L'affaire Bluetouff, c'est l'histoire incroyable d'un internaute qui sera condamné au pénal (3000 € d'amende et inscription au casier judiciaire) pour avoir simplement suivi un lien Google puis téléchargé des documents accessibles publiquement. Depuis son début, initié par la plainte de l'Anses le 6 septembre 2012, jusqu'à son terme conclu par l'arrêt de la cour de cassation le 20 mai 2015, l'affaire Bluetouff a fait l'objet de très nombreux articles dans la presse ou sur le Net. Mais une affaire de cybercriminalité n'est jamais très simple à comprendre car elle demande des connaissances juridiques et des compétences en sécurité informatique ou plus précisément en matière d'investigation numérique légale (forensic). En tant qu'expert judiciaire près la cour d'appel de Montpellier, je vous propose de réexaminer en détail le déroulement de cette histoire. L'objectif n'est pas de débattre une nouvelle fois sur le bien-fondé de la décision de la cour d'appel ou de la compétence informatique des magistrats mais plutôt de comprendre pourquoi Bluetouff a été condamné et ce qu'il aurait dû faire pour ne pas l'être malgré la plainte de l'Anses et les investigations de la DCRI.

- Rappel des faits
- Le jugement en 1ère instance par le TGI de créteil
- Le jugement de la Cour d'appel de Paris
- Le jugement de la Cour de cassation
- En garde à vue le silence est un droit !
- Sans aveux, une condamnation était-elle possible ?
- Conclusion

Rappel des faits

En août 2012, un internaute blogueur (reflets.info, bluetouff.com) dénommé Bluetouff, de son vrai nom Olivier Laurelli, navigue sur Internet via un serveur VPN hébergé au Panama. Il fait des requêtes sur Google puis suit un des liens proposés par le moteur de recherche pour atterrir sur un serveur de l'Anses (*l'Agence nationale de la sécurité sanitaire et l'alimentation, de l'environnement et du travail).* Il parcourt l'arborescence des répertoires du serveur et remonte jusqu'à la page d'accueil sur laquelle il constate la présence d'un contrôle d'accès (authentification par identifiant et mot de passe). *Il continue ensuite sa navigation dans les sous-répertoires et télécharge de nombreux documents (environ 8000 documents représentant un volume de* 7,7 Go). Il utilise quelques extraits issus de cette extraction (environ 200 Mo) pour publier (sous le pseudo Bluetouff) un article sur les nano-matériaux sur le site reflets.info. Il est important de noter à cet instant, qu'il n'y a strictement aucune protection d'accès à ces documents (aucun mot de passe ni chiffrement des données) et que tout internaute peut y accéder via Google avec un simple navigateur. Il faut préciser également, qu'il n'existe aucune mention de confidentialité sur les-dit documents.

Le 3 septembre 2012, un chef d'unité de l'Anses découvre un article relatif aux nano-matériaux mis en ligne sur le site d'information reflets.info, article accompagné d'un document Powerpoint de l'agence destiné uniquement à un usage interne provenant vraisemblablement de l'Extranet de l'Anses.

Le 6 septembre 2012, le RSSI de l'Anses dépose plainte auprès des services de police de Maisons-Alfort (94) pour intrusion dans le système informatique de l'Anses et vol de données. L'Anses étant considérée par l'état comme un opérateur d'importance vitale (OIV), c'est la DCRI (devenue DGSI depuis le 12 mai 2014) qui sera chargée de l'enquête.

L'analyse des journaux de connexions du serveur extranet et du firewall de l'Anses confirme les éléments fournis par l'agence lors du dépôt de plainte à savoir l'extraction les 27 et 28 août 2012 d'un volume d'environ 8 Go de donnée vers une adresse IP localisée au Panama. Cette adresse est rapidement identifiée comme provenant d'un serveur d'une société Panaméenne fondée et dirigée par Olivier Laurelli. D'autre part l'enquête de la DCRI permet d'identifier très rapidement Olivier Laurelli comme étant l'internaute agissant sous le pseudonyme Bluetouff.

Le 21 novembre 2012, Olivier Laurelli est placé en garde à vue durant 30 heures au siège de la DCRI. Lors de son audition, il reconnait avoir récupéré via son VPN panaméen l'ensemble des données accessibles sur le serveur extranet de l'Anses. Il reconnait également avoir parcouru l'arborescence des répertoires et être remonté jusqu'à la page d'accueil sur laquelle il constate l'apparition d'une « mire de login » destinée à restreindre les accès par une authentification utilisateur. C'est

le point clé de cette affaire : la reconnaissance formelle par Olivier Laurelli que les données n'étaient pas publiques mais bel et bien protégées par un mécanisme d'authentification mais dont une défaillance technique (dont l'entière responsabilité appartient à l'Anses) rendait accessibles publiquement. C'est d'ailleurs pour cette même raison que les données ont pu être indexées par Google.

Le jugement en 1ère instance par le TGI de créteil

L'affaire sera jugée en correctionnelle par le Tribunal de Grande instance de Créteil. Dans son jugement en date du 23 avril 2013, le tribunal indique :

Concernant l'accès frauduleux et le maintien frauduleux dans un système de traitement automatisé de données :

Néanmoins, il n'est pas contesté par l'Anses qu'une défaillance technique existait dans le système et que Monsieur Olivier L. a pu récupérer l'ensemble des documents sans aucun procédé de type « hacking ».
Compte tenu de l'ensemble de ces éléments, même s'il n'est pas nécessaire pour que l'infraction existe que l'accès soit limité par un dispositif de protection, le maître du système, l'Anses, en raison de la défaillance technique, n'a pas manifesté clairement l'intention de restreindre l'accès aux données récupérées par Monsieur Olivier L. aux seules personnes autorisées. Monsieur Olivier L. a pu donc légitimement penser que certaines données sur le site nécessitaient un code d'accès et un mot de passe mais que les données informatiques qu'il a récupérées étaient en libre accès et qu'il pouvait parfaitement se maintenir dans le système. En conséquence, il convient de relaxer Monsieur Olivier L. des chefs d'accès frauduleux et maintien frauduleux dans un système de traitement automatisé des données.

Concernant le vol des documents téléchargés et enregistrés sur plusieurs supports :

Selon l'article 311-1 du code pénal, le vol est la soustraction frauduleuse de la chose d'autrui.

En l'espèce, en l'absence de toute soustraction matérielle de documents appartenant à l'Anses, le simple fait d'avoir téléchargé et enregistré sur plusieurs supports des fichiers informatiques de l'Anses qui n'en a jamais été dépossédée, puisque ces données, élément immatériel, demeuraient disponibles et accessibles à tous sur le serveur, ne peut constituer l'élément matériel du vol, la soustraction frauduleuse de la chose d'autrui, délit supposant, pour être constitué, l'appréhension d'une chose. En tout état de cause, Monsieur Olivier L. a pu légitimement penser que ces documents étaient librement téléchargeables puisque non protégés par un quelconque

système. Il n'y a pas eu de sa part une volonté d'appropriation frauduleuse de ces fichiers informatiques et donc il n'y a pas d'élément intentionnel de l'infraction.

Le 23 avril 2013, Olivier Laurelli est donc relaxé par le tribunal de créteil. « Tout est bien qui finit bien » devait-il sans doute se dire mais c'était sans compter sur le parquet de Paris qui décide de faire appel de cette décision.

Le jugement de la Cour d'appel de Paris

Devant la cour d'appel, Bluetouff devait répondre de trois chefs d'accusation :

- avoir accédé frauduleusement au serveur de l'Anses,
- s'y être maintenu frauduleusement,
- avoir soustrait frauduleusement les documents stockés sur cet extranet, en les dupliquant sur plusieurs supports.

Par un arrêt en date du 5 février 2014, la Cour d'appel de Paris confirme le jugement du TGI de Créteil concernant l'absence de caractère frauduleux de l'accès mais elle déclare *Bluetouff* coupable de maintien frauduleux et de vol de données.

S'agissant de l'accès frauduleux et dans la mesure où l'Anses avait elle-même reconnue une erreur de sa part dans la gestion des accès à leur serveur, les magistrats de la cour d'appel relaxe Bluetouff de ce chef d'accusation.

Concernant le maintien frauduleux, la Cour d'appel souligne qu'après avoir accédé au site de l'Anses, *Bluetouff*, en parcourant l'arborescence, avait pu constater que l'accès était soumis à des restrictions d'accès. Il avait donc :
« parfaitement conscience de son maintien irrégulier dans le système de traitement automatisé de données visité où il a réalisé des opérations de téléchargement de données à l'évidence protégées ».

Concernant le vol de données, la Cour de cassation avait déjà par le passé qualifié de vol une copie de données (Cass.crim., n°07-84.002, 4 mars 2008, X/ Société Graphibus). Dans ses conclusions sur l'affaire *Bluetouff*, l'avocat général Frédéric Desportes s'est ainsi exprimé : *« Il serait paradoxal que la soustraction frauduleuse d'un document papier sans intérêt soit passible de trois ans d'emprisonnement mais non celle de milliers de fichiers stratégiques alors même que ces fichiers ne sont jamais que des documents numériques ou numérisés pouvant être imprimés et donc matérialisés ».*

A ce sujet, il est important de noter un changement récent de la législation. Ainsi

en application de la Loi n°2014-1353 du 13 novembre 2014 renforçant les dispositions relatives à la lutte contre le terrorisme, le code pénal (art. 323-3) sanctionne désormais l'extraction de données, mettant ainsi un terme au débat relatif au « vol de données ». Le Code pénal réprime donc aujourd'hui non seulement l'introduction, la modification et la suppression frauduleuses de données mais également l'extraction, la détention, la reproduction et la transmission frauduleuses de ces données. Bien entendu, la promulgation de ce texte étant postérieure aux faits, il ne pouvait être appliqué dans le cas de l'affaire Bluetouff.

Ainsi, par un arrêt en date du 5 février 2014, la cour d'appel de Paris a condamné Olivier Laurelli pour maintien frauduleux dans un système de traitement automatisé de données et vol de données à une peine délictuelle de 3000 € assortie d'une inscription au bulletin no2 de son casier judiciaire.

Le jugement de la Cour de cassation

Suite à la décision de la cour d'appel, Olivier Laurelli a donc décidé, par l'intermédiaire de son avocat Me Olivier Iteanu, de formuler un pourvoi en cassation. Dans son pourvoi, Me Iteanu avance de nombreux arguments :

- On ne commet pas le délit de maintien frauduleux dans un système de traitement automatisé de données (STAD) quand on utilise un moteur de recherche et un navigateur pour pénétrer un système non protégé.
- On ne peut déduire de la découverte d'un contrôle d'accès, la conscience d'un maintien irrégulier dans un système informatique.
- Il revient au responsable du système de manifester clairement et expressément sa volonté d'interdire ou restreindre l'accès.
- Les informations contenues dans une partie d'un site non protégé sont du coup réputées non confidentielles et publiées avec l'accord des intéressés.
- Il y a une contradiction évidente à reprocher à un internaute d'avoir « *réalisé des opérations de téléchargement de données à l'évidence protégées* » et « *fait des copies de fichiers informatiques inaccessibles au public* » en admettant dans le même temps qu'il a pu accéder librement à ces données.
- Le vol exige juridiquement la soustraction frauduleuse de la chose d'autrui (tel un individu a une chose, il se la fait voler, il ne l'a plus). Il n'y a donc pas de vol lorsqu'il n'y a pas de dépossession, sauf à violer le Code pénal qui est d'interprétation strict.

Malgré cet argumentaire tout à fait pertinent de Me Iteanu, les magistrats de la Cour de cassation ont estimé que la Cour d'appel avait jugé en droit et avait correctement interprété la Loi. En conséquence et en l'absence d'éléments nouveaux

dans le dossier, la Cour de cassation rejette le pourvoi par un arrêt du **20 mai 2015** et confirme la condamnation prononcée par la Cour d'appel de Paris à l'encontre d'Olivier Laurelli.

Le dernier recours pour Olivier Laurelli est maintenant de saisir la CEDH (Cour Européenne des Droits de l'Homme) comme l'a indiqué son avocat Me Olivier Iteanu dans Le Parisien. Ce recours reste cependant très hypothétique dans la mesure où seulement 5 % des plaintes reçues par la CEDH sont effectivement examinées par la Cour. La CEDH n'accepte en effet d'examiner que les affaires démontrant une certaine probabilité de violation des droits garantis par la Convention européenne des droits de l'homme dont l'entrée en vigueur remonte à 1953.

En garde à vue le silence est un droit !

Il y a bien sûr un coté subjectif dans le jugement d'une affaire pénale et une procédure n'est rarement jouée d'avance. Il n'est pas rare en effet d'être condamné en première instance puis relaxé en appel même si dans le cas de l'affaire Bluetouff c'est le contraire qui s'est produit. Dans ces conditions, et même si l'on pense n'avoir rien fait de répréhensible, il vaut mieux lors des auditions en garde à vue, ne rien dire ! C'est ce l'on appelle le droit au silence et qui reste un droit de défense peu connu des citoyens et qui aurait peut-être évité à Bluetouff d'être condamné par la justice. Le droit au silence c'est la possibilité de garder le silence et d'être informé de ce droit dans le cadre d'une garde à vue. Il peut être utile de rappeler ce qu'est précisément une garde à vue telle qu'est est définie à l'article 62-3 du Code de procédure pénale : « *La garde à vue est une mesure de contrainte prise au cours de l'enquête par laquelle une personne soupçonnée d'avoir commis ou tenté de commettre un crime ou un délit puni d'emprisonnement est maintenue à la disposition des enquêteurs.* »

La Convention européenne des droits de l'homme considère depuis longtemps que « *le droit de se taire lors d'un interrogatoire de police et le droit de ne pas contribuer à sa propre incrimination* » sont des normes internationales, au cœur d'un procès équitable (aff. Murray/ Royaume-Uni, 1996). Mais en France, la culture de l'aveu est bien ancrée dans notre système judiciaire. Or, depuis la Loi n° 2011-392 du 14 avril 2011, les policiers sont désormais dans l'obligation d'informer un suspect qu'il n'est pas tenu de répondre à leurs questions. Le Conseil Constitutionnel, dans sa décision du 30 juillet 2010, avait déjà jugé que l'absence de notification du droit de se taire était contraire à la Constitution. Mais il a fallu attendre la condamnation de la France par la CEDH (Cour Européenne des Droits de l'Homme) dans l'arrêt *Brusco c. France du 14 octobre 2010, n°1466/07*, pour que s'engage une véritable réforme du régime de la garde à vue pour le rendre plus

respectueux des droits de la défense. La France s'est donc pliée aux règles européennes et la Loi n° 2011-392 du 14 avril 2011 relative à la garde à vue a modifié le Code de procédure pénale. Le nouvel article 63-1 du Code de procédure pénale mentionne bien que la personne gardée à vue a le droit *« de faire des déclarations, de répondre aux questions qui lui sont posées **ou de se taire** »*.

Au terme de sa garde à vue, la personne concernée est soit remise en liberté, soit déférée, c'est-à-dire présentée à un magistrat qui décidera des suites à donner aux poursuites. Dans le cas où elle n'est pas remise en liberté, la personne gardée à vue peut être retenue par les services de police, avant d'être présentée, suivant sa situation, au procureur de la République, au juge d'instruction ou au juge des libertés et de la détention. Cette rétention supplémentaire, dont la durée maximale est de 20 heures, n'est qu'une simple attente et il est impossible de l'utiliser pour mener un nouvel interrogatoire. Précisons également et pour finir que l'article 116 du code de procédure pénale prévoit que le juge d'instruction, lors de la première comparution devant lui d'une personne qu'il envisage de mettre en examen, doit lui signifier « *qu'elle a le choix soit de se taire, soit de faire des déclarations, soit d'être interrogée* ».

Sans aveux, une condamnation était-elle possible ?

Dans l'affaire Bluetouff, il est évident que ce sont les déclarations d'Olivier Laurelli concernant la fameuse mire de login repérée tout en haut de l'arborescence qui ont entrainé sa condamnation. Sans ces aveux, quels sont les éléments qui auraient permis d'établir que Bluetouff avaient connaissance du caractère privé de ces documents ? Dans cette affaire, il y a pour les enquêteurs de la DCRI quatre sources d'information exploitables :

1. Les journaux d'évènements (logs) du serveur VPN situé au Panama
2. Les logs des fournisseurs d'accès Internet utilisés par Bluetouff (à Orléans et dans le Val de marne)
3. Les logs dans l'infrastructure d'hébergement du serveur de l'Anses (Firewall, reverse proxy et serveur Web Extranet)
4. L'historique de navigation et plus généralement toute information disponible sur le ou les postes clients utilisés par Bluetouff (historique, cache navigateur, fichiers résiduels,…)

Analysons, point par point, ces différentes sources d'information.

Source no1 : le serveur VPN

L'objectif du déploiement du service VPN de Bluetouff étant d'assurer l'anonymat, il est fort probable qu'il n'y ait aucune trace exploitable dans le serveur Panaméen en question. Pour exploiter cette source d'information dans le cadre d'une perquisition, c'est l'article 57-1 du code procédure pénale qu'il convient d'appliquer.

« *Les officiers de police judiciaire ou, sous leur responsabilité, les agents de police judiciaire peuvent, au cours d'une perquisition effectuée dans les conditions prévues par le présent code, accéder par un système informatique implanté sur les lieux où se déroule la perquisition à des données intéressant l'enquête en cours et stockées dans ledit système ou dans un autre système informatique, dès lors que ces données sont accessibles à partir du système initial ou disponibles pour le système initial.*
S'il est préalablement avéré que ces données, accessibles à partir du système initial ou disponibles pour le système initial, sont stockées dans un autre système informatique situé en dehors du territoire national, elles sont recueillies par l'officier de police judiciaire, sous réserve des conditions d'accès prévues par les engagements internationaux en vigueur. »

La seule convention internationale existante en la matière est la convention sur la cybercriminalité de Budapest du 23 novembre 2001 (Traité international No 185). Dans le cadre de la perquisition effectuée par la DCRI en novembre 2012, cette convention n'aurait pas pu s'appliquer puisque le Panama ne l'a ratifié que le 3 mars 2014 et qu'elle n'est entrée en vigueur avec ce pays qu'à compter du 1er juillet 2014.

Précisons que si l'enquête avait lieu aujourd'hui, les choses seraient bien différentes, puisqu'au-delà de l'application de la convention de Budapest (articles 25 et 32-b en particulier), la LOI n° 2014-1353 du 13 novembre 2014 relative à la lutte contre le terrorisme (Chapitre V – article 13) a modifié l'article 57-1 du code procédure pénale en renforçant les moyens d'investigation des services de police judiciaire .

Source no2 : Les logs des FAI

Et bien pas grand-chose aussi à exploiter ici par la DCRI car tout est chiffré entre le poste client et le serveur VPN. Les seules choses que peut voir un FAI sont les métadonnées des connexions (adresses IP sources et destinations, heure de connexion, volume des données échangées,…) mais en aucun cas le contenu des requêtes et donc la preuve que l'URL de la page de connexion a bien été sollicitée. Bien sûr, si l'internaute Bluetouff était déjà sous surveillance et soupçonné de terrorisme, il y aurait la possibilité (technique et juridique) pour la DCRI de déposer un mouchard d'interception sur son poste client (via un 0-day exploit dans flash player par exemple, technique très à la mode en cette année 2015…) afin d'analyser intégralement tous les flux échangés avec son ordinateur quelque soient les solutions ou techniques cryptographiques mises en œuvre (https, TOR, I2P, Freenet,

SSH, VPN IPsec ou SSL).

Source no3 : L'infrastructure d'hébergement du serveur de l'Anses

Beaucoup plus intéressant pour la DCRI car, que l'accès au serveur Web se fasse via http ou https (c'est le serveur Web de l'Anses qui décide et non pas le serveur VPN de bluetouff), les requêtes effectuées apparaissent en clair dans les journaux de logs du serveur Extranet et également dans les logs d'un éventuel reverse proxy déployé en amont. Mais quel est la valeur juridique d'un fichier de logs ? La preuve d'un fait juridique pouvant se faire par tout moyen, il est par conséquent possible d'utiliser un fichier de logs à titre de preuve dans le cadre d'une procédure pénale. Toutefois, sa recevabilité à titre probatoire est subordonnée à sa fiabilité. Ce critère dépend d'une part, des conditions dans lesquelles le fichier a été collecté puis conservé et d'autre part, de la qualité de la partie qui a réalisé ces opérations. Ainsi, la force probante d'un fichier de logs est maximale si son authenticité et son intégrité peuvent être tracées et garanties de la collecte de l'information recherchée jusqu'à sa fourniture aux enquêteurs judiciaires. Dans le cas de l'affaire Bluetouff, il est fortement vraisemblable que ce fichier de logs soit géré directement par l'Anses et que les administrateurs de l'agence aient la possibilité de l'altérer en toute discrétion. On peut par exemple imaginer d'y ajouter une ligne d'accès à la fenêtre d'authentification du serveur en provenance de l'adresse IP du serveur VPN pour incriminer Olivier Laurelli. Dans ces conditions, on peut difficilement imaginer que ce fichier logs soit recevable à titre de preuve. Il est important de noter que, même si un fichier de logs est recevable à titre probatoire, il reste néanmoins soumis à l'appréciation du juge qui peut décider de l'écarter des discussions.

Source no4 : Les informations sur le poste client de Bluetouff

Dernière source d'information intéressante à exploiter par les enquêteurs de la DCRI : le ou les ordinateurs dont s'est servi Olivier Laurelli pour accéder au serveur de l'Anses via son VPN. C'est d'ailleurs pour pouvoir exploiter cette source qu'il est placé en garde à vue pendant 30 heures, que son domicile à Orléans (Loiret) est perquisitionné et que son matériel informatique est saisi. Rappelons que la garde à vue (article 62-2 du code de procédure pénale) doit constituer l'unique moyen de parvenir à certains objectifs comme empêcher que la personne ne modifie des preuves ou des indices matériels. N'ayant pas eu accès aux pièces du dossier, il est impossible de se prononcer sur les éléments récupérés dans le matériel saisi par les enquêteurs. Une chose est sûre cependant, c'est que la solution VPN utilisée dans l'affaire Bluetouff (solution totalement différente d'un VPN entreprise utilisé pour le télé-travail par exemple) permet d'assurer l'anonymat. En d'autre terme, cela rend impossible à un Webmaster d'identifier l'origine réelle d'une requête effectuée sur son serveur Web. Mais si un enquêteur dispose physiquement du poste de l'utilisateur du service VPN, il peut alors retrouver un ensemble de traces informatiques comme par exemple la requête à la page d'authentification du serveur de l'Anses avec la date et l'heure exacte de l'opération. Il va sans dire que si ces éléments coïncident parfaitement avec le

journal de logs fourni par l'Anses et indiquent qu'une requête sur la page d'authentification a bien été effectuée, les aveux de Bluetouff ne semblent plus nécessaires pour démontrer à la Cour qu'il avait bien conscience de son maintien irrégulier dans le système. On peut également imaginer que Bluetouff n'est pas le premier venu et qu'il a pris quelques précautions au niveau de son poste client. Quoique la première des précautions qu'il me viendrait à l'esprit si je souhaitais naviguer de façon réellement anonyme via un VPN serait sans doute de ne pas m'appuyer sur le serveur VPN de ma propre entreprise fût-elle immatriculée au Panama ou ailleurs dans le monde. Cela dit, si Bluetouff a eu par exemple la bonne idée d'utiliser Tails ou de naviguer dans une machine virtuelle chiffrée puis de supprimer cette VM par une opération de « crypto shredding », il y a fort à parier qu'aucune information pertinente n'a pu être récupérée par la DCRI.

Conclusion

Pour gagner ce procès, il aurait fallu qu'Olivier Laurelli garde le silence lors de ses auditions mais qu'il soit également en mesure de faire disparaître toute trace de navigation sur les ordinateurs utilisés les 27 et 28 août 2012. Dès lors, comme il n'y pas eu d'accès frauduleux (ce qui est acté par tous y compris par l'Anses) et qu'il n'y a plus de moyen de prouver le maintien frauduleux, la Cour d'appel de Paris n'aurait pu que confirmer le jugement du TGI de créteil :
« En tout état de cause, Monsieur Olivier L. a pu légitimement penser que ces documents étaient librement téléchargeables puisque non protégés par un quelconque système. Il n'y a pas eu de sa part une volonté d'appropriation frauduleuse de ces fichiers informatiques et donc il n'y a pas d'élément intentionnel de l'infraction. »

Autres ressources :

- Bluetouff condamné pour maintien frauduleux et vol de fichiers
- 3000€ d'amende et un casier judiciaire pour une requête Google
- Affaire Bluetouff : la Cour de cassation consacre le vol de fichiers informatiques
- Notre pourvoi en cassation est rejeté

A l'issue d'une consultation publique (23 juillet – 15 octobre 2012), la commission Européenne a élaboré puis adopté le 7 février 2013 la proposition d'une nouvelle directive pour la sécurité des réseaux et de l'information. La directive NIS (Network and Information Security) a pour objectif de renforcer la réactivité des 28 États membres et de stimuler la coopération entre les autorités de lutte contre la cybercriminalité, tout en leur donnant des moyens techniques et légaux appropriés.

Approuvée par le Parlement Européen le 13 mars 2014 (521 voix pour, 21 voix contre), la directive NIS prévoit des mesures de sécurité à respecter pour les opérateurs de services essentiels mais également pour les acteurs du marché du numérique. Ces derniers étant définis à l'annexe II du document original de la directive : Plateformes de commerce électronique, Passerelles de paiement par internet, Réseaux sociaux, Moteurs de recherche, Services informatiques en nuage, Magasins d'applications en ligne.

Le 7 décembre 2015, les députés européens ont conclu un accord avec le Conseil pour arrêter le texte final de cette directive. Concrètement, l'accord a permis de finaliser la liste des sociétés concernées par la directive à savoir les infrastructures critiques (appelées OIV en France) mais également les acteurs du marché du numérique pour lesquels les réseaux sociaux sont finalement exclus. Les obligations des acteurs du marché sont beaucoup moins contraignantes que pour les OIV et concernent principalement le signalement obligatoire des incidents de sécurité aux autorités nationales compétentes.

En France, cette obligation n'est pas nouvelle. En effet suite à l'adoption du Paquet Télécom et l'ordonnance n° 2011-1012 du 24 août 2011 relative aux communications électroniques, les opérateurs télécoms ont déjà l'obligation d'informer les autorités nationales compétentes (ici la CNIL) des fuites de DCP (données à caractère personnel). Concernant les opérateurs d'importance vitale (OIV), des obligations de sécurité sont imposées depuis la loi de programmation militaire (LOI n° 2013-1168 du 18 décembre 2013). Ainsi, selon l'article L1332-6-1 du code de la défense : *« Le Premier ministre fixe les règles de sécurité nécessaires à la protection des systèmes d'information des opérateurs mentionnés aux articles L. 1332-1 et L. 1332-2 et des opérateurs publics ou privés qui participent à ces systèmes pour lesquels l'atteinte à la sécurité ou au fonctionnement risquerait de diminuer d'une façon importante le potentiel de guerre ou économique, la sécurité ou la capacité de survie de la Nation.»* Concernant les incidents de sécurité, l'article L1332-6-2 précise que les OIV doivent informer sans délai les services du Premier ministre (l'ANSSI) des incidents affectant le fonctionnement ou la sécurité des systèmes d'information. Des arrêtés sont en cours de finalisation pour définir précisément les modalités selon les secteurs concernés. Pour des raisons de sécurité, certains de ces arrêtés ne seront pas publiées.

Pour pouvoir entrer en vigueur, la Directive NIS devra encore être approuvée formellement par la commission du marché intérieur du Parlement le 14 janvier 2016 puis par le comité des représentants permanents du Conseil. Il s'agira ensuite pour chacun des 28 États membres de transposer la directive dans leur droit national respectif.

Chad Woolf, Directeur risques et conformité chez AWS, a déclaré le 30/11/2015 sur le blog officiel d'Amazon : "*I am happy to announce that AWS has achieved ISO 27017 certification*".

Cette annonce est pour le moins surprenante car contrairement à l'ISO 27001, la norme ISO 27017 ne décrit pas un processus de gestion mais fournit un guide de bonnes pratiques. Elle a été développée par l'ISO pour compléter le guide initial définie par l'ISO 27002 et propose un ensemble de mesures de sécurité destinées à améliorer la sécurité des services dans le cloud.

En pratique, AWS a réactualisé son SMSI (pierre angulaire de l'ISO 27001) et mis à jour sa DdA (Déclaration d'Applicabilité) en adoptant les bonnes pratiques de l'ISO 27017. AWS a ensuite demandé à Ernst & Young de procéder à un nouvel audit pour attester de la prise en compte de l'ISO 27017 dans sa démarche ISO 27001.

On peut ainsi lire dans le certificat 27017 d'AWS : *" … certified under certification number [2013-009], is also compliant with the requirements as stated in the standard : ISO/IEC 27017:2015 "*
(*pour information, le numéro de certification [2013-009] correspond au certificate ISO 27001 d'AWS)*

En d'autres termes, Ernst & Young atteste que le SMSI d'AWS prend en compte les bonnes pratiques issues de l'ISO 27017 ce qui n'apporte en soi aucune information précise sur le niveau de sécurité effectif du fournisseur. En effet, en l'absence de publication de la DdA, on ne sait strictement rien sur la façon dont les mesures de sécurité proposées par l'ISO 27017 sont réellement implémentées au sein du SMSI d'AWS. Il s'agit donc encore une fois d'une démarche purement marketing, destinée à rassurer le client perdu dans la jungle des normes ISO/IEC 270xx. Dans le même état d'esprit, AWS aurait pu également demander à Ernst & Young un certificat ISO 27002 puisque naturellement son SMSI s'appuie sur des mesures issues de l'ISO 27002. Et pourquoi ne pas demander dans la foulée un certificat ISO 27005 puisque l'analyse de risque effectuée par AWS s'appuie sur ce référentiel ?