Google, Microsoft et confidentialité

Dans l'affaire *Smith v. Maryland* [1], la Cour suprême des États-Unis s'est penchée sur la question de savoir si une personne, Michael Lee Smith, avait vu sa vie privée violée quand l'opérateur de téléphone avait mis en place à la demande de la police un système qui enregistrait les numéros de téléphone appelés par Smith, cela sans mandat d'un juge. En première instance, le tribunal a donné tort à Smith et la cour d'appel du Maryland a fait de même.

La Cour suprême a confirmé la décision : « Selon une jurisprudence constante de la présente cour, une personne n'a pas d'attente légitime en ce qui concerne sa vie privée pour des informations qu'elle transmet volontairement à des tierces parties ». Voici le passage concerné du jugement (la phrase traduite est à la troisième ligne) :

> Second, even if petitioner did harbor some subjective expectation that the phone numbers he dialed would remain private, this expectation is not "one that society is prepared to recognize as `reasonable.'" Katz v. United States, 389 U.S., at 361 . This Court consistently has held that a person has no legitimate expectation of privacy in information he [442 U.S. 735, 744] voluntarily turns over to third parties. E. g., United States v. Miller, 425 U.S., at 442 -444; Couch v. United States, 409 U.S., at 335 -336; United States v. White, 401 U.S., at 752 (plurality opinion); Hoffa v. United States, 385 U.S. 293, 302 (1966); Lopez v. United States, 373 U.S. 427 (1963). In Miller, for example, the Court held that a bank depositor has no "legitimate `expectation of privacy'" in financial information "voluntarily conveyed to . . . banks and exposed to their employees in the ordinary course of business." 425 U.S., at 442 . The Court explained:
>
> "The depositor takes the risk, in revealing his affairs to another, that the information will be conveyed by that person to the Government. . . . This Court has held repeatedly that the Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities, even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed." Id., at 443.

La doctrine de la tierce partie

Ce principe s'appelle la doctrine de la tierce partie (*third party doctrine*). Il a d'importantes conséquences sur le respect de la confidentialité des télécommunications et il touche pratiquement tout le monde, même en Europe, puisque toute donnée stockée aux États-Unis relève de la législation des États-Unis (règle de la *lex situs*) et que beaucoup de gens ont des données hébergées par des serveurs aux États-Unis.

C'est souvent le cas si on possède un appareil Android ou iOS, si on a un compte Google Drive, One Drive, iCloud ou Facebook, ou si on emploie Gmail, Outlook.com ou Yahoo Mail. Mais les pays européens adoptent généralement une position ferme pour ce qui relève de leur

[1] Smith v. Maryland (1979), No. 78-5374, *http://caselaw.findlaw.com/us-supreme-court/442/735.html*, 20 juin 1979.

compétence. Si les serveurs concernés par une enquête criminelle se trouvent en Europe, le gouvernement américain ne peut pas obtenir d'informations sans l'autorisation du juge local. Le cas s'est produit en 2013 avec des e-mails stockés en Irlande sur des serveurs de Microsoft [2].

Ce qui est frappant, dans l'affaire *Smith v. Maryland*, c'est que les juges ne se sont pas limités à dire que l'État était en droit d'examiner les messages sans mandat du juge ; ils sont allés jusqu'à affirmer qu'il n'y avait pas de droit à la vie privée quand un message passe par un tiers. Cette formulation très large autorise toute entreprise, même privée, à examiner les données qui transitent par elle pour autant qu'elle le fasse « dans le cours normal des activités ». Or cette condition me semble trop vague pour offrir une protection solide.

On pourrait objecter que personne n'est obligé d'utiliser les services de firmes américaines et que ceux que cela gêne peuvent s'adresser à des entreprises européennes, mais cela ne suffit pas : si une personne *A* envoie un e-mail à une personne *B* à l'adresse *B@gmail.com*, le message de *A* est soumis à la norme de la tierce partie à l'instant même où il entre aux États-Unis pour être stocké sur les serveurs Gmail.

Gmail

En 2013, à la suite d'une action de classe menée contre Google devant la Cour de district de San Jose, l'entreprise a soutenu ceci : « Quoique les plaignants qui n'ont pas Gmail ne sont pas liés par les termes d'un contrat avec Google, ils ont toutefois implicitement consenti aux pratiques de Google par le fait que *tous* les utilisateurs de messagerie électronique doivent nécessairement s'attendre à ce que leurs messages fassent l'objet d'un traitement automatique ». Elle a ajouté que « [...] aujourd'hui, les gens qui utilisent une messagerie électronique basée sur le web ne peuvent pas être surpris si leurs communications sont traitées par le fournisseur de services de télécommunications du destinataire dans le cadre de la distribution » [3]. Dans son argumentation, elle s'est explicitement appuyée sur la doctrine de la tierce partie.

Selon Google, les messages électroniques où l'expéditeur ou le destinataire a une adresse Gmail ne sont donc pas confidentiels ; la doctrine de la tierce partie lui donne le droit de les lire, avec pour seule limitation que cela doit se passer dans le cadre normal des activités.

Comme on pouvait s'y attendre, cette prise de position a fait l'objet de commentaires choqués dans la presse [4]. Il semblerait que Google intercepte les messages au vol, avant même qu'il soient stockés, au moyen d'un logiciel appelé Content One [5], ce qui irait d'autant plus dans le sens de l'illégalité.

En ce qui concerne l'action de classe, Google a remporté la victoire le 18 mars 2014, la Cour de district de San Jose ayant dit qu'il ne lui était pas possible d'aboutir à une conclusion parce que

---

[2] M. Apuzzo, D. E. Sanger, M. S. Schmidt, « Apple and Other Tech Companies Tangle With U.S. Over Data Access », *The New York Times*, 7 septembre 2015.

[3] Google Inc. Gmail Litigation, *Google's Motion to Dismiss Complaint Memorandum of Points & Auhtorities*, Case No. 5:13-md-02430-LHK, *https://www.documentcloud.org/documents/800448-google-wiretap-complaint-motion-to-dismiss-and.html*, 5 septembre 2013.

[4] Exemple : Dominic Rushe, « Google: don't expect privacy when sending to Gmail », *The Guardian*, 15 août 2013.

[5] Joel Rosenblatt, « Is Google Too Big to Sue Over Gmail Privacy Concerns? », *Bloomberg*, 6 mars 2014.

les demandeurs étaient trop nombreux et qu'elle ne parvenait pas à savoir qui, parmi eux, avaient consenti aux pratiques de Google. Il n'y a donc pas eu de décision sur le fond.

Pour prendre un exemple concret, le directeur de la CIA David Petraeus a perdu son travail à cause du traçage des e-mails qu'il envoyait via Gmail à sa maîtresse [6]. En croisant les méta-données, notamment le lieu d'origine des e-mails de l'un et l'autre avec leur localisation physique, les enquêteurs ont pu découvrir non seulement leur identité (Petraeus utilisait un pseudonyme), mais aussi les endroits où ils se rencontraient. Cet exemple montre jusqu'où peut aller la collaboration entre Google et les autorités : il n'y avait rien de pénal dans les frasques extraconjugales de Petraeus.

L'espionnage économique constitue aussi un problème important : si un e-mail contient des informations confidentielles sur un projet d'entreprise ou un contrat, Google peut le repérer au moyen de mots-clés et on ne peut pas être sûr qu'il n'est pas transmis au gouvernement américain : selon Edward Snowden, les moyens de surveillance des télécommunication des États-Unis sont employés au profit de l'économie américaine [7], et des documents secrets de la NSA dévoilés par le même Snowden montrent que Google coopère étroitement avec l'agence dans ce domaine [8].

Chrome

Chrome ne pose probablement pas plus de problèmes de confidentialité que les autres navigateurs, et, comme eux, on peut l'améliorer en le paramétrant et en ajoutant des plug-ins.

Par exemple, le paramètre DNT (*do not track*) ajoute aux requêtes HTTP un en-tête qui demande aux sites visités de ne pas pister l'utilisateur.

Malheureusement, les sites restent libres d'ignorer le contenu de cet en-tête : ce n'est pas une obligation légale. De plus, le traçage ne peut pas être désactivé. Si on active DNT, une fenêtre s'affiche dans Chrome qui mentionne ce problème :

> L'activation de la demande "Interdire le suivi" implique l'inclusion de cette dernière avec votre trafic de navigation. Le résultat dépend de la réponse d'un site Web à cette demande et de la façon dont cette dernière est interprétée. Par exemple, des annonces qui ne sont pas basées sur d'autres sites que vous avez consultés peuvent s'afficher sur certains sites Web en réponse à cette demande. Vos données de navigation continuent d'être collectées et utilisées sur de nombreux sites Web, notamment pour améliorer le niveau de sécurité, ou pour fournir du contenu, des services, des annonces et des recommandations sur le site, ainsi que pour générer des statistiques destinées à la création de rapports.

En fait, ce qui pose problème, ce n'est pas tant le navigateur que le moteur de recherche.

---

[6] E. Perez, S. Gorman, D. Barrett, « FBI Scrutinized on Petraeus », *The Wall Street Journal*, 12 novembre 2012.

[7] David Meyer, « Snowden accuses U.S. of industrial espionage », *Gigaom*, 25 janvier 2014.

[8] Glenn Greenwald, « Microsoft handed the NSA access to encrypted messages », *The Gardian*, 12 juillet 2013.

Le moteur de recherche Google

Qu'on emploie Chrome, Firefox, Safari ou tout autre navigateur, on travaille avec un produit de Google dès l'instant où on utilise le moteur de recherche de la firme. Or c'est ce qu'on fait le plus souvent puisque Google occupe la première place sur ce marché, loin devant Baidu, Bing, Yahoo, AOL, Ask, Lycos, etc. Beaucoup de gens ne connaissent pas même l'existence de ces moteurs.

Ce qui est fâcheux, c'est le traçage et l'analyse des visites de sites effectués en particulier pour proposer une publicité ciblée à l'utilisateur. Les outils employés pour cela sont notamment Adsense, Doubleclick et Google Analytics. Quand on visite un site, on peut voir nos données transmises à une dizaine de sociétés, cela même si ce site est aussi sérieux que, par exemple, le New York Times [9].

Si on se rend souvent sur des sites qui vendent du matériel photographique ou des billets de ferry, les publicités ciblées seront inoffensives, mais ce n'est pas toujours le cas. Par exemple, on n'a pas envie que des annonces qui portent sur l'alcoolisme ou le sida s'affichent sur l'écran si on prête son ordinateur à une autre personne.

Une manière simple d'éviter ce problème consiste à utiliser un navigateur sécurisé comme Epic (*https://epicbrowser.com*) et un moteur de recherche qui ne trace pas l'utilisateur comme Duck-duckgo (*https://duckduckgo.com*).

Android

Android constitue l'un des principaux canaux utilisés par Google pour collecter des données privées. Il est possible dans une certaine mesure de bloquer ces transmissions, mais c'est long (cela se fait application par application et la case à cocher est parfois difficile à trouver) et il arrive même que ce soit impossible [10].

Compte tenu du fait qu'Android occupe la première place sur le marché des smartphones, les serveurs de Google stockent probablement la majeure partie des mots de passe Wi-Fi du monde.

À ce problème s'ajoute celui qu'on ne peut pas utiliser un smartphone Android sans créer un compte Gmail.

Pour ce qui est du respect de la vie privée, la téléphonie pose le même genre de problèmes que les moteurs de recherche. Si une personne appelle régulièrement sa famille, le traçage de ces appels n'importe probablement pas. En revanche, si c'est une hotline qui concerne la consommation de drogue, il en va autrement.

---

[9] Alexis C. Madrigal, « I'm Being Followed: How Google — and 104 Other Companies — Are Tracking Me on the Web », *The Atlantic*, 29 février 2012.

[10] Egzthunder1, « The Rootkit Of All Evil — CIQ », Xda-developers, *http://www.xda-developers.com/the-rootkit-of-all-evil-ciq/*, 14 novembre 2011.

Street View

En 2010, les autorités allemandes ont posé des questions à Google au sujet des données collectées par les voitures utilisées par l'entreprise pour son programme Street View. Il en est ressorti que Google recueillait et stockait des données provenant des réseaux sans fil que les voitures détectaient au fil de leurs déplacements, notamment des noms et des adresses de routeurs Wi-Fi ainsi que des contenus transmis par des utilisateurs au moment du passage du véhicule.

Google s'est défendu en disant que les données avaient été récoltées par inadvertance et ce programme a été arrêté en 2010, mais il a fonctionné pendant quatre ans dans plus de trente pays.

Pour répondre aux critiques, Google a instauré une méthode qui permet aux réseaux Wi-Fi de demander de ne pas être enregistrés, et qui consiste à terminer le nom du réseau par « *_nomap* », mais c'est à bien plaire : ignorer cette demande n'expose les contrevenants à aucune conséquence.

Au cours des quatre ans d'espionnage par Street View, des millions de données ont été amassées. Ont-elles été détruites ? Google a dit qu'il s'en était défait, mais c'est la mission de la NSA d'espionner tous les types de télécommunications, ce qui veut dire qu'elle a peut-être considéré que c'était un devoir pour elle de récupérer cette masse d'informations.

L'affaire Street View fait l'objet d'une procédure actuellement en cours devant un tribunal de Californie. Elle est donc pendante sur le plan judiciaire.

Ce qui est préoccupant, c'est que les données de Street View ne constituent qu'une petite partie du problème. De la messagerie Gmail au moteur de recherche Google en passant par le système d'exploitation Android, les applications Google Docs, le stockage Google Drive, le service Google Now, etc., le déversement sur les serveurs de Google de données confidentielles de particuliers et d'entreprises est massif.

Les autres entreprises

Google absorbe la plus grande partie des flux de données confidentielles, mais toutes les entreprises de l'Internet sont potentiellement concernées, surtout celles qui se trouvent aux États-Unis, vu la faiblesse de la protection de la vie privée là-bas.

Un juge fédéral américain est allé jusqu'à considérer que les personnes qui souhaitent éviter d'être tracées dans leurs déplacements doivent éteindre leur smartphone : « Ainsi, j'estime que, pour ce qui est des données prévisionnelles de géolocalisation, les utilisateurs de téléphones cellulaires qui s'abstiennent d'éteindre leurs téléphones ne montrent pas une attente en matière de respect de la vie privée et, en tout état de cause, une telle attente ne serait pas raisonnable » [11].

---

[11] United States District Court, Eastern District of New York, *Memorandum and Order*, Case No. 2:13-mj-00242-GRB, *http://ia601705.us.archive.org/23/items/gov.uscourts.nyed.340535/gov.uscourts.nyed.340535.7.0.pdf*, 1er mai 2013, p. 26.

Les documents secrets de la NSA dont il a été question plus haut ont montré que Microsoft a été la première entreprise à collaborer avec cette agence en lui donnant un accès direct aux données stockées dans les serveurs d'Outlook.com et de Skype, mais Facebook, Apple et Yahoo collaborent aussi avec elle [12].

Le cas d'Apple est toutefois à part. À la suite d'un mandat du juge, la firme devait transmettre des messages électroniques au FBI, mais elle a répondu qu'elle ne pouvait pas le faire parce que ces messages étaient chiffrés de bout en bout et qu'il ne lui était techniquement pas possible de les transformer en texte lisible [13].

Le cas de Windows

En été 2015, Microsoft a décidé d'intégrer à Windows des fonctions de traçage et, ce qui est nouveau, d'espionnage des contenus des fichiers. Cela a provoqué des inquiétudes, d'autant que ces outils ont également été ajoutés aux versions 7 et 8 du système d'exploitation par le canal des mises à jour [14].

Il est possible de désactiver la majorité de ces fonctions [15], mais cela ne veut pas forcément dire qu'on les arrête. Dans certains cas, elles continuent apparemment de fonctionner en silence en arrière-fond [16].

Aux États-Unis, ces pratiques sont sans doute compatibles avec la doctrine de la tierce partie, mais, en Europe, leur légalité est douteuse [17]. Ce qui ne va pas, ce n'est pas leur existence ; c'est que Microsoft ne fournisse pas à l'utilisateur une façon simple de les bloquer complètement.

Microsoft est aussi indirectement à l'origine d'autres risques de fuites de données. Si un utilisateur de Windows 10 n'a pas désactivé la fonction Wifi Sense, ceux de ses contacts qui ont un compte Outlook.com, Skype ou (si la case a été cochée) Facebook auront accès au réseau Wi-Fi de cet utilisateur s'il clique sur « Oui » quand le logiciel lui demande l'autorisation. Cet accès ne concerne que l'Internet, mais il nécessite que l'ordinateur de l'invité connaisse la clé du réseau, ce qui constitue une brèche de sécurité [18].

Également préoccupant est le fait que, si une personne donne sa clé Wi-Fi à quelqu'un qui a activé la fonction Wifi Sense, la propagation de la clé s'effectuera auprès de tous les contacts de l'invité s'il clique sur « Oui ».

---

[12] Glenn Greenwald, « Microsoft handed the NSA access to encrypted messages », *The Gardian*, 12 juillet 2013.

[13] M. Apuzzo, D. E. Sanger, M. S. Schmidt, « Apple and Other Tech Companies Tangle With U.S. Over Data Access », *The New York Times*, 7 septembre 2015.

[14] Gordon Kelly, « Windows 10 Worsts Feature Installed On Windows 7 And Windows 8 », *Forbes*, 30 août 2015.

[15] Doug Bolton, « Windows 10 spying: How to opt out of Microsoft's intrusive new terms of use », *The Independent*, 2 août 2015.

[16] Peter Bright, « Microsoft accused of adding spy features to Windows 7, 8 », *Arstechnica*, 1 septembre 2015.

[17] Voir les directives européennes 2002/58/CE, 2006/24/CE et 2009/136/CE, la loi informatique et libertés en France, la loi vie privée en Belgique, la loi fédérale sur la protection des données en Suisse.

[18] Simon Rockman, « UH OH: Windows 10 will share your Wi-Fi key with your friends' friends », *The Register*, 30 juillet 2015.

Il est possible de se protéger contre Wifi Sense en terminant le nom du réseau Wi-Fi par les caractères « *_optout* », mais cette solution entre en collision avec « *_nomap* » : il est évident que, dans *nom-du-réseau_optout_nomap*, les caractères *_optout* ne terminent pas le nom, ce qui veut dire qu'ils seront ignorés.

Le droit d'accès aux fichiers constitue une autre faille importante. Dans le contrat d'utilisation de Windows 10, il est spécifié ceci (section 3) :

> En acceptant le présent contrat ou en utilisant le logiciel, vous acceptez que Microsoft collecte, utilise et transmette ces informations selon les conditions définies dans la Déclaration relative aux Données personnelles de Microsoft disponible sur le site (aka.ms/privacy) et selon les conditions éventuellement définies dans l'interface utilisateur des fonctionnalités logicielles.

Cela donne le droit à Microsoft d'accéder à toutes les données de l'utilisateur, y compris le *contenu* de ses fichiers. Est-ce que cela concerne seulement les données stockées sur les serveurs de Microsoft ou aussi les fichiers qui se trouvent sur l'ordinateur de l'utilisateur, c'est une question controversée, mais, même s'il ne s'agit que des serveurs, cela pose de gros problèmes de confidentialité.

En Russie, ces problèmes ont conduit le vice-président du parlement Nikolai Levichev à demander au gouvernement d'interdire l'emploi de Windows dans le secteur public [19].

En Suisse, le préposé suppléant à la protection des données Jean-Philippe Walter a parlé de « violations crasses » à propos de Google et Microsoft et il a déclaré qu'il irait si nécessaire jusqu'au Tribunal fédéral pour éclaircir le cas de Windows [20]. De son côté, le préposé du canton du Valais a publié un communiqué où il a dénoncé « une communication de données irréversible », incitant les décideurs du secteur public valaisan à ne pas installer Windows 10 [21].

Il y a encore une autre facette à ces problèmes. Elle concerne le droit des contrats et l'obligation de confidentialité qui accompagne beaucoup de contrats. Non seulement Microsoft se donne le droit d'accéder au contenu des fichiers des utilisateurs (en tout cas ceux qui se trouvent sur ses serveurs), mais il dit ouvertement qu'il va divulguer ce contenu s'il le juge nécessaire (Déclaration de confidentialité de Microsoft, section « Raisons pour lesquelles nous partageons vos données personnelles ») :

> Enfin, nous accéderons à, divulguerons et préserverons les données personnelles, notamment votre contenu (comme le contenu de vos emails, d'autres communications privées ou des fichiers de dossiers privés), lorsque nous pensons de bonne foi qu'il est nécessaire de le faire :

Cette disposition est en contradiction avec la clause de confidentialié qui accompagne certains contrats, clause qui interdit aux parties de communiquer des informations confidentielles à des tiers. Or Microsoft est par définition un tiers — et la situation est d'autant plus alarmante que la firme se donne en plus le droit de transmettre le contenu des fichiers privés des utilisateurs à *d'autres* tiers.

---

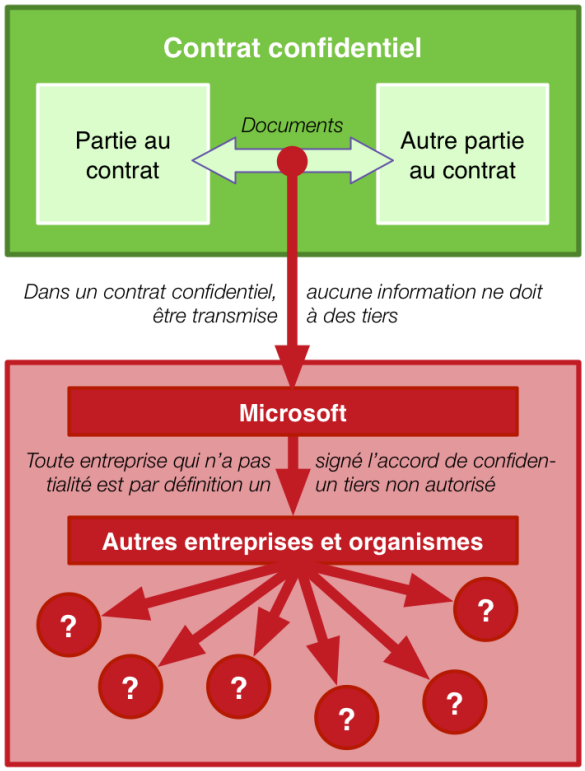
[19] « Senior Russian lawmaker seeks ban on Windows 10 in state agencies », *RT*, 21 août 2015.

[20] Mehdi Atmani, « "Chaque jour, on rogne davantage la sphère privée" », *Le Temps*, 24 août 2015.

[21] « Recommandation contre Windows 10 en Valais », *Bluewin.ch*, *http://www.bluewin.ch/fr/infos/suisse/2015/8/28/les-ecoles-valaisannes-priees-de-ne-pas-installer-.html*, 28 août 2015.

Quels sont les contrats concernés ? Beaucoup de contrats conclus entre entreprises sont confidentiels, mais il y a aussi les médecins, les infirmiers, les pharmaciens, les policiers, les gendarmes, les ecclésiastiques, les notaires, les avocats, les comptables, etc., qui sont liés par le secret professionnel (la liste varie d'un pays à l'autre). Par exemple, comment un juriste peut-il garantir le secret à propos d'un brevet s'il travaille avec Windows 10, ce qui veut dire qu'il a accepté le contrat d'utilisation du logiciel, contrat qui autorise Microsoft à lire le contenu de ses fichiers ? Je ne vois pas comment cela pourrait être compatible avec l'obligation au secret professionnel.

Selon la déclaration de confidentialité de Microsoft, l'entreprise divulgue le contenu des fichiers d'un utilisateur « pour répondre à des requêtes légales valides, notamment celles émanant des organismes d'application de la loi et d'autres organismes gouvernementaux » (section « Raisons pour lesquelles nous partageons vos données personnelles »).



Qui sont ces « autres organismes gouvernementaux » qui ne relèvent *pas* de l'application de la loi ? Cette désignation est d'une étendue préoccupante.

Il faut aussi penser aux effets sur la situation de la personne qui se trouve à la source de la fuite. Exemple imaginaire (mais pas invraisemblable [22]) : une entreprise, par exemple Airbus, est en discussion avec un client et elle s'aperçoit qu'un concurrent américain, par exemple Boeing, sait tout des termes des tractations, ce qui permet à ce concurrent de remporter le contrat. L'enquête menée sur cette fuite montre qu'elle a eu lieu sur l'ordinateur d'un ingénieur d'Airbus et que les informations ont été communiquées à l'un de ces « autres organismes gouvernementaux » non spécifiés, qui les a transmises à Boeing. Quelles peuvent être les conséquences pour cet ingénieur ? Cela concerne la clause de confidentialité incluse dans le contrat de travail.

Le secret professionnel fait l'objet de l'article 226-13 du code pénal français, de l'article 458 du code de droit pénal belge et de l'article 321 du code pénal suisse, mais il ne s'applique qu'aux membres des métiers assujettis au secret comme les médecins ou les avocats. De plus, il ne concerne que les révélations faites volontairement.

Par contre, cet ingénieur pourrait-il être accusé de négligence, l'argument étant qu'on ne peut pas en même temps autoriser un tiers à accéder à des données (en acceptant le contrat d'utilisation de Windows 10) et garantir le secret de ces mêmes données ?

[22] Voir par exemple : « Espionnage de la NSA : Airbus porte plainte », *La Tribune*, 30 avril 2015.

À cette question, la réponse est oui si la direction a interdit à ses employés d'utiliser Windows. Cela pourrait entraîner des sanctions disciplinaires, voire des poursuites civiles, cela même en l'absence de faute lourde. C'est un motif de licenciement.

La réponse est certainement non si l'entreprise n'a pas interdit à ses employés d'utiliser Windows. Dans ce cas, c'est potentiellement elle qui a fait preuve de négligence.

Toutefois, le problème est qu'un accord de confidentialité entraîne une obligation de résultat, ce qui veut dire que la négligence n'est pas nécessaire pour que la responsabilité de cet ingénieur soit en cause. Autrement dit, le seul fait qu'une divulgation ait eu lieu suffit à établir sa responsabilité, cela même s'il n'a pas fait preuve d'imprudence.

Pour conclure

Est-il acceptable que Google, Microsoft et d'autres entreprises de l'Internet détiennent et communiquent à d'autres organismes des milliers d'informations qui nous appartiennent et relèvent de notre vie privée ou de notre obligation de confidentialité en tant qu'employés d'une entreprise ? Cette question concerne beaucoup de monde. Personne n'est à l'abri de stocker un jour par inadvertance un document confidentiel sur Microsoft Office 365 ou de transmettre sur Gmail des informations confidentielles au sujet d'un contrat, d'un brevet ou d'un projet d'entreprise.

Pour éviter les conséquences de la doctrine de la tierce partie, il y a des solutions.

Pour ce qui est du stockage, la Commission européenne a lancé une initiative appelée *European Cloud Partnership* dans le but de promouvoir le développement des services de cloud en Europe (*https://ec.europa.eu/digital-agenda/en/european-cloud-partnership*).

Pour la messagerie électronique, on peut taper dans un moteur de recherche les mots clés *secure email europe*.

Par exemple, la poste française (*http://www.laposte.fr/particulier*) offre une messagerie électronique gratuite, sous la protection de la loi informatique et libertés.

En Belgique, le fournisseur de services de messageries Mail.be garantit explicitement la confidentialité des informations qu'on lui confie (*https://www.mail.be*) :

> Vos données et leurs sauvegardes sont hébergées exclusivement sur des serveurs localisés en Europe. Ils sont dès lors soumis aux législations européenne et belge, notamment en ce qui concerne la protection de vos données. Vous disposez donc d'un droit de consultation, de rectification et également de suppression de vos données (droit à l'oubli). Concrètement, si vous demandez la suppression de votre compte, vos données seront totalement supprimées de notre application.
>
> Nous contrôlons totalement nos serveurs: nous sommes l'éditeur du logiciel et aucun sous-traitant n'a accès à notre infrastructure. Les membres de notre personnel qui ont accès aux serveurs ont signé un engagement de confidentialité.
>
> Nous exigeons un ordre signé par un juge ayant autorité sur nous avant de transmettre la moindre de vos données.

En Allemagne, Posteo met à disposition pour 12 euros par an une messagerie électronique accompagnée d'outils de chiffrement (*https://posteo.de/en*). Grâce à une particularité de la loi allemande sur les télécommunications, les utilisateurs n'ont même pas besoin de donner leurs noms et adresses.

Toutefois, il faut souligner que la situation est complexe et que les législations et les pratiques européennes ont aussi leurs limites. Selon un axiome bien connu, si vous avez quelque chose à

transmettre sur l'Internet, ne le faites pas sauf si vous pouvez accepter le risque que cela devienne public un jour.

Mais ce qui préoccupe le plus les spécialistes en sécurité, c'est qu''il n'est pas exclu que le nouveau contrat de Windows 10 aille en direction d'une logique encore plus invasive : si vous avez quelque chose à stocker sur votre ordinateur, ne le faites pas sauf si vous pouvez accepter le risque que cela devienne public un jour.