cependant, un laps de temps important peut s'écouler entre l'apparition d'un logiciel malveillant et son ajout à la base de données des logiciels antivirus, et la stratégie générale des attaques ciblées (par piratage) consiste à exploiter une vulnérabilité qui n'a pas encore fait l'objet d'une mise à jour au sein d'un logiciel antivirus ou sur l'ordinateur cible. Ces vulnérabilités sont connues sous le nom de vulnérabilités au jour zéro (*zero-day*).

Si l'infection a déjà eu lieu et que le logiciel de protection contre les logiciels malveillants est incapable d'en venir à bout, il est recommandé aux avocats de faire appel à des professionnels avant de restaurer les anciennes données à partir de sauvegardes étant donné qu'un logiciel malveillant encore actif peut corrompre les données restaurées. Il est également nécessaire que les cabinets d'avocats exigent que les utilisateurs signalent ce type d'incidents.

La protection contre les logiciels malveillants conduit à la question délicate de savoir quand mettre à jour le logiciel. Les fabricants de logiciels fournissent souvent des mises à jour pour corriger les dernières vulnérabilités découvertes. Installer rapidement toutes les mises à jour et les solutions de réparation permet de réduire considérablement l'exposition aux codes malveillants et aux attaques informatiques ciblées. L'installation de mises à jour comporte néanmoins le danger d'altérer, au lieu de le réparer, un logiciel qui fonctionnait parfaitement auparavant. Les grands cabinets, qui disposent de ressources suffisantes, devraient donc d'abord effectuer des essais avec les mises à jour dans un environnement test approprié, plutôt que sur un ordinateur utilisé pour les dossiers des clients.

5. Contrôles pour l'enlèvement sécurisé des supports employés par les avocats (8.3.2./10.7.2. ISO 27001)

Les données du client font partie des ressources les plus précieuses des avocats et doivent donc être protégées, même une fois qu'elles ne sont plus utiles. La suppression ou la destruction de ces données doit également être sécurisée.

Les données des clients sont hébergées à la fois sur des dispositifs de stockage de données (clés USB, disques durs externes) et des supports intégrés (mémoires SSD/flash par exemple). Ceci doit être gardé à l'esprit lorsque ces appareils sont mis à disposition pour leur entretien ou lors de leur enlèvement ou la vente des appareils qui ne sont plus utilisés. Les avocats doivent garder à l'esprit que ces données sont stockées non seulement sur les ordinateurs, les tablettes et les téléphones intelligents, mais également sur les photocopieurs, scanners et télécopieurs.

Une simple suppression des données stockées ou un reformatage de l'appareil n'empêchera pas un individu déterminé de restaurer les données : des mécanismes de suppression spéciaux devraient être utilisés lors du transfert des supports à l'extérieur de l'organisation, ou alors ces supports de données ne devraient être ni vendus, ni même enlevés.

6. Aperçu des catégories des activités de surveillance et des risques liés (voir par exemple les contrôles réseau et du chiffrement 13.1.1. et 10.1.1. ISO 27001)

Afin d'obtenir un aperçu des outils pouvant aider les avocats à améliorer la sécurité informatique dans le contexte de la surveillance illégale, un certain nombre de scénarios sont présentés ci-après pour présenter les différentes catégories (1) d'activités de surveillance (2) de risques de surveillance et (3) de situations dans lesquelles les avocats sont exposés à de tels risques. L'objectif de ces scénarios est de donner une analyse des mesures permettant d'identifier et d'offrir une protection contre le risque de surveillance illégale. En raison de la compétence extraterritoriale (qui n'est pas exceptionnelle en vertu du droit pénal ou du droit de la concurrence), certaines situations pourraient survenir lorsque les autorités d'un pays procéderaient à des activités de surveillance légale sur son territoire alors qu'elles ne le sont pas dans tous les pays concernés (par exemple, dans le pays de l'autre partie à la communication).

Ces différences devraient normalement être résolues par l'utilisation de méthodes traditionnelles de coopération internationale entre les forces de l'ordre et les agences de sécurité nationales, ce qui ne se produit évidemment pas toujours. Même au sein de l'UE, les États membres peuvent effectuer des opérations pour des raisons de sécurité nationale qui vont à l'encontre des intérêts ou de la législation de l'autre État membre concerné. Dans ce type de cas, la préparation de mesures de protection contre la surveillance des gouvernements serait justifiée en tant qu'acte légitime, souhaitable et utile, à la condition évidente que cela soit techniquement possible. Même si le fournisseur d'un service de communications électroniques (« **ECS** ») est tenu en vertu de son droit local de donner l'accès aux communications effectuées par le biais de son réseau ou de son service, cela ne signifie pas pour autant que la mesure de surveillance sera nécessairement légale. C'est la raison pour laquelle ces situations figurent également dans l'analyse qui suit.

1) Catégories d'activités de surveillance

a) Les activités de surveillance reposant sur la mise à disposition à l'avance, par les fournisseurs de services, de l'accès à une infrastructure spécifique à des organismes habilités à effectuer des activités de surveillance dans leur législation nationale.

b) Les activités de surveillance reposant sur un processus juridique spécifique de surveillance, par exemple l'obtention de mandats ou d'autres autorisations externes. Une distinction peut être établie entre l'accès au contenu des données et l'accès aux métadonnées, mais il est important de savoir que les données sont de plus en plus interprétées comme métadonnées et de plus en plus de données peuvent être recueillies à partir des métadonnées des communications, notamment les communications entre les avocats et leurs clients. Par conséquent, du point de vue de la confidentialité, la différence pratique entre les métadonnées et le contenu des données est infime, et le niveau de la menace envers les communications entre l'avocat et son client est le même dans les deux cas.

c) Les activités de surveillance réalisées de manière non ciblée sur une population entière ou une partie importante de celle-ci (la surveillance de masse). Il s'agit d'une forme de surveillance qui n'est devenue techniquement possible que récemment.

d) Les activités de surveillance ciblées impliquant la collecte de renseignements sur des individus ou des groupes d'individus précis, appelée ici « surveillance ciblée ».

Quoi qu'il en soit, la frontière entre la surveillance de masse et la surveillance ciblée n'est pas clairement définie et peut subir des modifications, en particulier lors d'un contrôle juridictionnel. Par exemple, lorsqu'un tribunal déclare que « la collecte non ciblée d'informations par interception, que ce soit en masse ou non, serait illégale »[20], la question la plus importante est de savoir quel genre de « critères » rendraient la surveillance légale. La surveillance en question ne constituerait une surveillance ciblée qu'à partir du moment où au moins un objet de surveillance est identifié avant le lancement de l'opération.

2) Risques de la surveillance

Du point de vue de l'avocat, les différentes catégories de risques suivants doivent être identifiées.

a) **L'enregistrement d'une conversation** à l'insu des participants (avec ou sans le concours de certains ou de tous les fournisseurs de services qui participent à la réalisation technique de la communication électronique en ligne ou hors ligne, par exemple, avec le concours du fournisseur d'accès à Internet ou d'un fournisseur tiers de courriels ou d'autres systèmes de livraison de messagerie électronique).

b) **L'enregistrement de métadonnées** de la conversation (identifiant ou identité des parties, heure, durée, longueur et volume des messages, emplacement géographique des parties, adresses IP ou adresses physiques d'accès, etc.)

c) **L'accès aux appareils** de communication de l'utilisateur (smartphone ou ordinateur) pour enregistrer des communications ou des métadonnées associées du côté de l'utilisateur ou enregistrer ou accéder aux journaux et à d'autres métadonnées (historique des conversations, etc.) conservées sur l'appareil de l'utilisateur.

d) L'accès à des données lors de la **restauration** de matériel **enlevé** ou à partir de **supports de données**.

e) **L'accès** à des **données non relatives aux conversations**, par exemple les documents stockés, l'historique des recherches ou d'utilisation.

3) Scénarios d'utilisation

Les principaux scénarios d'utilisation qui présentent des risques possibles de surveillance sont les suivants :

a) L'avocat communique avec un client ou un autre avocat (par téléphone classique du bureau, voix sur IP ou par des offres hors du fournisseur d'accès à Internet tels que WhatsApp, etc.).

b) L'avocat envoie un courriel à un client ou à un autre avocat.

c) L'avocat envoie des documents à un client ou à un autre avocat par l'intermédiaire d'une autre technologie que le courrier électronique.

d) L'avocat utilise des solutions en ligne du gouvernement ou des tribunaux pour l'envoi, la réception et l'archivage des communications (par exemple des requêtes judiciaires).

e) L'avocat archive ou récupère des dossiers, des pièces et des archives par voie électronique (sans les envoyer à des tiers).

f) L'avocat effectue des recherches juridiques.

20 Investigatory Powers Tribunal Liberty et al. vs. GCHQ 160 (ii) at http://www.ipt-uk.com/docs/IPT_13_168-173_H.pdf.

g) L'avocat dispose de matériel informatique présentant des risques de sécurité (téléphones, ordinateurs, ainsi que fax, scanners, imprimantes et photocopieurs disposant d'une mémoire ou de disques durs).

La première partie de l'analyse qui suit se penchera sur les caractéristiques qui sont communes à la plupart des scénarios ci-dessus, et la deuxième partie examinera les caractéristiques particulières des scénarios pertinents.

7. Garantir la confidentialité des communications : risques de surveillance spécifiques et mesures de prévention possibles

Premier risque : l'enregistrement des conversations et de métadonnées connexes

En fonction des technologies et des services utilisés, un certain degré de protection des conversations est généralement présent. Mais les communications passent souvent à travers différents segments de réseau dont les capacités et les dangers divergent fortement. Les boucles locales des appels téléphoniques traditionnels ne sont protégées que sur le plan physique (par exemple dans des armoires verrouillées), une protection qui peut facilement être contournée physiquement au sein des bâtiments.

a) L'enregistrement par le biais des fournisseurs de services

L'exigence d'un certain niveau de protection des conversations est énoncée dans le cadre des services qui sont soumis à des normes bien définies, par exemple au sein de l'infrastructure fournie par les technologies sans fil (comme UMTS et LTE). En même temps, les fournisseurs de ce type de services peuvent également être tenus d'accorder aux agences gouvernementales l'accès à des conversations par ailleurs protégées. Dans l'UE, les réseaux et les services autorisés sous le régime des « communications électroniques » de 2002 sont tenus d'autoriser l'interception légale (voir l'annexe A.11 de la directive 2002/20/ CE). En cas de manquement, la plupart des autorités nationales peuvent mettre fin à la fourniture du service ou du réseau. Cette mesure comprend les services de téléphonie fixe, de téléphonie mobile et l'accès à internet.

Toutefois, les services reposant sur un accès Internet déjà existant ne sont pas considérés comme des services de « communication électronique ». En effet, bien que le courrier électronique et la messagerie instantanée (chat) soient considérés comme des communications électroniques, des services tels que Skype, Viber ou autres services similaires utilisant des appels passant par l'application en question ne sont pas toujours considérés comme des services de communication électronique dans tous les États membres de l'UE (dans le présent document, ceux-ci sont considérés comme des « offres hors du fournisseur d'accès à Internet »).

Certains organismes chargés de l'application de la loi ou certaines agences de sécurité nationale ont réussi à convaincre certains fournisseurs de services hors fournisseurs d'accès à Internet à coopérer et à fournir pratiquement le même niveau d'accès qu'un service traditionnel de communication électronique. Toutefois, si le fournisseur de services hors fournisseur d'accès à Internet n'est pas techniquement présent dans un pays (s'il n'y dispose que de personnel de vente par exemple), il s'avère très difficile pour la plupart des agences de faire pression sur ces fournisseurs lorsqu'ils ne veulent pas coopérer. Par conséquent, les agences doivent se tourner vers des moyens internationaux de coordination et de coopération. En outre, aucun fournisseur de services hors fournisseur d'accès à Internet n'est obligé par la loi à disposer de capacités particulières pour permettre de réaliser l'interception à ses propres frais. Par conséquent,

si un fournisseur de services hors fournisseur d'accès à Internet choisit de coopérer, il serait économiquement plus intéressant pour lui de transférer les coûts de l'interception légale vers l'agence gouvernementale qui en fait la demande.

L'utilisation des services hors fournisseur d'accès à Internet qui ne sont présents physiquement que dans d'autres juridictions que celle de l'utilisateur peut en quelque sorte servir de mesure de protection contre la surveillance ciblée de la part d'organismes locaux, à condition que la coopération ne soit pas très forte entre ces juridictions. En même temps, il convient de garder à l'esprit que les fournisseurs de services hors fournisseurs d'accès à Internet les plus demandés sont physiquement situés dans des pays où (du moins d'après les preuves anecdotiques) le risque de surveillance de masse est le plus élevé. Par ailleurs, il faut savoir que tous les services hors fournisseur d'accès à Internet peuvent être enregistrés au niveau du fournisseur d'accès à Internet et qu'un opérateur de réseau mobile ou un fournisseur d'accès Internet fixe local peut de toute évidence enregistrer facilement des courriels à des fins d'interception légale.

Mesures préventives possibles

La mise en œuvre de mesures de protection contre la surveillance peut avoir des effets sur la facilité d'utilisation ou l'efficacité du service. Cette question mériterait d'être gardée à l'esprit, même si la priorité doit être donnée à l'obligation déontologique de chercher à garantir la confidentialité.

a) Protection par chiffrement des communications

Une solution possible consiste à procéder au chiffrement des conversations. Les méthodes de chiffrement étant nombreuses et variées, il est donc nécessaire d'approfondir ses connaissances pour comprendre ce qui est chiffré et ce qui ne l'est pas. Par exemple, bien que les appels mobiles, même de deuxième génération, soient chiffrés entre l'appareil de l'utilisateur et la station de base, le chiffrement reste faible, même contre un pirate individuel disposant d'un minimum de ressource. Même si un fournisseur vend son service comme étant chiffré, le fournisseur peut encore avoir accès aux clés de chiffrement, ne sécurisant une conversation donnée que tant que le fournisseur n'est pas obligé de coopérer avec les organismes d'application de la loi.

Néanmoins, certains appareils (par exemple les téléphones, PBX) fournissent un chiffrement de bout en bout entre les appareils compatibles, en chiffrant à la fois les appels téléphoniques traditionnels, et les appels hors fournisseur[21]. Cependant, il est important de noter que :

- l'ensemble de ces solutions n'empêchent pas les agences gouvernementales de trouver des moyens juridiques détournés pour accéder aux communications ;
- le chiffrement de bout en bout fonctionne si les deux utilisateurs ont des appareils compatibles et
- dans certains pays, même au sein de l'UE, l'importation ou la vente de ces produits peut être limitée pour des raisons de sécurité nationale[22].

Le chiffrement de bout en bout est possible en exécutant un logiciel spécial sur un smartphone ou une tablette[23]. WhatsApp et Viber ont également fait en sorte (ou même fourni cette option par défaut) que le logiciel utilisé pour accéder à leurs services puisse comprendre le chiffrement des conversations de bout en bout.

La plupart des solutions reposant uniquement sur des logiciels n'utilisent les numéros de portable traditionnels pour l'acheminement des appels ou des messages.

21 http://www.cryptophone.de/en/products/mobile/, le Blackphone https://www.silentcircle.com/products-and-solutions/devices/, http://www.bull.com/hoox, etc.

22 Par exemple, l'importation et la vente du Cryptophone en Hongrie sont interdites pour des motifs de sécurité.

23 Voir par exemple d'autres produits de Cellcrypt, Chatsecure, Signal Private Messenger, Silent Circle, wickr, etc.

Enfin, un chiffrement de bout en bout reposant uniquement sur du logiciel n'empêche pas les conversations de faire l'objet de piratage à partir du système d'exploitation ou d'un environnement logiciel en cours d'exécution sur l'appareil (par exemple, Android) (voir ci-dessous de manière plus détaillée à la rubrique « Accès aux appareils »).

En ce qui concerne le risque de moyens juridiques détournés sur les appareils ou le risque de promesses non fiables de la part des fournisseurs de services de communication électronique, il est très difficile pour les avocats d'y faire quoi que ce soit à l'échelle individuelle. Il est également impossible de prendre des mesures contre les moyens détournés sur un équipement réseau ou le fait qu'une autorité de certification peu fiable délivre, par exemple, des certificats SSL à un pirate.

b) Utilisation de téléphones non enregistrés ou de téléphones dont les données de l'abonné ou de l'utilisateur ne sont plus à jour

Comme cela a été largement signalé, les auteurs des attentats du Bataclan à Paris, plutôt que d'utiliser le chiffrement, ont simplement utilisé des téléphones jetables pour communiquer. Comme dans la plupart des États membres il est possible d'acheter une carte SIM sans fournir l'identité de l'utilisateur et il existe des téléphones à carte prépayée dont les utilisateurs ne sont pas contraints de déclarer le passage de l'abonnement vers un nouvel utilisateur (certains États membres ne disposant en effet d'aucun mécanisme réglementaire ou autre rendant cela possible), cette possibilité restera également ouverte afin de réduire les risques de surveillance.

b) Enregistrement des métadonnées des conversations

La différence la plus importante entre l'enregistrement de métadonnées et l'enregistrement d'une conversation en soi est généralement qu'aucun mandat ni aucune autre approbation externe n'est nécessaire pour qu'une agence gouvernementale obtienne l'accès toutes les métadonnées d'une communication (la « trace écrite » de la surveillance sera également moindre dans ce cas.)

Mesures préventives possibles

La plupart des métadonnées des conversations créées au cours de la fourniture d'un service peuvent être enregistrées par le fournisseur de services, à moins que le fournisseur ne choisisse expressément d'exclure l'enregistrement de ces données. Il est techniquement impossible pour un avocat (ou n'importe qui d'autre) d'empêcher l'enregistrement de ces métadonnées. Même en utilisant le chiffrement de bout en bout, si un avocat appelle un numéro de téléphone traditionnel, toutes les métadonnées importantes seront enregistrées au niveau du fournisseur de services : le numéro appelé, la durée de l'appel, etc.

Si cela constitue un problème, l'avocat devrait alors éviter d'avoir recours à cette méthode de communication et utiliser les services hors fournisseurs d'accès à la place.

Deuxième risque : l'accès aux appareils

Comme indiqué plus haut, même bout à bout, le chiffrement peut s'avérer inutile si la personne malveillante obtient l'accès à l'appareil de l'utilisateur.

En raison de la grande variété de logiciels pouvant être installés sur un grand nombre d'appareils, le plus grand risque est la vulnérabilité des logiciels, c'est-à-dire des erreurs non résolues dans certaines parties de l'environnement informatique d'un appareil donné. Un pirate pourrait exploiter ces vulnérabilités pour obtenir, sans y être autorisé, l'accès à des fonctionnalités de l'appareil et en prendre le contrôle, notamment en enregistrant les appels, ou en accédant à des journaux contenant des métadonnées importantes.

Les logiciels malveillants (virus, vers, etc.) présents sur un appareil peuvent également offrir le même type d'accès non autorisé à des pirates. Un logiciel malveillant peut être installé

accidentellement, y compris par le biais de sites Internet malveillants ouverts à partir de l'appareil.

Enfin, il est primordial de savoir que l'accès physique à un appareil offre de telles possibilités à des personnes malveillantes.

Mesures préventives possibles

Ces risques peuvent être réduits en suivant les routines de sécurité informatique de base prévues dans les conseils ci-dessus et en limitant l'accès physique à l'appareil ou en changeant d'appareil à intervalles réguliers. L'activation d'un mot de passe sur chaque appareil et le chiffrement des données contenues sur les appareils susceptibles d'être égarés est une précaution minimale importante que tous les avocats devraient prendre, qu'ils cherchent à se protéger des activités de surveillance ou non. Les mots de passe doivent de toute évidence être activés et changés régulièrement.

Troisième risque : les données supprimées

Les avocats et les cabinets d'avocats doivent régulièrement recycler du matériel informatique contenant des mémoires non volatiles ou des supports de données, comme les téléphones, les ordinateurs portables et les ordinateurs de bureau. Les scanners et les photocopieurs modernes renferment très souvent une mémoire ou un disque dur.

Si ce matériel n'est pas recyclé de la manière adéquate, toute personne ayant accès à ces supports de données est en mesure de restaurer des parties importantes des données stockées sur les appareils, même lorsque ces données ont déjà été supprimées.

Mesures préventives possibles

Il est important que les avocats veillent à ce que toutes les données présentes sur ces supports de données soient écrasées avant de se débarrasser de l'appareil, ou que les supports de données soient physiquement détruits ou encore que tous les supports de données soient conservés pour des motifs de sécurité (et non revendus). La plupart des destructeurs de documents de qualité sont capables de déchiqueter des CD et des DVD, mais la destruction de disques durs et disques durs SSD peut s'avérer relativement onéreuse.

Si des supports de données sont détruits à l'extérieur du cabinet de l'avocat par un tiers, il est recommandé d'obtenir la certification de la part du tiers que la destruction a eu effectivement lieu.

Quatrième risque : l'accès à des données (stockées) sans rapport avec les conversations

Les données sans rapport avec les conversations, telles que les données stockées ou sein du cabinet ou auprès d'un tiers, subissent un risque similaire de surveillance que dans le cas des données relatives aux conversations. Habituellement, l'accès par une agence gouvernementale à ces données au sein du cabinet est soumis à des garanties supplémentaires prévues dans la réglementation (par exemple un mandat). Toutefois, l'accès aux données conservées par un tiers au nom d'un avocat est rarement soumis aux mêmes garanties réglementaires qui sont applicables dans le cas du cabinet d'avocats lui-même, et le fournisseur de service ne saura pas forcément établir la distinction entre les informations relevant du secret professionnel et le reste.

Mesures préventives possibles

Même si le transfert entre le cabinet d'avocats vers le lieu de stockage est protégé par un procédé tel que le chiffrement SSL, il est recommandé d'utiliser des services de stockage permettant un « chiffrement côté client »[24].

24 Ex. SpiderOak, TresorIT.

Dans ce cas, l'avocat doit absolument faire en sorte de protéger le mot de passe ou tout autre mécanisme de sécurité (clé d'authentification) servant à accéder aux données chiffrées. Les utilisateurs se sont habitués à obtenir l'accès même en cas de perte du mot de passe grâce à une méthode alternative et fiable d'authentification. Mais ce n'est pas le cas avec le chiffrement : si l'avocat venait à perdre le mot de passe, le fournisseur de service n'aura aucun moyen technique de donner l'accès aux données chiffrées, ce qui en provoquera à coup sûr la perte.

8. Recommandations à l'égard de certaines technologies de communication

a) Sécurité des réseaux d'accès

Bien que l'utilisation de réseaux Wi-Fi soit très répandue, il est nécessaire que l'avocat prennent des précautions. Le Wi-Fi n'est en général pas vraiment adapté à un usage professionnel comprenant le fait de manipuler des données confidentielles, à moins de disposer d'une couche de sécurité supplémentaire par chiffrement de bout en bout similaire à celle employée lors de l'utilisation de réseaux privés virtuels (RPV, ou VPN en anglais).

En l'absence d'une telle couche de chiffrement supplémentaire, l'avocat ne devrait pas utiliser de connexion Wi-Fi sans contrôle d'accès fondamental pour envoyer des informations liées aux clients. Si ces précautions ne sont pas prises, toute personne (personnes anonymes et machines comprises) présente dans le voisinage peut avoir accès à l'ensemble du trafic de données et l'enregistrer.

En outre, la simple protection d'un réseau par mot de passe ne le rend pas plus sûr que les réseaux Wi-Fi « ouverts ». Si une personne malveillante non identifiée se connecte au même réseau parce que le mot de passe est partagé (par exemple, toute personne pouvant consulter le mot de passe, ou ayant déjà utilisé le réseau), cette personne pourra accéder au trafic de données de l'avocat comme sur un réseau Wi-Fi sans mot de passe. Les avocats devraient dès lors s'abstenir d'utiliser le Wi-Fi sans réseau privé virtuel s'il ne peut pas être affirmé que le mot de passe du réseau Wi-Fi a été modifié dans les deux jours précédents[25]. L'authentification fiable et sécurisée des « invités » sur le réseau reste assez compliquée et, sûrement pour cette raison, très rare.

L'utilisation de l'Internet mobile est plus sûre que l'utilisation du Wi-Fi, mais il n'est pas toujours possible d'utiliser l'Internet mobile à l'étranger.

La solution la plus sûre est d'établir une connexion à un réseau privé virtuel entre le cabinet et l'appareil mobile ou toute autre ressource informatique mobile à risque.

Ce problème doit être gardé à l'esprit lorsque les avocats mettent à la disposition de leurs clients une connexion Wi-Fi gratuite au sein de leur cabinet. Le cabinet d'avocats pourrait exposer sans le savoir les données de ses clients à des risques inutiles. La connexion Wi-Fi mise à disposition des clients ne doit pas être la même que celle qui est utilisée dans le cabinet. La différence entre les deux réseaux doit être expliquée à tous les membres et employés du cabinet qui ne devraient jamais utiliser le Wi-Fi client pour les activités du cabinet. Les avocats devraient par ailleurs offrir une connexion Wi-Fi gratuite à leurs clients uniquement s'ils peuvent assurer la protection et la fiabilité correcte du réseau[26].

25 Le pirate peut intercepter la communication entre le point d'accès au Wi-Fi et l'appareil utilisé au moment de la saisie des mots de passe partagés et utilisés par un certain nombre de personnes. Ce n'est toutefois pas aussi facile qu'avec un réseau Wi-Fi ouvert. (WPA PSK).

26 Au lieu d'une connexion Wi-Fi sans ou avec un seul mot de passe partagé, il est possible d'utiliser un générateur de points d'accès, par exemple http://www.zyxel.com/us/en/products_services/uag50.shtml.

Les praticiens exerçant seuls et les petits cabinets devraient garder à l'esprit que s'ils utilisent un réseau câblé (par exemple Ethernet) fourni par leur propriétaire (par exemple dans un environnement de bureau avec services), ils devraient vérifier auprès de leur propriétaire (ou de préférence auprès d'un expert en informatique) que les réseaux locaux de chaque locataire sont bien distincts les uns des autres. Si les autres locataires sont en mesure d'accéder aux ordinateurs du cabinet d'avocats, ces ordinateurs et les dossiers des clients qui s'y trouvent sont exposés à un risque considérable, même si un utilisateur lambda ne sait pas forcément comment y accéder.

b) Courriels

Les courriels des cabinets d'avocats peuvent être enregistrés de différentes manières, soit par le fournisseur du réseau d'accès local de l'expéditeur ou du destinataire, soit par le fournisseur d'accès à Internet du destinataire ou de l'expéditeur (s'ils sont différents du fournisseur de la boucle locale), soit par le fournisseur qui accorde l'accès aux courriels, soit par celui qui relaie les courriels à envoyer au destinataire.

Du point de vue de la surveillance gouvernementale et de l'obligation du fournisseur de service, les fournisseurs de messagerie électronique sont plus des fournisseurs de services hors fournisseur d'accès et ne sont a priori pas soumis aux exigences sophistiquées d'enregistrer et d'archiver les messages en fonction des besoins des organismes de surveillance, du moins pas avant d'avoir été approchés par ces agences afin de coopérer. Quoi qu'il en soit, accorder l'accès aux courriels aux organismes de surveillance devrait toujours faire l'objet d'une autorisation externe (un mandat judiciaire par exemple).

La connexion entre le fournisseur de messagerie électronique et le logiciel client local est de plus en plus souvent sécurisée par un chiffrement SSL, mais cela ne signifie pas nécessairement que le message restera chiffré lorsque le fournisseur le transmettra au fournisseur du destinataire ou à des prestataires intermédiaires. Ce chiffrement pourrait devenir plus courant à l'avenir, mais compte tenu du grand nombre de fournisseurs de services de messagerie électronique et de leurs configurations diverses, il est très difficile de garantir le chiffrement des courriels de bout en bout sans sacrifier la capacité de les acheminer.

Du point de vue des assurances juridiques pour les communications client-avocat, un service de messagerie en interne, géré par le cabinet d'avocats, devrait fournir davantage de protection juridique. Toutefois, dans la pratique de la majorité des cabinets d'avocats, la sécurité et la fiabilité opérationnelles et techniques souffriraient probablement davantage de cette approche « maison » qu'en disposant de la couverture offerte par une assurance juridique supplémentaire. La surveillance de masse des plus grands fournisseurs de services de messagerie électronique est techniquement possible.

Il est donc primordial que la possibilité d'utiliser le chiffrement des courriels de bout en bout figure déjà dans la plupart des clients de messagerie (« agents de messagerie utilisateur »). En outre, un grand nombre d'avocats européens ayant accès à des certificats X.509 pour la signature électronique (et des certificats similaires pour le chiffrement), la sécurité des courriels pourrait s'améliorer de manière significative au sein de l'UE s'il existait un répertoire facile à utiliser et fiable des certificats de chiffrement pour les avocats.

Si ce chiffrement n'est pas possible parce que l'on a voulu envoyer un courriel à un client sans certificat de chiffrement par exemple, il serait préférable de chiffrer les informations les plus importantes du client dans une pièce jointe et d'envoyer un mot de passe unique au client par un autre moyen de communication (par exemple par SMS ou par téléphone et non par courriel).

c) Procédures électroniques des tribunaux et des gouvernements

Les avocats doivent de plus en plus souvent utiliser des infrastructures de transmission électronique fournies par les autorités judiciaires afin d'envoyer et de recevoir des documents. L'utilisation de telles solutions présente un risque d'accès non autorisé par des tiers ou de gouvernements étrangers. Le chiffrement de la transmission et de l'archivage des documents est une mesure de protection importante mais il ne peut le plus souvent être assuré que par le fournisseur des autorités publiques, qui accorde l'accès à son système.

Dans certains États membres, les barreaux fournissent parfois l'infrastructure de transmission électronique, le rôle de l'État se limitant à l'offre d'un portail vers cette infrastructure. Malgré les avantages indéniables, tels que le fait de garder le contrôle du système au sein de la profession et d'offrir aux avocats des solutions complètes adaptées à leurs besoins et garantir qu'ils disposent d'informations complètes d'utilisation et concernant tout incident pouvant s'être produit, cette approche laisse reposer les coûts sur les barreaux qui fournissent l'infrastructure. C'est la raison pour laquelle cette solution n'est pas forcément souhaitable pour tous les barreaux.

CONCLUSION

4

La protection absolue des systèmes informatiques face à la surveillance, qu'elle soit légale ou non, et face à d'autres formes de piratage est impossible à atteindre. Les systèmes informatiques seront toujours vulnérables, et, comme ces conseils le démontrent, aucun système complet ne sera en mesure d'offrir une protection totale des données. Les données conservées par les avocats et les communications entre les avocats et leurs clients sont exposées tous les jours à un grand nombre de risques de sécurité.

Face à cela, il est important que les avocats montrent à leurs clients et au public les mesures qu'ils ont prises. Une part essentielle de cette approche consiste à considérer toute analyse des risques de manière structurée et cohérente.

Par conséquent, ces conseils définissent un cadre qui est proposé pour que les barreaux puissent établir des recommandations à leurs propres membres quant au type d'approche systématique et structurée possible pour faire réduire les risques. Les propositions formulées dans ces conseils pourraient servir aux barreaux afin d'établir des recommandations plus approfondies, voire des obligations pour leurs membres, de manière similaire aux régimes en place pour la conservation des documents papier et des communications en face à face.

Le suivi de ces conseils ne devrait toutefois pas être considéré comme le simple fait de « cocher des cases ». Les menaces envers la sécurité des systèmes informatiques évoluent sans arrêt, à l'instar des systèmes informatiques eux-mêmes. Les grandes organisations, qui disposent de ressources bien plus grandes que les plus grands cabinets d'avocats, connaissent des failles de sécurité en dépit de tous leurs efforts pour s'en protéger.

La question n'est donc pas de savoir si les failles de sécurité peuvent être évitées, mais plutôt de savoir comment les avocats peuvent démontrer qu'ils ont réfléchi à la question et trouvé des solutions et pris les mesures préventives nécessaires.