Regards sur la loi Godfrain du 5 janvier 1988 relative à la fraude informatique

par Marc Watin-Augouard
Directeur du Centre de recherche de l'EOGN
Fondateur du Forum International de la cybersécurité (FIC)
Président du Centre expert de lutte contre la cybercriminalité Français (CECyF)

Le 21 octobre 2016, la cyberattaque par déni de service distribué « 10-21 » a visé l'important serveur internet américain Dyn qui fait le lien entre l'adresse Internet Protocol (IP) et le nom de domaine internet en redirigeant les flux internet vers les hébergeurs. Ce jour marque incontestablement une rupture en raison de l'utilisation massive d'objets connectés contre l'infrastructure de l'espace numérique. Pendant plusieurs heures, le botnet[1] *Mirai*, dont l'auteur se vante de disposer de 380 000 objets connectés piratés, a fortement perturbé le fonctionnement d'un certain nombre de services en ligne. Par la suite, le fabricant de caméras de surveillance, Hangzhou XiongMai Technology, a été obligé de rappeler des modèles vendus aux États-Unis qui présentent une faible sécurité et offrent des mots de passe par défaut. Le code source de *Mirai* ayant été mis en *open source*, on peut s'attendre à de nombreuses répliques. L'attaque massive par *Mirai,* dont a été victime le Liberia[2], le 2 novembre 2016, est sans doute annonciatrice d'autres séismes[3].

1. Mise en action de plusieurs milliers d'ordinateurs « zombies », dont l'attaquant a pris le contrôle pour adresser à la cible autant de requêtes simultanées qui saturent le système. Sur le botnet, on se référera à la thèse fondatrice d'Eric Freyssinet : « Lutte contre les botnets : analyse et stratégie », Thèse de doctorat en informatique de l'Université Pierre et Marie Curie, novembre 2015.
2. L'attaque a été d'autant plus pénalisante que le Liberia ne possède qu'un accès par câble sous-marin à internet.
3. La cyberattaque massive qui a frappé, en mai 2017, 150 pays avec le rançongiciel wannacry, a eu des conséquences particulièrement importants avec plus de 300 000 victimes répertoriés.

La société Dyn a notamment pour clients Amazon, Twitter, Paypal, eBay, Airbnb, CNN, Spotify, Reddit, GitHub, le New York Times, Netflix, Financial Times, The Guardian… au total, une trentaine de sites qui n'ont pas pris la précaution de doubler leurs serveurs DNS. Cette cyberattaque, ajoutée à celle qui a frappé Yahoo, accompagnée de la compromission massive de données personnelles de 500 millions de ses utilisateurs, semble donner raison au cryptologue Bruce Schneier qui, le 13 septembre 2016, a annoncé que « quelqu'un apprend comment détruire internet[4] ». Selon Ben Johnson, cofondateur de Carbon Black et ex-hacker de la NSA, « internet continue de reposer sur des protocoles et une infrastructure conçus avant que la cybersécurité ne soit un problème ».

La généralisation de l'internet des objets a, bien évidemment, des conséquences en termes de sécurité. Les objets connectés sont généralement moins protégés et sont donc vulnérables[5]. L'existence de *Shodan* est tout aussi inquiétante. Ce moteur de recherche repère les objets connectés à internet et favorise donc leur détournement. « Google fouille les sites web, je fouille les objets », dit John Matherly, son fondateur[6]. Dans un rapport[7], le sénateur américain Edward-J Markey alerte sur les voitures intelligentes. 250 millions devraient circuler en 2020, avec des risques de cyberattaque, car « les constructeurs automobiles sont nouveaux dans le monde des logiciels et manquent d'expérience dans les programmes malveillants et de piratage ». En 2013, la DARPA avait déjà averti des dangers[8].

Avec l'attaque « 10-21 », le 21 octobre 2016 entre dans l'histoire de la cybercriminalité. Trente ans plus tôt, en 1986, le député Jacques Godfrain[9] est avant-gardiste, lorsqu'il dépose une proposition de loi protégeant pénalement les systèmes de traitement automatisés de données. Les premiers exploits des « hackers » malveillants (*black hat*)[10] avaient déjà souligné la fragilité des systèmes connectés. En 1981, Kevin Mitnick, âgé de 17 ans, réussit à pénétrer le système d'un central téléphonique américain. Deux ans plus tard, il s'introduit dans un ordinateur du Pentagone. En 1986, « *Brain* », le premier virus pour PC, est diffusé

4. Bruce Schneier, « Someone is learning how to take down internet », 13 septembre 2016, lawfareblog.com

5. Au Defcon de Las Vegas, en août 2016, des chercheurs ont montré comment prendre le contrôle d'un vibromasseur connecté. Standard innovation, le fabricant canadien, aurait collecté des données personnelles intimes…

6. www.shodanhq.com ; Le moteur recense la localisation de tous les appareils connectés à internet.

7. Edward-J Markey, Tracing&Hacking, février 2015, www.markey.senate.gov/imo/media.

8. Charlie Miller & Chris Valasek Adventures in Automotive Networks and Control Units, DARPA, 2013, http://illmatics.com/car_hacking.pdf.

9. Loi n° 88-19 du 5 janvier 1988 relative à la fraude informatique. Proposition déposée en août 1986.

10. Il existe des hackers « bienveillants », les « chapeaux blancs » (*white hat*), professionnels de la sécurité informatique qui, en conformité avec la loi et en accord avec leur propriétaire, testent les failles d'un système.

par des disquettes en provenance du Pakistan. En 1988, Robert Morris crée le premier ver[11] qui bloquera internet pendant une journée. Kevin Poulsen, actuel rédacteur en chef du magazine *Wired*, est, lui aussi, une figure de hackers célèbres. Les atteintes aux systèmes de traitement automatisé de données sont aussi le fait des « hacktivistes » qui ajoutent à la matérialité des faits un mobile politique. Au moment où ces attaques sont médiatisées[12], le député Jacques Godfrain est témoin d'un hacking organisé pendant lequel des données particulièrement sensibles sont extraites. Cet événement motive sa proposition de loi qui sera promulguée le 5 janvier 1988. Environ 5 000 machines sont alors reliées à Internet[13]. En 2016, on dénombre 10 milliards de machines connectées. Les estimations atteignent les 50 milliards en 2020, tandis que le cap des 1 000 milliards devrait être dépassé pendant la prochaine décennie, grâce aux objets et systèmes connectés.

Lors de la réforme du code pénal (1992-1994), les principales dispositions de la loi Godfrain ont été intégrées dans le livre III[14], à l'exception des anciens articles[15] relatifs à la falsification et documents informatisés et à leur usage, insérés à juste titre dans le nouveau livre IV[16].

Le texte est régulièrement abondé par des apports, comme ceux de la loi du 21 juin 2004 pour la confiance dans l'économie numérique, de la loi n° 2012-410 du 27 mars 2012 relative à la protection de l'identité, de la loi de programmation militaire du 18 décembre 2013, de la loi du 13 novembre 2014 renforçant les dispositions relatives à la lutte contre le terrorisme, de la loi du 24 juillet 2015, relative au renseignement et de la loi du 3 juin 2016 renforçant la lutte contre le crime organisé, le terrorisme et leur financement, et améliorant l'efficacité et les garanties de la procédure pénale. Malgré les ajouts postérieurs, il est d'usage d'évoquer la « loi Godfrain », sans doute en hommage à son auteur clairvoyant, mais aussi par ce qu'elle constitue un « bloc » de référence.

La loi n'a pas pris de ride, car elle n'a pas été associée à des technologies particulières, ni à une définition figée de la notion de « système de traitement automatisé de données[17] » qui auraient pu la rendre obsolète dès sa première évolution. Ainsi le Sénat avait envisagé une définition des systèmes de traitement automatisé de

11. Logiciel malveillant qui, contrairement au virus, ne se multiplie pas.
12. Le 28 novembre 1984, le Canard Enchaîné explique comment des journalistes ont eu accès à des bases de données relatives aux essais nucléaires de Mururoa à l'aide d'un Minitel.
13. C'est en 1989 qu'Internet s'ouvre au grand public et à l'exploitation commerciale.
14. Chapitre III du titre II du livre III du code pénal consacré aux systèmes de traitement automatisé de données.
15. Art. 462-5, 462-6 et 462-7 anc. CP
16. La nature informatisée du document n'a pas d'influence sur la nature de l'infraction. C'est la falsification qui est réprimée (art. 441-1 et s. CP).
17. Par exemple, un disque dur (cour d'appel de Douai, 7 oct. 1992), un radiotéléphone (cour d'appel de Paris, 18 novembre 1992), l'annuaire électronique de France Télécom (Trib. Cor. Brest, 14 mars 1995), le réseau Carte bancaire (Trib. Cor. Paris, 25 février 2000) un système de messagerie électronique (Trib. Cor. Le Mans, 7 novembre 2003). Lorsque le Sénat envisageait une définition, les smartphones, les clés USB, etc. n'existaient pas.

données, lors de l'écriture du nouveau code pénal : « Tout ensemble composé d'une ou plusieurs unités de traitement, de mémoire, de logiciel, de données, d'organes d'entrées-sorties et de liaisons, qui concourent à un résultat déterminé, cet ensemble étant protégé par des dispositifs de sécurité ». Mais cette précision n'a pas été retenue. Jacques Godfrain, lors du 5e Forum international de la cybersécurité (Lille 2013), a rappelé quelle fut alors la recherche d'équilibre entre un texte suffisamment précis et un texte « ouvert » aux mutations technologiques. La loi Godfrain est hélas plus que jamais d'actualité, tant les systèmes de traitement automatisés de données apparaissent aujourd'hui vulnérables aux attaques, qu'il s'agisse des systèmes numériques de contrôle-commande (SNCC), des systèmes de supervision et de contrôle (SCADA[18]), des automates programmables industriels (API) et, bien sûr, des objets connectés.

La loi Godfrain est donc vivante, évolutive. L'affaire « Bluetouff » est une des illustrations jurisprudentielles des attaques qui visent les systèmes, les traitements et les données (**I**). Les infractions peuvent être aggravées ou, au contraire, donner lieu à des formes d'irresponsabilité pénale ou à un « filtrage » par l'ANSSI des « fautes avouées » (**II**).

I. La loi Godfrain au regard de la jurisprudence

La loi Godfrain protège les « systèmes », les « traitements » et les « données ». L'accès ou le maintien frauduleux (**A**) dans un système de traitement automatisé de données (SATAD) est souvent le préalable à toute action pouvant nuire à son fonctionnement (**B**) ou aux données qu'il contient (**C**) conduisant à une analyse *in concreto* de chaque cyberattaque (**D**). Les infractions prévues et réprimées par la loi sont éclairées par la jurisprudence et, tout particulièrement, par l'arrêt de la Cour de cassation du 20 mai 2015, communément appelé arrêt « Bluetouff », pseudonyme utilisé sur la toile par Olivier Laurelli, journaliste, hacker, très connu au sein du milieu de internautes.

A. L'accès ou le maintien frauduleux dans un STAD

L'article 323-1 du code pénal sanctionne le fait d'accéder ou de se maintenir, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données.

Le même article aggrave la peine lorsque la pénétration ou le maintien frauduleux ont entraîné soit la suppression ou la modification de données contenues dans le système, soit une altération du fonctionnement de ce système. Cette atteinte aux données ou au fonctionnement est dans ce cas involontaire et résulte, par exemple, d'une manœuvre accidentelle. En effet, les articles 323-2 et 323-3

18. *Supervisory Control And Data Acquisition*.

répriment les mêmes faits commis avec le dol spécial de l'intention de nuire. C'est l'enquête qui peut faire le partage.

1. Les éléments constitutifs de l'infraction éclairés par la jurisprudence

Le terme « frauduleux » souligne bien que la pénétration n'est pas accidentelle. Elle résulte d'une violation de la volonté du « maître du système[19] » et suppose la conscience chez le délinquant que l'accès ou le maintien lui est interdit. Il n'est pas nécessaire, pour que l'information soit constituée, que l'accès soit limité par un dispositif de protection[20]. L'accès à une messagerie par un ancien salarié alors qu'il a conscience qu'il n'a plus le droit de l'utiliser est une pénétration frauduleuse[21].

La cour d'appel de Paris (5 avril 1994) a considéré que « l'accès frauduleux, au sens de la loi, vise tous les modes de pénétration irréguliers d'un système de traitement automatisé de données, que l'accédant travaille déjà sur la même machine mais entre dans un autre système, qu'il procède à distance ou qu'il se branche sur une ligne de communication ».

L'entrée frauduleuse oblige souvent à « casser » un mot de passe, mais elle peut être constituée par l'utilisation d'un système auquel un individu n'a pas de droit d'accès. Elle peut aussi être facilitée par un logiciel espion (*spyware*) ou un « cheval de Troie » qui permet de prendre le contrôle d'un ordinateur à distance. EDF a ainsi été condamnée pour avoir installé des chevaux de Troie dans les ordinateurs de membres de Greenpeace[22]. Mais le délit n'est pas constitué si le système n'est pas protégé contre les intrusions[23]. Ainsi, l'accès par erreur à un site non sécurisé ne peut être incriminé[24].

S'agissant du maintien frauduleux, la Cour de cassation[25] qualifie ainsi le fait de se connecter gratuitement avec son personnel au moyen d'un code d'accès qui avait été attribué pour une période d'essai.

---

19. Le Sénat, en première lecture, avait défini le « maître du système » comme étant « toute personne physique ou morale, toute autorité publique, tout service ou tout organisme qui est compétent pour disposer du système ou pour décider de sa conception, de son organisation ou de ses finalités ». Mais, comme pour les systèmes de traitement automatisés de données, l'Assemblée nationale n'a pas voulu figer la loi par des définitions qui pourraient se révéler trop rigides avec l'évolution des technologies ou des usages.
20. CA. Toulouse, 21 janvier 1999, « l'accès à un système informatisé de données tombe sous le coup de la loi pénale dès lors qu'il est le fait d'une personne qui n'a pas le droit d'y accéder ; la présence d'un dispositif de sécurité n'est pas nécessaire ».
21. Trib. Cor. Paris 1er janvier 2007.
22. Trib. Cor. Nanterre, 10 novembre 2001, Greenpace c/EDF.
23. TGI de Créteil, 21 février 2013
24. CA Paris, 30 octobre 2002, Kitetoa/Tati.
25. Cass. crim n° 07-81.045 du 3 octobre 2007.

2. L'affaire « Bluetouff »

L'affaire « *Bluetouff* » est l'illustration jurisprudentielle la plus médiatisée et politisée de la loi Godfrain, puisqu'elle va même être au cœur des débats parlementaires à l'occasion de l'examen de la loi pour une République numérique. En 2012, un internaute, Olivier Laurelli, navigant sous le pseudonyme *Bluetouff,* est entré dans le site extranet de l'Agence nationale de sécurité sanitaire de l'alimentation, de l'environnement et du travail (ANSES), opérateur d'importance vitale (OIV), via un VPN (*Virtual Private Network*) qui lui appartenait au Panama. L'accès, normalement autorisé par un contrôle avec identifiant et mot de passe, lui a été facilité par une faille du système. Il a été poursuivi devant le tribunal de grande instance de Créteil pour :

– accès frauduleux dans un système de traitement automatisé de données, infraction prévue par l'article 323-1 al. 1 du code pénal et réprimé par les articles 323-1 al. 1 et 323-5 du même code ;

– maintien frauduleux dans un système de transmission automatisé de données, infraction prévue et réprimée par les mêmes articles ;

Par jugement du 23 avril 2013, le tribunal relaxe *Bluetouff*.

2.a. Sur l'accès frauduleux

Pour le tribunal, les éléments constitutifs de l'accès frauduleux ne sont pas retenus, car c'est grâce à une défaillance technique qu'il a pu entrer sur le site et non par un « *hacking* ». Le maintien frauduleux, quant à lui, n'est pas caractérisé, l'auteur ayant pu penser que les données qu'il a consultées étaient libres d'accès. Sur appel du parquet, l'affaire vient devant la cour d'appel de Paris qui, par arrêt du 5 février 2014, confirme le jugement du TGI s'agissant de l'absence de caractère frauduleux de l'accès. Dans une autre affaire (CA Paris, 30 octobre 2002, Kitetoa/Tati), la cour avait déjà considéré que l'accès par erreur à un site non sécurisé ne pouvait être incriminé. Selon cet arrêt, « Il ne peut être reproché à un internaute d'accéder aux, ou de se maintenir dans les parties des sites qui peuvent être atteintes par la simple utilisation d'un logiciel grand public de navigation, ces parties de site, qui ne font par définition l'objet d'aucune protection de la part de l'exploitant du site ou de son prestataire de services, devant être réputées non confidentielles à défaut de toute indication contraire et de tout obstacle à l'accès ».

Plus récemment, le tribunal de grande instance de Paris[26] relaxe un prévenu qui est allé sur le site des billetteries de Weezent par simple consultation, sans intrusion, et a repéré les adresses des utilisateurs, disponibles et en accès libre pour chaque internaute par le moteur de recherche Google. Le tribunal rappelle que le

26. Tribunal de grande instance de Paris, 12e chambre, jugement correctionnel du 20 juin 2016, Weezevent /M. G.T. Voir note Marc Watin-Augouard, veille juridique septembre 2016, www.gendarmerie.interieur.gouv.fr/crgn

maintien dans un système automatisé de données, pour être frauduleux, suppose la conscience pour le contrevenant de l'irrégularité de ses actes. Pour que les infractions existent, il faut que le maître du système ait manifestement l'intention d'en restreindre l'accès aux « seules personnes autorisées ». Or, toutes les données auxquelles le prévenu a eu accès par un robot sont situées sur la partie publique du site et sont accessibles. Aucun avertissement relatif au caractère confidentiel du site ou des données n'apparaît au visiteur. Les conditions générales d'utilisation (CGU) des services de Weezevent, relatives à l'hébergement du contenu, montrent que ni la société Weezevent, ni les organisateurs, par le paramétrage de leur compte, n'ont manifesté l'intention d'en restreindre l'accès aux seules personnes autorisées.

2.b. Sur le maintien frauduleux

Sur le maintien frauduleux, la cour d'appel souligne qu'après avoir accédé au site, Bluetouff, en parcourant l'arborescence, avait pu constater que l'accès était soumis à des conditions d'authentification. Il avait donc « 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 ».

Par arrêt du 20 mai 2015, la chambre criminelle de la Cour de cassation[27] confirme l'arrêt de la cour d'appel de Paris. Elle condamne aussi l'auteur pour vol de données (voir infra).

B. L'entrave au fonctionnement d'un STAD

L'article 323-2 du code pénal réprime le fait d'entraver ou de fausser le fonctionnement d'un système de traitement automatisé de données. Cette infraction peut être constituée par l'injection d'un *malware,* d'une *bombe logique* ou par une attaque par déni de service (*Distributed Denial off Service* DDoS) par un *botnet*[28] qui met en action plusieurs milliers d'ordinateurs « zombies », dont

27. Cass. crim n° 14-8136, Olivier Laurelli, 20 mai 2015

28. Un botnet est un réseau d'ordinateurs, appelés « zombies », connectés à distance à un système de commande après avoir été infectés par un logiciel malveillant.
Le « pasteur » prend la main sur ce réseau avec le système de contrôle-commande pour, selon le but poursuivi :
– procéder à une attaque par déni de service ;
– diffuser des mails non sollicités (SPAM) ;
– extraire de manière frauduleuse des données.
La location d'un botnet de 80 à 120 000 machines revient environ à 200 $, ce qui fait du botnet l'arme du pauvre. Un réseau des machines infectées est à l'origine de l'attaque subie par la NSA, le 25 octobre 2013. En janvier 2012, à la suite de la fermeture du site Megaupload par le FBI, de nombreux sites officiels ont fait l'objet d'une telle attaque par les Anonymous. L'utilisation illégale du botnet ne doit pas être confondue avec la mise en réseau d'ordinateurs en vue de procéder à un travail de calcul ou de stockage distribué (par ex. blockchain). Sur le *botnet*, on se référera à la thèse fondatrice d'Eric Freyssinet : « Lutte

l'attaquant a pris le contrôle pour adresser à la cible autant de requêtes simultanées qui bloquent le système. Le déni de service peut résulter d'une attaque par réflexion. Des ordinateurs « réflecteurs » sont utilisés pour envoyer des requêtes sur la cible. Ces réflecteurs, leurrés par l'attaquant qui usurpe l'adresse Internet Protocol (IP) de la cible, lui répondent et génèrent ainsi un trafic qui la sature. D'autres attaques, dites volumétriques, augmentent l'occupation de la bande passante et obèrent ainsi les ressources de traitement de la cible. Constitue, par exemple, une entrave au fonctionnement d'un système de traitement automatisé de données, le fait de procéder à une attaque par « mailbombing » adressant simultanément 12 000 messages identiques[29] qui vont ralentir ou bloquer le fonctionnement par saturation.

L'intention de nuire doit être prouvée, comme le précise la cour d'appel de Bordeaux, dans un arrêt du 15 novembre 2011. La cour relaxe le prévenu qui, avec un robot générant 1 569 connexions en deux heures, avait, selon la plaignante C-Discount, ralenti puis bloqué son site. La cour relève que le trafic du site est de 16 000 requêtes/heure et que, selon un expert, une attaque efficace devrait être de 80 000 requêtes/heure. Elle souligne les moyens dérisoires déployés par le prévenu au regard des capacités informatiques du site.

C. La protection pénale des données

L'article 323-3 protège les données. C'est le seul article ayant fait à ce jour l'objet d'une demande de QPC. La Cour de cassation, saisie par la cour d'appel de Rennes, qui avait à examiner l'appel d'une condamnation d'une personne ayant défiguré un site internet du Front national, a déclaré la loi « claire et précise », et n'a donc pas renvoyé la QPC au Conseil constitutionnel.[30]

1. Les éléments constitutifs de l'atteinte aux données

L'article 323-3 du code pénal réprime l'introduction, la suppression ou la modification frauduleuse de données dans les systèmes de traitement automatisé.

La modification des données peut résulter d'une transgression de règles imposées à ceux qui sont en charge de leur gestion. Ainsi la cour d'appel de Riom, chambre correctionnelle, a condamné Jean-Claude X., par arrêt en date du 30 avril 1998, pour avoir modifié frauduleusement des données comptables saisies sur le logiciel de comptabilité de la CCI du Puy-en-Velay Yssingeaux,

---

contre les botnets : analyse et stratégie », Thèse de doctorat en informatique de l'Université Pierre et Marie Curie, novembre 2015.

29. Tribunal de grande instance de Nanterre, n° 0613971065 du 8 juin 2006, Société Amen/Michel M.

30. Décision du 10 avril 2013 de la Cour de cassation.

estimant qu'une écriture validée et introduite dans un système comptable automatisé constitue une donnée dont la suppression et la modification sont prohibées par les règles et principes comptables. La Cour de cassation[31] rejette son pourvoi en précisant que « le seul fait de modifier ou supprimer, en violation de la réglementation en vigueur, des données contenues dans un système de traitement automatisé caractérise le délit prévu à l'article 323-3 du Code pénal, sans qu'il soit nécessaire que ces modifications ou suppressions émanent d'une personne n'ayant pas un droit d'accès au système ni que leur auteur soit animé de la volonté de nuire ».

Les données peuvent être modifiées par défiguration (ou défacement ou « tag numérique ») de sites dans lesquels l'attaquant s'introduit pour changer le contenu des pages web. Cette action a pour objectif de nuire à l'image d'une personne (la photo d'une personnalité politique est remplacée par celle d'Hitler) ou à la réputation d'une entreprise. La modification peut consister en un remplacement de données (changement des notes d'un candidat à un examen, modification des prix pratiqués par un service de commerce en ligne, etc.).

Les données peuvent aussi être modifiées par un chiffrement malveillant préalable à une demande de rançon[32].

2. Le « vol » des données

M. Pietrasanta, rapporteur de la loi du 13 novembre 2014 renforçant les dispositions relatives à la lutte contre le terrorisme[33], affirmait lors des débats que « l'article 331-1 du code pénal définissant le vol comme la soustraction frauduleuse de la chose d'autrui pose deux conditions qui s'avèrent inadaptées au vol de données : d'une part, une donnée n'est pas une chose, mais un élément immatériel distinct de tout support de stockage ; d'autre part, une donnée extraite d'un STAD à la suite d'un accès ou d'un maintien frauduleux n'est pas nécessairement soustraite de celui-ci mais seulement extraite par sa reproduction sur un autre support[34] ». Pour le vol d'énergie, bien immatériel, le législateur a du recourir à une incrimination spécifique (article 311-2 du code pénal). La copie de données n'est pas une soustraction, puisque le légitime propriétaire les conserve et n'est à aucun moment dépossédé de la chose, sauf en cas de vol d'un disque dur. Les constituants de la propriété (*usus-abusus-fructus*) sont aussi inadaptés : peut-on parler de propriété sur les données à caractère personnel, puisque, tout en étant éventuellement exploitées commercialement, elles ne peuvent faire l'objet

31. Cass. Crim. n° 98-84752, 8 décembre 1999, Bulletin criminel 1999 N° 296 p. 917.
32. L'exemple le plus récent est celui du rançongiciel wannacry qui a fait plus de 300 000 victimes en mai 2017.
33. Loi n° 2014-1353 du 13 novembre 2014 renforçant les dispositions relatives à la lutte contre le terrorisme
34. Rapport n° 2173 CL. AN, 22 juillet 2014, M. Pietrasanta rapporteur.

d'un abandon de la part de leur détenteur[35] ? Pour éviter cet écueil, plusieurs voies étaient jusqu'alors possibles : poursuites pour contrefaçon, pour abus de confiance[36], etc. Mais elles ne couvraient pas toutes les hypothèses.

La jurisprudence a tenté d'y remédier. Dans un arrêt du 4 mars 2008[37], la Cour de cassation a qualifié de vol une copie de données, mais cette décision s'éloigne du principe selon lequel la loi pénale est d'interprétation stricte. Plus récemment, la Cour d'appel de Paris, dans son arrêt du 5 février 2014 précité, a condamné pour vol de données (7,7 Go) *Bluetouff* qui s'était introduit frauduleusement dans le site extranet de l'ANSES (voir supra). Il a, en effet, téléchargé des données qu'il a fixées sur plusieurs supports et partiellement publiées pour un article sur la légionellose, sans l'autorisation de l'Agence. En première instance, le tribunal correctionnel de Créteil avait considéré que, l'ANSES n'ayant jamais été dépossédée de fichiers qui sont restés accessibles et disponibles sur son site, il n'y a pas eu de soustraction de données et donc de vol.

La Cour de cassation a pourtant considéré que le vol était constitué. Dans ses conclusions, l'avocat général Frédéric Desportes s'est ainsi exprimé[38] : « Tout en respectant le principe d'interprétation stricte de la loi pénale, vous avez toujours su adapter les incriminations aux évolutions technologiques, veillant à ce que soit atteints les objectifs du législateur et donc à ce que la loi soit appliquée conformément à la fois à sa lettre et à son esprit. Cela est particulièrement vrai s'agissant du vol dont la définition a révélé une certaine

35. Nicolas Ochoa, « Pour en finir avec l'idée d'un droit de propriété sur ses données personnelles : ce que cache véritablement la principe de libre disposition », *RFDA* 2015, p. 1157.
36. Cass. crim, n° 13-82630 du 22 octobre 2014. « Le prévenu ayant, en connaissance de cause, détourné en les dupliquant, pour son usage personnel, au préjudice de son employeur, des fichiers informatiques contenant des informations confidentielles et mis à sa disposition pour un usage professionnel, la cour d'appel, qui a caractérisé en tous ses éléments, tant matériel qu'intentionnel, le délit d'abus de confiance, a justifié sa décision ». Alors qu'il rejoint une société concurrente, un salarié démissionnaire d'un cabinet de courtage d'assurances s'adresse en 54 messages, via sa messagerie personnelle, 305 fichiers informatisés. À la suite du contrôle interne, une perquisition à son domicile permet de découvrir 13 clés USB portant la dénomination de son ancien employeur et refermant 9 824 fichiers et documents de la société. Pour se justifier, il prétend que c'est pour son fonds documentaire personnel et pour travailler à son domicile. Il avait signé le 22 mai 2003 une « charte pour l'utilisation des ressources informatiques et des services Internet » lui rappelant l'interdiction d'extraire ces données ou de les reproduire sur d'autres supports informatiques sans l'accord préalable d'un responsable de service et de les détourner enfin de leur utilisation normale à des fins personnelles. La Cour de cassation qualifiant de « biens » des données informatiques, confirme l'arrêt de la cour d'appel de Bordeaux qui avait condamné le prévenu pour abus de confiance (art. 314-1 du Code pénal), car les fichiers informatiques ne lui avaient été remis qu'à charge d'en faire un usage déterminé, conforme à la charte informatique interne proscrivant l'extraction de ces documents de l'entreprise.
37. Cass. crim., n° 07-84.002, 4 mars 2008, X/ Société Graphibus non publié.
38. Avis non publié.

plasticité. *[…]* 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 ». Cet arrêt n'a désormais qu'un intérêt historique (sauf pour les affaires antérieures ou si la CEDH donne raison à *Bluetouff*).

Pour sortir de toute ambiguïté, l'Assemblée nationale a donc modifié l'article 323-3, par la loi du 13 novembre 2014[39]. Celle-ci, sans jamais évoquer le « vol », réprime désormais l'extraction, la détention, la reproduction, la transmission de données contenues dans le système. Les victimes seront désormais plus enclines à porter plainte, les procédures bénéficieront d'une meilleure sécurité juridique.

D. L'analyse *in concreto* des atteintes aux STAD

Les infractions présentées *supra* peuvent se cumuler, car elles portent sur des intérêts distincts. Une même attaque peut commencer par une pénétration suivie généralement d'un maintien frauduleux. Elle peut avoir pour effets d'entraver le fonctionnement du système, tout en portant atteinte aux données. Si dans l'esprit du législateur, chaque article satisfait à une finalité particulière, l'analyse *in concreto* est souvent nécessaire. C'est l'enquête judiciaire et l'expertise technique qui permettent de trancher.

Par exemple, le chiffrement volontaire de données peut entraver le fonctionnement d'un système qui ne peut plus les exploiter. Mais ce chiffrement correspond aussi à une modification des données qui ne sont plus les mêmes, une fois appliquée la clef aux données initiales. Doublé d'une demande de rançon, c'est une extorsion. C'est donc l'effet majeur escompté par l'auteur qui permet de qualifier l'infraction avec précision.

Les infractions à la loi Godfrain sont indifférentes au mobile. Elles s'appliquent à la délinquance comme au terrorisme, ou à la cyberconflictualité. Une attaque par déni de service peut aussi bien viser un objectif crapuleux (demande de rançon pour lever le blocage d'un site), un objectif terroriste[40] (atteinte d'un STAD troublant gravement l'ordre public par l'intimidation ou la terreur) ou un objectif politique. Dans ce dernier cas, on comprend que la lutte contre la cybercriminalité rejoigne, dans le haut du spectre, ce que l'on qualifie de cyberconflictualité. Il s'agit bien de cybercriminalité, car aucune preuve de l'implication

39. Loi n° 2014-1353 du 13 novembre 2014 renforçant les dispositions relatives à la lutte contre le terrorisme (art. 16).

40. Dès la réforme du code pénal (1992-1994), le législateur est dans une démarche d'anticipation lorsqu'il inscrit les infractions en matière informatique prévues par la loi Godfrain parmi celles dont la finalité permet de recevoir une qualification terroriste (article 421-1 2°).

d'un État n'est généralement avancée. Tant que le droit des conflits armés ne peut être invoqué, le droit commun s'applique et avec lui la loi Godfrain.

Indifférente au mobile, la loi Godfrain ne l'est pas à la pluralité des attaquants ou aux cibles visées.

II. Une responsabilité pénale des hackers à géométrie variable

Les atteintes aux systèmes de traitement automatisé de données sont sanctionnées par le droit pénal. Quelle que soit leur ampleur, en dehors de tout contexte juridique de guerre, la loi Godfrain s'applique. Elle est aggravée dans certaines circonstances qui prennent en compte la pluralité des acteurs ou la nature des systèmes ciblés (**A**). Mais, parce que les mesures les plus « offensives » de cybersécurité peuvent être mises en œuvre dans un contexte d'application du droit commun, il convient de protéger les acteurs contre toute poursuite pénale, lorsqu'ils sont conduits à commettre eux-mêmes des actes prévus et réprimés par la loi Godfrain (**B**). Plus délicate est la question de la responsabilité pénale du « hacker éthique », dont le rôle est croissant, compte tenu des enjeux de sécurité de l'espace numérique (**C**).

A. Les cas d'aggravation

L'action du hacker isolé demeure d'actualité. Elle n'est pas, en principe, de nature à déstabiliser un État, un secteur critique, une entreprise, même si une attaque bien ciblée peut avoir des conséquences graves, comme le souligne l'attaque 10-21 commise par un individu mécontent du Playstation Network de Sony… Les actions menées par des groupes sont, en général, plus dangereuses pour les STAD, ce qui justifie une répression plus sévère. Par ailleurs, depuis 2012, le législateur a voulu protéger davantage les systèmes de l'État mettant en œuvre des données à caractère personnel.

1. Une répression plus sévère de l'action commise en bande organisée

Dès 1988, la loi Godfrain a prévu la pluralité des auteurs d'attaques informatiques en réprimant l'association de malfaiteurs (art. 323-4 CP), c'est-à-dire la participation à un groupement formé ou à une entente en vue de la préparation, caractérisée par un ou plusieurs faits matériels, d'une ou de plusieurs infractions prévues par les articles 323-1 à 323-3-1. Cette incrimination permet d'agir à titre préventif, au stade de la préparation de l'infraction. Mais elle ne conduit pas à une aggravation, car les faits sont punis des peines prévues respectivement pour l'infraction elle-même ou pour l'infraction la plus sévèrement réprimée.

La loi renforçant les dispositions relatives à la lutte contre le terrorisme introduit la circonstance aggravante de bande organisée (art. 323-4-1) qui répond au

passage du hacker isolé au groupe structuré, organisé. Par exemple, le groupe appelé *Cybervor* serait composé d'une douzaine de russes, dont l'activité a été révélée en août 2014. À leur actif, le piratage de 1,2 milliards de données (combinaisons d'émail et de mots de passe) sur 420 000 sites web. On est loin du pirate isolé des années quatre-vingt.

Les infractions de la loi Godfrain ne figuraient pas dans la liste dressée par l'article 706-73 du code de procédure pénale, mais l'article 706-74 du même code disposait que « lorsque la loi le prévoit, les dispositions du présent titre sont également applicables aux crimes et délits en bande organisée autres que ceux relevant de l'article 706-73 ». Dans le nouveau titre XXIV, créé par la loi du 13 novembre 2014 renforçant les dispositions relatives à la lutte contre le terrorisme, et intitulé « De la procédure applicable aux atteintes aux systèmes de traitement automatisé de données », le législateur insère l'article 706-72 pour les seules infractions à l'encontre d'un système de traitement automatisé de données à caractère personnel mis en œuvre par l'État. Cet article, qui énumère les articles de procédure applicables aux atteintes aux STAD, emprunte la plupart des dispositions prévues pour la lutte contre la criminalité organisée (cyberinfiltration, captation de données, etc.), à l'exception de certaines mesures (garde à vue portée à quatre jours et perquisition de nuit).

La loi renforçant la lutte contre le crime organisé, le terrorisme et leur financement, et améliorant l'efficacité et les garanties de la procédure pénale aligne le régime procédural dérogatoire applicable à ces atteintes informatiques sur celui qui est prévu pour toutes les infractions de gravité comparable qui figurent à l'article 706-73-1 du code de procédure pénale. Il permet notamment la compétence des juridictions interrégionales spécialisées et les perquisitions de nuit jusqu'alors exclues. Toutefois l'application à ces infractions des règles dérogatoires de la garde à vue prolongée (article 706-88 CPP) n'est toujours pas possible puisque, selon la jurisprudence du Conseil constitutionnel, elles sont réservées aux seules infractions susceptibles de porter atteinte « à la sécurité, à la dignité ou à la vie des personnes[41] ».

La combinaison de l'article 706-72 avec l'article 706-73-1 montre l'étendue des investigations qui peuvent être menées.

Article du CPP	
art. 706-80	Extension de la compétence territoriale des OPJ et des APJ pour surveiller les personnes suspectes
art. 706-81 et s.	Opérations d'infiltration permettant aux OPJ et APJ d'utiliser une identité d'emprunt et de commettre certains actes illicites limitativement énumérés
art. 706-87-1	Enquête sous pseudonyme

41. Décision n° 2015-508 QPC du 11 décembre 2015

Article du CPP	
art. 706-89 à 706-94	Perquisitions de nuit
art. 706-95	Interception de correspondances émises par la voie des télécommunications
Art. 706-95-1 et s.	Saisies de données informatiques
art. 706-96 à 706-102	Sonorisation et la fixation d'images de certains lieux ou véhicules
art. 706-102-1 et s.	Captation des données informatiques à l'insu de la personne
art. 706-103	Mesures conservatoires sur les biens de la personne mise en examen
Art. 706-75 et suivants	Compétence possible des JIRS

L'aggravation et la procédure décrites supra ne concernent que les atteintes aux systèmes de traitement automatisé de données à caractère personnel mis en œuvre par l'État.

2. La protection particulière des systèmes de traitement automatisé de données « à caractère personnel » mis en œuvre par l'État

La loi assortit chacune des trois infractions principales (art. 323-1 à 323-3) d'une aggravation de peine lorsqu'elles sont commises à l'encontre d'un système de traitement automatisé de données *à caractère personnel* mis en œuvre par l'État. Selon l'article 2 de la loi « informatique et libertés », « constitue un traitement de données à caractère personnel toute opération ou tout ensemble d'opérations portant sur de telles données, quel que soit le procédé utilisé, et notamment la collecte, l'enregistrement, l'organisation, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, ainsi que le verrouillage, l'effacement ou la destruction ».

Cette disposition, introduite par la loi relative à la protection de l'identité[42], a notamment pour objectif de protéger le fichier TES, base centrale des titres sécurisés, le casier judiciaire, le fichier des empreintes génétiques (FNAEG), le fichier CASSIOPEE[43] de la justice, etc.

L'écriture des articles précités indique que les autres systèmes mis en œuvre par l'État ne sont pas concernés. Des systèmes analogues hébergés par des collec-

42. Loi n° 2012-410 du 27 mars 2012 relative à la protection de l'identité (article 9).
43. Chaîne Applicative Supportant le Système d'Information Oriente Procédure pénale Et Enfants.

tivités territoriales ou leurs établissements publics, voire par des personnes privées exerçant des missions de service public, pourraient avoir la même sensibilité mais ne sont pas surprotégés.

Lors de l'examen du projet de loi renforçant la lutte contre le crime organisé, le terrorisme et leur financement, un amendement rejeté avait pour objet d'étendre la circonstance aggravante à l'ensemble des STAD mis en œuvre par les organismes publics ou privés, opérateurs d'importance vitale définis à l'article R. 1332-1 du code de la défense. Outre le fait qu'une telle mesure n'aurait concerné que le traitement automatisé à caractère personnel mis en œuvre par les opérateurs d'importance vitale, l'absence de publication de la liste des OIV aurait heurté le principe de légalité : comment imposer une aggravation si l'auteur ignore qu'il atteint un opérateur, dont la qualité est tenue secrète ? Cette absence d'extension est paradoxale : l'atteinte portée à certains systèmes critiques des OIV pourrait avoir des conséquences autrement plus graves.

En vérité, les sites les plus sensibles semblent être protégés par l'article 411-9 du code pénal qui réprime le fait de détruire, détériorer ou détourner tout […] système de traitement automatisé d'informations ou d'y apporter des malfaçons, lorsque ce fait est de nature à porter préjudice aux intérêts fondamentaux de la nation. On notera que les peines sont alors de quinze ans de détention criminelle, ce qui requiert un degré de gravité particulier quant à l'attaque et à ses conséquences. Le positionnement de cet article dans le livre IV soulève toutefois plusieurs interrogations :

– est-ce sa place, alors qu'il devrait figurer au sein de la « loi Godfrain », dans le livre III ? L'atteinte aux intérêts fondamentaux est le but poursuivi, la « destruction, la détérioration, le détournement ou l'apport de malfaçons » un moyen d'atteindre un système de traitement automatisé de données. Faut-il privilégier l'une à l'autre ? Il eût été plus cohérent d'ajouter dans la loi Godfrain une circonstance aggravante d'atteinte aux intérêts fondamentaux de la nation ;

– les atteintes ne sont pas définies de manière similaire dans l'article 411-9 et l'article 323-2, alors que les modes opératoires sont les mêmes ou sont très voisins. Le fait d'entraver ou de fausser le fonctionnement d'un STAD (art. 323-2 CP) est peut-être moins agressif que sa destruction ou sa détérioration. Mais une destruction, une détérioration ne portant pas préjudice aux intérêts fondamentaux de la nation relèverait bien de l'article 323-2. Si une nuance devait être apportée, il conviendrait alors de la préciser dans la circonstance aggravante évoquée s*upra* ;

– pourquoi attribuer à l'auteur d'une telle atteinte le statut de délinquant politique, comme le prouve la nature de la peine (détention criminelle) ? Les hackers « au chapeau noir » méritent-ils une telle exception sous prétexte qu'ils ont porté atteinte aux intérêts fondamentaux de la nation ?

B. L'irresponsabilité pénale reconnue à certains acteurs étatiques

Certains actes qui seraient normalement passibles de poursuites pénales au titre de la loi Godfrain font l'objet de dispositions législatives qui écartent la responsabilité des services ou des agents, dans des circonstances ou pour des finalités particulières. Sont ainsi protégés les services étatiques qui agissent dans le cadre de la cyberdéfense et les agents des services de renseignement appartenant au « premier cercle ».

1. L'irresponsabilité des services étatiques agissant dans le cadre de la cyberdéfense

S'agissant des actions liées à la cyberdéfense, la loi autorise plus qu'elle ne crée d'irresponsabilité. L'article L. 2321-2 du code de la défense (créé par l'article 21 de la loi du 18 décembre 2013 relative à la programmation militaire) porte sur les services de l'État et non sur les personnes physiques qui servent dans leurs rangs. Il va de soi que les agents de ces services sont indirectement protégés par l'ordre de la loi et le commandement de l'autorité légitime (art. 112-4 CP). Sont concernés les services[44] qui, dans les conditions fixées par le Premier ministre, répondent à une attaque informatique visant les systèmes d'information affectant le potentiel de guerre ou économique, la sécurité ou la capacité de survie de la Nation. Sans précision de la loi, on imagine aisément qu'il s'agit des systèmes intéressant la défense et la sécurité et plus généralement des systèmes critiques des opérateurs d'importance vitale. Ces services peuvent procéder aux opérations techniques nécessaires à la caractérisation de l'attaque et à la neutralisation de ses effets en accédant aux systèmes d'information qui sont à l'origine de l'attaque. Accéder signifie pénétrer, se maintenir, bien évidemment sans accord du « maître du système ». Cette exonération ne concerne que la réponse à une attaque et non des actions préventives ou préemptives qui relèvent d'une cyberdéfense très « offensive » que la loi ne couvre pas.

---

44. Arrêté du 7 juillet 2015 déterminant les services de l'État mentionnés au second alinéa de l'article L. 2321-2 du code de la défense
Article 1 : Les services de l'État mentionnés au second alinéa de l'article L. 2321-2 du code de la défense sont :
1° parmi les services relevant du Premier ministre : l'Agence nationale de la sécurité des systèmes d'information ;
2° Parmi les services relevant du ministre de la défense : le service du commandement opérationnel de cyberdéfense de l'Etat-major des armées, la direction technique de la direction générale de l'armement et la direction technique de la direction générale de la sécurité extérieure ;
3° Parmi les services relevant du ministre de l'intérieur : le service du haut fonctionnaire de défense et la direction technique de la direction générale de la sécurité extérieure.
[…]

Pour être également en mesure de répondre aux attaques mentionnées au premier alinéa, les services de l'État déterminés par le Premier ministre peuvent détenir des équipements, des programmes informatiques et toutes données susceptibles de permettre la réalisation d'une ou plusieurs des infractions prévues aux articles 323-1 à 323-3 du code pénal en vue d'analyser leur conception et d'observer leur fonctionnement. Sans cette autorisation, l'article 323-3-1 Code pénal (créé par art. 34 de la loi du 21 juin 2004 pour la confiance dans l'économie numérique) sanctionnerait le fait, sans motif légitime, notamment de recherche ou de sécurité informatique, d'importer, de détenir un programme informatique ou toute donnée conçus ou spécialement adaptés pour commettre une ou plusieurs infractions prévues par les articles 323-1 à 323-3[45]. Compte tenu de la montée en puissance de la cyberdéfense, il est indispensable d'écarter la responsabilité pénale des policiers, gendarmes, membres des armées, ingénieurs, experts, etc. appelés à utiliser ces moyens pour comprendre les attaques, voire pour mener, dans le cadre de la stratégie de cyberdéfense, une action plus « offensive ».

On s'étonnera du positionnement de l'article L. 2321-2 dans le code de la défense sous prétexte qu'il est issu de la LPM. La « dispersion législative » est de nature à priver la loi Godfrain de sa cohérence.

2. L'irresponsabilité pénale des agents des services de renseignement du « premier cercle »

Est, en revanche, correctement placé l'article 323-8 du code pénal, créé par la loi du 24 juillet 2015 relative au renseignement. Selon cet article, n'est pas pénalement responsable des infractions commises sur des systèmes de traitement automatisés de données prévues par les articles 323-1 à 323-7 du code pénal l'agent des services spécialisés de renseignements mentionnés à l'article L. 811-2 du code de la sécurité intérieure qui agit pour assurer, hors du territoire national, la protection des intérêts fondamentaux de la Nation mentionnés à l'article L. 811-3 du même code. Les services sont limitativement fixés par le décret du 28 septembre 2015[46] : Direction générale des services extérieurs (DGSE), Direction générale de la sécurité intérieure (DGSI), Direction du renseignement militaire (DRM), Direction du renseignement et de la sécurité de défense (DRSD), Direction nationale des recherches et enquêtes douanières (DNRED)

45. La Cour de cassation retient l'intention coupable d'un individu ne pouvant ignorer, en raison de son expertise, qu'il diffuse sur le portail interne, accessible à tous, d'une société, dont il est le gérant, des informations présentant un risque d'utilisation à des fins de piratage par un public particulier en recherche de ce type de déviance. Cass. crim., n° 09-82.346, 27 octobre 2009, Bulletin criminel 2009, n° 177.
46. Décret n° 2015-1185 du 28 septembre 2015 portant désignation des services spécialisés dans le renseignement.

et le service du traitement du renseignement et action contre les circuits financiers clandestins (TRACFIN). Ne sont donc pas concernés les services de police et de gendarmerie qui relèvent du « deuxième cercle » (art. 811-4 CSI). Cette exclusion s'explique par le fait que l'irresponsabilité pénale ne couvre que les faits commis hors du territoire national. S'agissant des objectifs visés, ils sont énoncés par l'article 811-3 du CSI qui ne donne pas la même définition des intérêts fondamentaux de la Nation que l'article 410-1 du code pénal. Comprenne qui pourra !

C. « Hackers Ethiques » et loi Godfrain

La cybersécurité repose aussi sur l'action des acteurs privés, opérateurs, fournisseurs d'accès, hébergeurs, intégrateurs, éditeurs de produits de sécurité, prestataires de services de confiance et organismes de qualification etc. Dès l'apparition des « hackers au chapeau noir[47] », dans les années quatre-vingt, un secteur privé de la sécurité des systèmes d'information (SSI) s'est développé pour s'inscrire, depuis 2008, dans la stratégie de cybersécurité. Il agit le plus souvent en amont de la cybercriminalité (prévention) et en aval (continuité et rétablissement d'activité). Dans le cyberespace, « État et entreprises doivent être solidaires, échanger leurs informations et mettre en commun leurs moyens »[48].

Une contribution moins institutionnelle est aussi apportée par des internautes agissant généralement seuls. Les « hackeurs éthiques » sont au cœur de la réflexion, car chacun est conscient de l'impossibilité de résoudre tous les problèmes de sécurité de l'espace numérique par le seul recours à l'offre régalienne ou à l'offre des opérateurs privés. Ces hackers produisent une sécurité du bas vers le haut (ou « bottom up »…) et contribuent de manière collaborative et originale à la sécurité des systèmes en détectant les failles, notamment les failles « zero day », celles qui sont inédites.

Si le cas des hackers agissant dans le cadre d'un contrat de *bug bounty* ne pose guère de difficultés, la situation au regard de la loi des hackers « autonomes » est plus délicate, car toute brèche ouverte dans la loi Godfrain en affaiblirait la portée.

1. Les Bug bounty

Des *Ethical Hackers* sont sollicités par des entreprises pour détecter des failles dans la sécurisation de leurs données. Ils sont recrutés (*inside*) ou agissent par

47. Ces « hackers », contrairement aux « hackers au chapeau blanc » qui agissent pour protéger les systèmes, ont une démarche illégale puisqu'ils cherchent à pénétrer avec des intentions frauduleuses les systèmes de traitement automatisé de données.
48. Alain Juillet, président du CDSE, interview, *Les Échos*, 5 octobre 2014.

contrat (*outside*) pour effectuer des tests de pénétration, entraîner le personnel des SOC (Security Operation Center), effectuer des audits de sites, de produits. Ils n'ont pas toutefois le « permis de cyber-tuer ». Le concept de *Bug Bounty Program* est né aux États-Unis en 1996 chez Netscape. Facebook a ainsi fait appel à des hackers qui ont découvert, en 2014, plus de 17 000 bugs, dont 61 considérés comme particulièrement graves. Le programme *Cyber Fast Track*, lancé en 2011 par la DARPA[49], repose en partie sur la collaboration de communautés de hackers… En avril 2016, le programme *Hack the Pentagone* a mobilisé plus de 1 000 hackers.

Cette pratique se développe avec l'association de hackers ou de pentesters[50] qui sont sollicités par les propriétaires de systèmes pour rechercher les failles. La création, début 2016, par des Français, de Bug Bounty Factory, première entreprise européenne offrant de tels services est une illustration parfaite de la « sécurité venant du public » (crowd security).

Le contrat de bug bounty délimite clairement dans le temps et dans l'espace le périmètre des investigations sur l'infrastructure, les sites ou les logiciels permises au pentester. Il exclut toute altération du système, toute destruction de données. Les contraintes sont d'autant plus fortes que des données à caractère personnel sont en jeu. Outre son obligation de confidentialité, le cocontractant n'a pas une obligation de moyens mais de résultat. Généralement, la découverte d'une faille est rémunérée selon son importance[51]. Le montant de sa rémunération est d'autant plus élevé que la faille découverte est critique et assortie de recommandations (Proof of Concept). L'avantage du système est de mobiliser un nombre très important d'experts à un coût plus faible que le recours à un cabinet d'audit qui, comme le souligne la plate-forme Yogosha, spécialisée en bug bounty, facture en jour/homme, qu'il trouve dix failles ou qu'il ne trouve rien. Le pentester est évalué, ce qui permet de faire évoluer son profil et d'offrir une garantie de crédibilité.

L'université de Valenciennes dispense un master en cyberdéfense qui s'appuie sur le hacking éthique. Le Forum international de la cybersécurité (FIC) organise, depuis 2013, des challenges permettant aux entreprises ou aux administrations de détecter des compétences. En 2015, le « Nuit du Hack », qui rassemble près de 2000 participants, a été ouverte par Guillaume Poupard, directeur général de l'ANSSI… C'est dire si le regard vis-à-vis des hackers a évolué, le terme ne devant plus avoir la connotation péjorative qu'on lui attribue habituellement.

Eric Filiol, ancien militaire, directeur de recherche à l'École supérieure d'informatique, électronique, automatique (ESIA) ne peut être considéré comme un laxiste. Il invite à aller chercher la ressource là où elle est, c'est-à-dire chez les

49. Defense Advanced Research Projects Agency.

50. *Pentest*, contraction en anglais de *penetration test.*

51. Par exemple Swisscom rémunère de 150 francs suisses à 10 000 francs suisses pour les failles les plus importantes.

hackers que l'on a tendance, selon lui, à diaboliser à l'excès, car « ils sont capables d'analyser en profondeur un système – que ce système soit technique comme un ordinateur ou un téléphone, mais également humain, social, législatif – de sorte à en comprendre les mécanismes les plus intimes, en privilégiant le résultat sur la méthode, contrairement souvent à l'approche académique[52] ».

Si le contrat de Bug Bounty offre un cadre juridique clair qu'en est-il du lanceur d'alerte, dont le statut est en cours d'adoption dans le cadre du projet de loi Sapin 2 ?

2. Les lanceurs d'alerte

Les lanceurs d'alerte sont, d'après le Conseil d'État[53], des personnes qui « signalent, de bonne foi, librement et dans l'intérêt général, de l'intérieur d'une organisation ou de l'extérieur, des manquements graves à la loi ou des risques graves menaçant des intérêts publics ou privés, dont ils ne sont pas l'auteur ». Cette définition a le mérite de clarifier la position du lanceur d'alerte au regard du code pénal : il n'est pas l'auteur des faits qu'il dénonce ou signale. Il leur est extérieur. Le lanceur d'alerte ne participe pas à un ou plusieurs actes matériels de l'infraction, sinon il serait auteur, coauteur ou complice. Cette précision est d'importance, car le discours de certains commentateurs, voire de parlementaires, sur la loi « Sapin 2 », n'est pas dépourvu d'ambiguïtés.

Dans sa rédaction, l'article 6 définit le lanceur d'alerte comme « une personne physique qui révèle ou signale, de manière désintéressée et de bonne foi, un crime ou un délit, une violation grave et manifeste d'un engagement international régulièrement ratifié ou approuvé par la France, d'un acte unilatéral d'une organisation internationale pris sur le fondement d'un tel engagement, de la loi ou du règlement, ou une menace ou un préjudice graves pour l'intérêt général, dont elle a eu personnellement connaissance. Les faits, informations ou documents, quel que soit leur forme ou leur support, couverts par le secret de la défense nationale, le secret médical ou le secret des relations entre un avocat et son client sont exclus du régime de l'alerte défini par le présent chapitre. »

Le mot « désintéressé » place donc le lanceur d'alerte dans un cadre distinct de celui du *pentester* qui agit dans un cadre contractuel et reçoit une prime. Dans son rapport[54], le député Sébastien DENAJA est explicite : « nous refusons la vision anglo-saxonne qui, à certains égards, transforme les lanceurs d'alerte en chasseurs de prime. En France, au lieu de chasseurs de primes, nous voulons des gens qui défendent l'intérêt général et qui le fassent de bonne foi ».

---

52. Eric Filiol, Cyberguerre, le retard français, blog Club des Vigilants, 9 septembre 2011.
53. « Le droit d'alerte : signaler, traiter, protéger », étude adoptée le 25 février 2016 par l'Assemblée générale plénière, La Documentation française.
54. Sébastien DENAJA, rapporteur, rapport AN n° 405, 21 septembre 2016.

Le lanceur d'alerte peut utiliser trois canaux dont la gradation est prévue par la loi. Le premier niveau est celui du déontologue de l'entreprise ou de l'administration ou, à défaut, du supérieur hiérarchique. Les interlocuteurs externes (justice, autorités administratives sectorielles[55], autorités administratives indépendantes[56], ordres professionnels, etc.) appartiennent au second niveau. En dernier ressort, en cas d'échec de l'alerte ou d'urgence, l'opinion peut être saisie.

S'agissant d'atteintes aux systèmes de traitement automatisé de données, le lanceur d'alerte peut être le témoin d'actes malveillants qui lui sont étrangers. On notera toutefois que s'il est « autorité constituée, officier public, ou fonctionnaire dans l'exercice de ses fonctions », l'article 40 du code de procédure pénale l'oblige à porter à la connaissance du procureur de la République les faits susceptibles de constituer une infraction.

S'ils ne peuvent avoir la qualité de lanceur d'alerte et la protection qui s'y rattache, comment alors analyser les « autonomes » au regard du code pénal ?

3. Les « hackers autonomes »

Ces hackers sont autonomes dans la mesure où ils agissent sans concertation avec le « maître du système ». Les « autonomes » testent les systèmes et, pour ce faire, y pénètrent ou s'y maintiennent le plus souvent sans droit ni titre. Ils commettent donc des actes matériels qui entrent dans la définition des infractions à la loi Godfrain.

3.a. Ni lanceurs d'alerte ni repentis

L'arrêt de la chambre criminelle de la Cour de cassation[57] du 20 mai 2015 cité supra a été fortement médiatisé et politisé, car il oppose les « libertaires » aux « sécuritaires ». Il connaît un rebondissement, à l'Assemblée nationale, lors de l'examen de la loi pour une République Numérique, avec la proposition d'un amendement[58] ainsi rédigé : « Ne peut donner lieu à des poursuites pénales, le délit prévu au premier alinéa (NDLR : de l'article 323-1), commis par une personne qui a averti immédiatement l'autorité administrative ou judiciaire, la Commission nationale de l'informatique et des libertés ou le responsable du traitement automatisé de données ». L'exposé sommaire fait directement référence à « Bluetooff ». On peut s'interroger sur une telle disposition qui aurait limité l'action action publique (art. 1er du CPP). Comment peut-on envisager qu'une infraction tentée ou commise ne puisse donner

55. Par exemple L'ANSSI pour l'atteinte aux STAD.
56. Par exemple la CNIL pour les traitements illégaux de données à caractère personnel.
57. Cass. crim n° 14-8136, Olivier Laurelli, 20 mai 2015.
58. Amendement n° 496 soutenu notamment par Isabelle Attard et Serge Coronado.

lieu à un examen par le ministère public, seul juge de l'opportunité des poursuites[59] ?

Finalement, les députés se mettent d'accord lors de la première (et seule) lecture du texte[60] : toute personne qui a tenté de commettre ou a commis le délit d'accès ou de maintien frauduleux serait exemptée de peine, si elle a immédiatement averti l'autorité administrative ou judiciaire ou le responsable du système de traitement automatisé de données en cause d'un risque d'atteinte aux données ou au fonctionnement du système. Mais une telle disposition aurait créé une confusion avec le « statut » de repenti : dans le « monde réel », le repentir est pris en considération par le code pénal, notamment depuis la loi « Perben II » du 9 mars 2004 (art. 132-78 CP[61]), avec pour objectif d'empêcher la concrétisation d'une menace imminente et non un risque potentiel, ou de limiter les effets d'une infraction consommée.

Une faille dans un logiciel est un risque et non une menace, tant qu'une personne mal intentionnée ne l'a pas exploitée. L'amendement aurait remis en cause l'équilibre de l'article 323-1 et l'aurait même fortement affaibli. Comment imaginer une enquête longue et coûteuse dont l'issue serait connue d'avance s'agissant de la peine ? De fait, n'irait-on pas vers une exemption des poursuites ? Comment se matérialiserait l'avertissement immédiat de l'autorité ? Un simple mail serait-il suffisant pour obtenir l'impunité ? Il convient de ne pas mélanger des situations différentes au regard de l'intention coupable. Les « hackers » sans scrupule doivent être sanctionnés, tandis que les pentesters, agissant sans comportement frauduleux, doivent être protégés.

Nathalie Kosciusko-Morizet revient sur cette disposition à l'occasion de l'examen de la loi « Sapin 2 » avec une amendement complétant l'article 323-1 du code pénal par une phrase ainsi rédigée : « Toute personne qui a tenté de commettre ou commis ce délit de bonne foi est exemptée de poursuites si, ayant averti immédiatement l'autorité administrative ou judiciaire, ou le responsable du système de traitement automatisé de données en cause, elle a permis d'éviter toute atteinte ultérieure aux données ou au fonctionnement du système ». Une novation et une confusion : la novation, la commission d'une action frauduleuse « de bonne foi » qui ne manquera de susciter des interrogations chez les pénalistes, la « bonne foi » étant par nature contraire à la démarche « frauduleuse » constitutive de l'infraction prévue à l'article 323-1 ; une confusion, celle du statut de repenti avec celui de lanceur d'alerte : Afin de permettre aux internautes de continuer à exercer leur vigilance sur les failles de sécurité, jouant ainsi le

59. Même si, dans certains cas particuliers, l'action publique est conditionnée par la plainte de la victime, la dénonciation d'autorités étrangères, etc.
60. Article 20 septies du texte adopté en première lecture par l'AN.
61. Le décret d'application n° 2014-346 a été publié le 17 mars 2014, soit près de dix ans après… Le code pénal, vise les infractions de complot contre la sûreté de l'État, le terrorisme, la traite des êtres humains, l'association de malfaiteurs, les infractions concernant la fausse monnaie, le blanchiment, la corruption, le trafic d'influence, etc.

rôle utile de sentinelles du web, et afin d'éviter la répétition de jurisprudences contradictoires et incertaines, il serait souhaitable d'établir un cadre juridique exonérant de responsabilité les lanceurs d'alerte, personnes détectant et signalant les failles de sécurité informatique de bonne foi, sans intention de nuire, par exemple en s'inspirant de l'article 221-5-3 du code pénal qui dispose pour les assassinats : « Toute personne qui a tenté de commettre les crimes d'assassinat ou d'empoisonnement est exempte de peine si, ayant averti l'autorité administrative ou judiciaire, elle a permis d'éviter la mort de la victime et d'identifier, le cas échéant, les autres auteurs ou complices ». Curieuse et hasardeuse comparaison entre l'assassinat et la pénétration frauduleuse dans un système de traitement automatisé de données !

Finalement, à défaut d'être idéale, la solution retenue par la loi pour une République numérique semble être la plus acceptable.

3.b. L'ANSSI « arbitre des élégances »

Les hackers désintéressés peuvent contribuer à la cybersécurité, à condition qu'ils s'appuient sur un code de conduite clair garantissant l'absence de dol spécial. Cette position est soutenue par Guillaume Poupard, directeur général de l'ANSSI. Lors de l'examen de la loi pour la République Numérique, Axelle Lemaire exprime le souhait de « faire alliance avec la multitude d'informaticiens compétents et avec la communauté externe des développeurs pour identifier et corriger plus rapidement les failles de sécurité dans un cadre légal sûr ».

Pour éviter les écueils énoncés supra, une solution plus sage est trouvée par le Sénat. Il s'agit d'une dispense des obligations prévues par l'article 40 du CPP au profit de l'ANSSI, dès lors que celle-ci est saisie par un hacker ayant agi de bonne foi, sans avoir donné une publicité à sa découverte. « Pour les besoins de la sécurité des systèmes d'information, l'obligation prévue à l'article 40 du code de procédure pénale n'est pas applicable à l'égard d'une personne de bonne foi qui transmet à la seule autorité nationale de sécurité des systèmes d'information une information sur l'existence d'une vulnérabilité concernant la sécurité d'un système de traitement automatisé de données ». L'ANSSI préserve la confidentialité de l'identité de la personne à l'origine de la transmission ainsi que des conditions dans lesquelles celle-ci a été effectuée. Elle peut procéder aux opérations techniques strictement nécessaires à la caractérisation du risque ou de la menace qui lui est présenté pour avertir l'hébergeur, l'opérateur ou le responsable du système d'information. On notera que l'expression « de bonne foi » est restée dans le texte, alors qu'il eût été préférable, pour les raisons exposées supra, de mentionner l'absence de volonté de nuire.

Pour autant, la dispense ainsi reconnue ne fait pas obstacle à l'exercice de l'action publique qui demeure une prérogative du parquet. Libre à lui de poursuivre s'il estime que l'infraction est constituée et, en particulier, en cas de plainte de la victime. Faute avouée n'est pas obligatoirement pardonnée. On peut toutefois

concevoir qu'un « blanc-seing » de l'ANSSI entraîne, pour des motifs d'opportunité, un classement sans suite. Malheureusement, cette disposition est intégrée dans le code de la défense (art. L. 2321-4), ce qui affaiblit une fois de plus l'unité de la loi Godfrain.

Les atteintes aux systèmes de traitement automatisé de données mettent en jeu des mécanismes complexes et nécessitent pour leur traitement judiciaire une compréhension des aspects techniques afin d'appliquer le droit. Si le numérique est entré dans tous les prétoires, les infractions les plus graves requièrent un certain niveau de spécialisation, à l'instar de ce qui existe pour le terrorisme, la criminalité organisée, la santé publique, la mer, les accidents collectifs[62]. Cette nécessaire spécialisation a été prise en compte par François Molins, procureur de la République de Paris qui a créé, en septembre 2014, une section spécialisée – dite F1 – dédiée à la lutte contre la délinquance astucieuse et la cybercriminalité, dont le pôle cybercriminalité, composé de deux vice-procureurs et d'un assistant spécialisé, compétent pour les atteintes aux systèmes de traitement automatisé de données et les faux ordres de virements internationaux.

Jean-Marie Bockel dans son rapport sur la cyberdéfense[63] et l'auteur de ces lignes[64] ont régulièrement soutenu cette position, défendue avec constance par Myriam Quéméner, magistrate, conseillère du préfet « cyber », pionnière de la lutte contre la cybercriminalité au sein de la justice. Pour écarter cette idée, le garde des Sceaux considérait que l'organisation judiciaire, reposant notamment sur l'existence de huit juridictions interrégionales spécialisées (JIRS), était apte à prendre en charge ce type de contentieux. Lors de l'examen de la loi renforçant la lutte contre le crime organisé, le terrorisme et leur financement, et améliorant l'efficacité et les garanties de la procédure pénale, cette question est venue à l'ordre du jour. Si le député Meyer Habib a déposé sans succès un amendement en vue de créer « des parquets et de juridictions spécialisées composés de magistrats *disposant des connaissances techniques suffisantes pour conduire les instructions et juger les dossiers* », la commission des lois du Sénat a imposé ses vues, malgré l'avis défavorable du gouvernement.

La loi du 3 juin 2016 renforçant la lutte contre le crime organisé, le terrorisme et leur financement, et améliorant l'efficacité et les garanties de la procédure pénale crée l'article 706-72 du CPP. Les actes incriminés par les articles 323-1 à 323-4-1 et 411-9 du code pénal, lorsqu'ils sont commis sur un système de traitement automatisé d'informations, sont désormais poursuivis, instruits et jugés selon des règles particulières fixées par les articles 706-72-1 à 706-72-6

62. Le décret n° 2014-1634 du 26 décembre 2014 crée à Paris et à Marseille des juridictions interrégionales spécialisées en matière d'accidents collectifs.
63. Jean-Marie Bockel, rapport d'information n° 681 fait au nom de la commission des affaires étrangères, de la défense et des forces armées, déposé le 18 juillet 2012.
64. Marc Watin-Augouard, *Cybermenaces et sécurité nationale*, Le droit de la sécurité et de la défense en 2013, Presses Universitaires d'Aix-Marseille, p. 306 ; du même auteur, *Pour que le crime ne paie pas,* www.lesechos.fr, 20 janvier 2014.

du CPP. Ces articles instituent une compétence concurrente du procureur de la République, du pôle de l'instruction, du tribunal correctionnel et de la cour d'assises de Paris. Cela ne signifie pas le dessaisissement automatique des juridictions compétentes en vertu des articles 43, 52 et 382 du CPP. L'initiative appartient au procureur de la République territorialement compétent. La juridiction parisienne a l'obligation de se déclarer incompétente quand les faits ne relèvent pas des infractions de cybercriminalité limitativement énumérés. Les infractions commises au moyen des nouvelles technologies de l'information, soit pour véhiculer des contenus illicites, soit pour faciliter la commission d'une autre infraction, ne sont pas concernées par cette compétence concurrente.

Comme le souligne Michel Mercier, ancien garde des Sceaux et rapporteur de la loi, « Cette compétence non exclusive permet aux juridictions territoriales de droit commun de pouvoir mener investigations et poursuites dans un cadre souple sans induire une compétence systématique de la juridiction parisienne. Néanmoins, la nécessaire communication avec celle-ci entraîne une centralisation des informations et donc des recoupements et une exploitation optimale des informations. Elle organise une certaine centralisation du contentieux, une synergie des moyens en confiant le traitement des affaires les plus complexes à des services spécialisés ; enfin elle contribue à la définition d'une stratégie pénale[65] ». Le rapporteur ajoute pour justifier sa position qu'il existe « un important contentieux lié aux infractions terroristes commises par la voie d'un service de communication au public en ligne qui relève d'ores et déjà de la compétence de la juridiction parisienne. De plus, les cyber-attaques relèvent parfois de la même organisation et de l'utilisation des mêmes techniques que les groupements terroristes. Par ailleurs, le parquet de Paris dispose d'une compétence concurrente, en application de l'article 693 du code de procédure pénale, pour connaître des infractions commises hors du territoire français, à l'instar de la plupart des infractions cybercriminelles. Il est à souligner que l'exercice de cette compétence pourrait s'appuyer sur le réseau de référents cybercriminalité, dont un membre est présent dans chaque parquet ».

La poursuite devant les juridictions des infractions à la loi Godfrain nécessite l'arrestation du ou des auteurs et la mise en évidence des preuves numériques. Dans de nombreux cas, la cyberattaque ne peut être attribuée, compte tenu des méthodes employées pour rendre difficile ou impossible son attribution. De plus en plus, les victimes potentielles se tournent vers la prévention en ayant recours au renseignement d'origine cyber (ROC) ou d'intérêt cyber (RIC) pour contrer les menaces. La « Threat Intelligence » agit au début de la « chaîne cybercriminelle » (Cyber Killchain), *iter criminis* adapté par Lockeed Martin[66]. La « Threat intelligence » porte sur le contexte (international, national, propre à

65. Rapport n° 491 Tome I, de Michel Mercier, fait au nom de la commission des lois, mars 2016.

66. www.lockeedmartin.com/us/news. Voir également Adrien Petit, *Cyber Threat Intelligence*, Observatoire FIC, 3 avril 2015.

la cible), sur la connaissance des modes opératoires de l'adversaire, sur les actes préparatoires annonciateurs d'une cyberattaque, en analysant les signaux faibles, les comportements atypiques qui, corrélés par le Big data, sont annonciateurs d'une cyberattaque. Elle exige donc un dispositif de veille et la possession d'outils permettant d'identifier et de discriminer les informations utiles. Un nouveau champ pour la prévention de la délinquance qui associe pleinement les acteurs publics et les acteurs privés, dont la coopération est catalysée par les difficultés d'application de la loi Godfrain.