La Revue des droits de l'homme

Actualités Droits-Libertés

Félix Tréguer

Le droit pénal de la fraude informatique, nouvel ami des censeurs ?

Liberté d'expression (Loi Godfrain du 5 janvier 1988 et code pénal)

Référence électronique
Félix Tréguer, « Le droit pénal de la fraude informatique, nouvel ami des censeurs ? », *La Revue des droits de l'homme* [En ligne], Actualités Droits-Libertés, mis en ligne le 02 juin 2015, consulté le 20 juillet 2015. URL : http://revdh.revues.org/1328

Éditeur : Centre de recherches et d'études sur les droits fondamentaux (CREDOF)
http://revdh.revues.org
http://www.revues.org

Document accessible en ligne sur :
http://revdh.revues.org/1328
Document généré automatiquement le 20 juillet 2015.

Félix Tréguer

Le droit pénal de la fraude informatique, nouvel ami des censeurs ?

Liberté d'expression (Loi Godfrain du 5 janvier 1988 et code pénal)

1 Sale temps pour la liberté d'expression sur Internet. Alors qu'après avoir obtenu la « jurisprudence Dieudonné » l'an dernier[1], le gouvernement français vient de consacrer le retour de la censure administrative en droit français avec le décret sur le blocage de sites Internet[2] ; alors que le passage du délit d'apologie du terrorisme dans le code pénal décidé par le Parlement à l'automne se traduit par des dizaines de condamnations totalement disproportionnées à des peines de prison ferme[3] ; alors que le secret des affaires reste à l'agenda européen[4] tandis que la protection des sources piétine au niveau national, une nouvelle menace se fait jour : le dévoiement de la loi Godfrain du 5 janvier 1988 relative à la fraude informatique.

2 Plusieurs évolutions récentes, dont un arrêt de la Cour de cassation rendu le 20 mai dernier, montrent en effet que cette loi, depuis intégrée aux articles 323-1 à 323-7 du code pénal, pourrait bien devenir le nouvel ami des censeurs. Adoptée à une époque où le développement de la mouvance hacker suscitait déjà une véritable panique du côté des États, elle est conçue à l'origine pour réprimer les actes de fraude informatique. À l'instar d'autres pays, la France inscrivait alors dans son droit des dispositions permettant de réprimer les usages frauduleux des systèmes informatiques (accès frauduleux, maintien frauduleux), les atteintes qui leur sont portées (entrave et faussement du fonctionnement du système), ainsi que les atteintes aux données qu'ils contiennent (introduction, modification, suppressions frauduleuses de données).

3 La loi Godfrain a donné lieu à d'importantes controverses du fait de son application à des actes quotidiens et nécessaires à la recherche en sécurité informatique.[5] Désormais, elle est également directement mobilisée pour restreindre des expressions de nature politique.

1°/- Trois affaires emblématiques d'une dérive

4 Trois affaires récentes permettent d'illustrer cette dérive.

A - Affaire Bluetouff : du délit de maintien dans l'espace public à des fins journalistiques

5 La première affaire concerne le hacker et journaliste Bluetouff, spécialiste de sécurité informatique et cofondateur du site reflets.info. À l'été 2012, il enquête sur le régime syrien. Au détour d'une recherche sur Google, il découvre des documents confidentiels diffusés sur le réseau privé de l'Agence nationale de sécurité sanitaire, de l'alimentation, de l'environnement et du travail (Anses). Celle-ci dispose en effet d'un extranet qui permet à ses experts d'échanger des documents. Mais il est mal sécurisé, et les fichiers qui s'y trouvent sont librement accessibles. Bluetouff télécharge alors une archive de 7,7 gigaoctets. Il décide ensuite d'utiliser quelques fichiers pour écrire avec un de ses collègues de reflets.info un article sur les « *cas de légionellose à proximité des centrales nucléaires* », en illustrant l'article d'extraits d'un fichier « Powerpoint ».

6 L'Anses prend alors conscience alors de la faille informatique, et que le contrôle d'accès fondé sur un identifiant et un mot de passe est défaillant. L'agence saisit la police, et l'enquête est confiée à la Direction générale du renseignement intérieur (l'ex-DCRI). Olivier Laurelli est aisément identifié et détenu trente heures durant en garde à vue. Poursuivi pour « *accès frauduleux dans un système de traitement automatisé de données* » et « *vol de documents* », il encourt jusqu'à trois ans de prison et 45 000 euros d'amende.

7 En avril 2013, le Tribunal correctionnel de Créteil le relaxe, estimant que la responsabilité de la fuite incombait à l'Anses puisqu'elle avait manifestement mal sécurisé son réseau. Pourtant, le Parquet fait appel et les juges de la Cour d'appel de Paris décident dans un arrêt du 5 février 2014 de le condamner à 3 000 euros d'amende. Les juges renversent la jurisprudence Kitetoa –

qui depuis 2002 mettait à la charge du responsable de traitement une obligation de sécurisation minimale de son site[6]– en invoquant le fait que Bluetouff avait reconnu lors de sa garde à vue avoir constaté la présence d'une procédure d'authentification sur le site. Le procureur avait ainsi plaidé la mauvaise foi du prévenu, déclarant à l'adresse de ce dernier : « *vous saviez que cet extranet était normalement protégé* »[7]. Au cours des débats, les magistrats feront preuve d'une grande méconnaissance des réalités techniques de l'Internet : en ouverture d'audience, la juge chargée de rappeler les faits semble ne même pas connaître Google, qu'elle prononce à la française (« gogleu »). Un de ses collègues demande au prévenu : « *Mais il faut tout de même taper des mot-clés (…) ? Comment faites-vous pour arriver sur des questions de santé publique alors que vous cherchiez des choses sur la Syrie* ? »[8] .

8 Saisie, la Cour de cassation a décidé le 20 mai 2015 de rejeter le pourvoi du journaliste[9]. Bluetouff a donc été condamné pour s'être maintenu dans un espace numérique *de facto* public, et pour avoir exploité à des fins journalistiques les documents qui s'y trouvaient – documents qui étaient par ailleurs librement accessibles par d'autres biais que cet extranet mal sécurisé. Dans leur décision, les juges ne prêtent aucune attention à la liberté d'expression et au droit à l'information pour sous-peser les conclusions de la Cour d'appel.

B - L'affaire Rachida Dati : l'exploitation d'une faille de sécurité à des fins parodiques n'est pas du goût des juges

9 La deuxième affaire pose la question du droit de parodie. Début 2012, l'eurodéputée Rachida Dati porte plainte contre un informaticien et son hébergeur pour « *intrusion frauduleuse de données dans un système de traitement automatisé* » et « *usurpation d'identité numérique* ». Leur faute ? Avoir respectivement édité et hébergé le site Tweetpop.fr, qui parodiait le site officiel de l'élue pour permettre aux internautes de rédiger de faux communiqués de presse. N'importe qui pouvait ainsi proposer un texte destiné à être injecté sur le site officiel de Rachida Dati. À travers une banale faille de sécurité dite XSS, il était en effet possible d'afficher sur ce dernier n'importe quel texte inséré dans l'URL. Les communiqués parodiques ainsi générés par les utilisateurs incluaient par exemple une mention « groupe PIPE » au lieu du groupe politique de l'eurodéputée au Parlement européen, le groupe PPE, en référence à un malencontreux lapsus de l'ancienne Garde des sceaux. Tweetpop proposait aussi des fonctionnalités permettant de partager les communiqués parodiques sur Twitter ou Facebook.

10 La plaisanterie n'a pas été du goût des juges. Dans son jugement du 18 décembre 2014[10], le Tribunal correctionnel de Paris a en effet condamné les défendeurs. D'abord, en estimant qu'il y avait eu intrusion informatique : en exploitant la faille de sécurité XSS pour modifier le fonctionnement du site, l'informaticien aurait en effet cherché à introduire frauduleusement des données sur le site. Le tribunal n'a pas voulu tenir compte du fait que la page détournée n'apparaissait que pour l'internaute ayant généré le communiqué ou pour les personnes avec lesquelles il partageait l'adresse URL détournée, et qu'en aucun cas le site ou le serveur n'avait fait l'objet d'une intrusion forcée ou d'une modification. Les juges écartent également le moyen de défense tiré du fait que la faille de sécurité en question était connue et identifiée depuis plusieurs mois par le gestionnaire. Comme dans l'affaire Bluetouff, le tribunal estime que la négligence de la victime ne pouvait exonérer l'auteur du fait délictueux.

11 En second lieu, les juges ont estimé que l'infraction d'usurpation d'identité numérique est elle-aussi caractérisée, appliquant pour la première fois cette infraction créée en 2011 avec l'adoption de la loi LOPPSI[11]. Pour ce faire, ils procèdent dans le jugement à l'analyse des textes présents sur Tweetpop.fr : « *Ces mentions ["je vous offre un communiqué... " ou "merci pour ce geste citoyen"], aux côtés du nom de Madame Rachida Dati et sur un site reprenant la photographie officielle de la député-maire, sa mise en page et sa charte graphique, ne peut que conduire l'internaute à opérer une confusion avec le site officiel de celle-ci* ». L'éditeur du site aurait ainsi contrevenu à l'article 226-4-1 du code pénal, qui réprime l'« *usage d'une ou plusieurs données de toute nature permettant de l'identifier en vue de troubler sa tranquillité ou celle d'autrui, ou de porter atteinte à son honneur ou à sa considération* ». L'intention délictueuse est caractérisée selon les juges par le fait que le prévenu ait cherché à faire connaître son site parodique en le diffusant sur Twitter, conduisant à certain retentissement médiatique

de son initiative. Ils soulignent en outre le caractère « *particulièrement injurieux et diffamant* », voire « *obscènes* » de certains des faux communiqués rédigés par les internautes et l'absence de modération, rendant ainsi l'éditeur du site et son ami hébergeur coupables des propos tenus par d'autres.

12 À l'audience, le président du tribunal se fera gardien de la morale et du bon goût, dénonçant « *l'humour stupide* » des internautes : « *Vous dites que c'est de l'humour, mais ça ne fait rire personne ! La France en est-elle à ce niveau ? La France vaut mieux que ça* ! »[12]. Et la procureur de renchérir : « *Vous dites que cet humour ne fait rire personne, monsieur le président, eh bien sur Internet si, malheureusement. Chacun fait ce qu'il veut en matière d'action politique. Mais quand l'humour potache devient infraction, c'est non* »[13]. L'auteur de Tweetpop.fr a depuis fait appel.

C - L'affaire Greenrights : manifestation pacifique ou cyber-terrorisme ?

13 La troisième affaire concerne la mouvance « hacktiviste » Anonymous. En mars 2011, suite à l'accident nucléaire de Fukushima, des collectifs « Anons » souhaitent exprimer leur indignation face à l'industrie nucléaire. Pour ce faire, ils vont recourir à mode d'action politique qui revient sur le devant de la scène depuis quelques mois : les attaques distribuées par déni de service (DDoS, selon l'acronyme anglais). Une action de DDoS consiste à inonder un serveur web de requêtes afin de le rendre temporairement inaccessible.

14 Traditionnellement employés par des cybercriminels à des fins d'extorsion ou par des États pour se livrer à des opérations de censure extra-légale, les DDoS font aussi parti du répertoire d'action hacktiviste depuis la fin des années 1990, lorsque leur utilisation dans le cadre de mobilisations citoyennes est théorisée par des groupes militants comme les electrohippies[14]. À partir de septembre 2010, Anonymous semble la redécouvrir : des DDoS sont alors lancés contre les sites des majors hollywoodienne et de certaines entreprises qu'elles emploient, pour protester contre les DDoS commandités par des groupes des industries culturelles contre The Pirate Bay et pour protester contre les poursuites pénales en masses intentées contre des internautes. Quelques semaines plus tard, ce sont Amazon, PayPal et d'autres sites d'entreprises ayant cédé aux pressions du gouvernement américain pour censurer WikiLeaks qui sont visés en décembre 2010. Richard Stallman, fondateur du mouvement du logiciel libre, défend alors ces actions comme l'équivalent numérique de *sit-ins* et autres manifestations dans l'espace public[15].

15 En mars 2011, Anonymous délaisse donc pour un temps le champ de l'activisme numérique et se mobilise pour la cause environnementale. Le 25, soit deux semaines après la catastrophe nucléaire de Fukushima, des Anonymous annoncent dans une vidéo le début de l'opération Greenrights. C'est d'abord les sites de BP et de Shell qui sont visés par la mouvance. Puis des hacktivistes italiens – échaudés par un câble diplomatique américain révélé par WikiLeaks faisant état des pressions exercées par EDF sur le gouvernement italien pour que ce dernier passe outre le rejet du nucléaire décidé en 2011 par referendum – proposent de prendre pour cible l'entreprise française. EDF porte alors plainte contre X. L'entreprise dit avoir vu son site bloqué pendant treize heures, et avoir subi un préjudice s'élevant à 162.000 euros du fait de l'impossibilité pour ses clients de faire leurs démarches en ligne, ce qui aurait également conduit à la saturation du standard téléphonique. Comme dans l'affaire Bluetouff, l'enquête est confiée à l'actuelle DGSI, sous l'autorité du Parquet de Paris.

16 Après huit mois d'enquête, la DGSI procède en janvier 2012 à trois arrestations. Parmi eux, Pierrick Goujon, alias Triskel, 29 ans à l'époque, qui gère un site fournissant des liens passerelles vers des salons de discussion IRC, et dont l'adresse URL s'était retrouvée sur un tract Anonymous consacré à l'opération Greenrights. Son adresse IP a également été relevée sur les serveurs d'EDF au moment du DDoS. Il est arrêté au domicile de sa petite-amie en Bretagne. Selon son avocat, maître Joseph Breham, 80 gendarmes sont alors mobilisés, en plus des 16 agents de la DGSI. Un deuxième individu, connu sous le pseudonyme de Kloud, suspecté d'avoir publié sur YouTube une vidéo appelant à rejoindre l'opération Greenrights, est également interpellé à son domicile près de Montpellier.

17 Tous deux seront conduits dans les locaux parisiens de la DGSI et détenus près de 45 heures en garde à vue. Présentés au juge David Benichou du Tribunal de grande instance de Paris, ils sont mis en examen pour avoir « *participé à la campagne Greenrights, entente formée en vue de conduire des entraves par déni de service contre des producteurs/distributeurs d'électricité* ». Les DDoS sont évidemment réprimés par la loi Godfrain.

18 Quelles ont été les suites ? S'agissant de Kloud, on sait que l'instruction a été close en décembre 2013 et le dossier transféré Procureur de la République. Une rapide recherche en ligne ne permet pas de trouver de nouvelles plus récentes de la procédure qui le concerne, en dehors d'un témoignage publié au printemps 2014 dans lequel il livre sa version des faits. À propos du préjudice estimé par EDF, il indique que « *l'attaque était prévue pour ne pas endommager le serveur, pour que le site fonctionne de nouveau normalement à la fin du DDoS. Donc, il n'y a eu aucunes détériorations, pas de piratage, pas d'intrusions d'infrastructures ou autres, pas de divulgations de données sensibles. De plus, comme pour une grève, nous avions fait une vidéo pour prévenir EDF de la date et de l'heure de l'attaque* ». Il rejette les accusations portées contre lui, pointant le caractère politique et légitime de l'action de DDoS : « *Ce n'est en rien une entente en vue de commettre une infraction ou une manifestation dans le but de faire passer des idées n'a rien d'illégale* ». Et pourtant, sa libération conditionnelle s'accompagne de conditions particulièrement sévères : il lui est interdit de sortir du territoire, de fréquenter les salons de discussion IRC ou tout autre moyen de communication lié à Anonymous sous peine d'emprisonnement. Il voit également son nom inscrit au très controversé fichier Gaspard.

19 Quant à Pierrick Goujon, il est relaxé en première instance en novembre 2014[16]. Sa défense convainc alors les juges, qui comprennent qu'il ne faisait qu'offrir un service d'intermédiation technique vers les salons IRC d'Anonymous, sans jouer aucun rôle dans la mouvance. Pourtant, lors de l'audience, relatée par le site Next INpact, la procureure insiste et tente de présenter IRC – l'un des plus anciens protocoles de messagerie en ligne – comme un outil destiné à l'action politique clandestine : « *On sait tous qu'IRC est très majoritairement utilisé pour définir des dates et des cibles. Dans ce dossier, c'est très clairement passé par ces canaux qui sont très peu faciles d'accès par le néophyte* » ; IRC « *a été très très majoritairement utilisé par les membres de la nébuleuse anonymous* » ; « *IRC s'avère être un vecteur crucial pour permettre l'attaque informatique dont il est ici question* » (…) ». Face à quoi Triskel continue d'appeler au bon sens (« *mais IRC permet juste de discuter* ! »)[17]. Rien n'y fait, et le Parquet fera appel de la relaxe fin décembre 2014. L'avocat de Pierrick Goujon y voit alors « *un acharnement pour tenter de justifier les moyens colossaux et disproportionnés mis en œuvre, ces nombreux policiers, des brigades spécialisées, (...)* »[18].

2°/- Des ingérences disproportionnées dans la liberté d'expression

20 Quel bilan peut-on tirer de ces trois affaires ?

21 Elles révèlent d'abord que la loi Godfrain peut s'appliquer à trois des fonctions démocratiques essentielles de la liberté d'expression et d'information, à savoir : critiquer ceux qui exercent un mandat public et nous gouvernent, le cas échéant à distance des canons de la bienséance en se livrant à des exercices de carnavalisme politique moquant les puissants, avec des propos qui « *heurtent, choquent ou inquiètent* » selon l'expression consacrée de la Cour européenne des droits de l'Homme (affaire Rachida Dati) ; surveiller le pouvoir et porter à la connaissance du public des informations capables d'éclairer le débat démocratique (affaire Bluetouff) ; protester, exprimer son opposition à une mesure ou des politiques (affaire Greenrights)[19].

22 Or, à chaque fois, les moyens engagés pour poursuivre les personnes concernées et l'acharnement du ministère public témoignent d'une absolue détermination dans la volonté des autorités de lutter contre les formes innovantes que peuvent prendre chacune de ces trois fonctions sur Internet. Le droit de la fraude informatique semble instrumentalisé dans des procès qui paraissent surdéterminés par l'enjeu politique au cœur de chacune de ces affaires. Comme lorsque le Premier ministre, Manuel Valls, invoque « *la force de frappe d'Internet et son influence sur les citoyens* » pour justifier la remise en cause des garanties qu'apporte la loi sur la presse de 1881 à la liberté d'expression et le passage de certains délits de presse

dans le code pénal, il s'agit d'augmenter la capacité coercitive de l'État pour mieux lutter contre la capacité d'expression, d'auto-organisation, de mobilisation qu'Internet offre aux citoyens. La loi Godfrain permet ainsi à la répression d'expressions politiques de s'affranchir des règles protectrices des libertés publiques, ce dont témoigne l'absence quasi-totale de prise en compte des implications et exigences de la liberté d'expression et de manifestation par les magistrats dans ces affaires.

23 À cette explication politique de la sévérité de la réponse des autorités s'ajoutent des aspects proprement juridiques, qui conduisent à un traitement disproportionné lorsqu'ils sont appliqués à ces formes de participation politique. C'est le cas par exemple des spécificités procédurales du droit de la fraude informatique, et en particulier le rôle joué par les services de renseignement[20]. La DGSI – dont la mission est *« sur l'ensemble du territoire de la République, de rechercher, de centraliser et d'exploiter le renseignement intéressant la sécurité nationale ou les intérêts fondamentaux de la Nati*on »[21] – est compétente pour *« la surveillance des communications électroniques et radioélectrique*s » pour les besoins des multiples missions mentionnées à l'article 2 du décret n° 2014-445[22].

24 À ce titre, elle est compétente pour les investigations relatives à tout acte de criminalité informatique touchant à des systèmes informatiques considérés comme stratégiques. Y compris donc des DDoS, aux conséquences le plus souvent symboliques, conduits à des fins politiques dans le cadre de campagnes citoyennes. D'où la gabegie à laquelle donnent lieu autant l'affaire Bluetouff que l'affaire Greenrights, pour lesquelles la mobilisation d'agents du renseignement apparaît complètement disproportionnée, en particulier à l'heure où certains responsables politiques pointent le manque de moyens consacrés à l'antiterrorisme.

25 Il y a ensuite l'échelle des peines, là encore disproportionnée. Lorsqu'elle est commise contre les systèmes informatiques de l'État, la fraude informatique est sanctionnée de 7 ans d'emprisonnement et 100 000 euros d'amende, soit autant que l'organisation de la traite d'êtres humains (art. 225-4-1 du code pénal), l'homicide involontaire en état d'ivresse manifeste au volant d'un véhicule terrestre à moteur (art. 221-6-1) ou de créer un réseau pédophile et diffuser volontairement des images à caractère pédopornographique sur Internet (art. 227-23)[23]. Un DDoS ou la défiguration d'un site d'une entreprise comme EDF – par exemple pour afficher sur la page d'accueil un placard revendicatif, également typique du répertoire d'action hacktiviste – sont punis bien plus sévèrement que leurs équivalents du monde physique. Ainsi, les tags ou graffitis non-autorisés sur la façade du siège social de l'entreprise auraient été punis au maximum de 3750 € d'amende et d'un travail d'intérêt ou de deux ans d'emprisonnement et 30 000 euros d'amende, selon que les dommages occasionnés soient jugés légers ou importants. Le cyber-vandalisme du site edf.com, annoncé plusieurs jours à l'avance et qui eut pour effet principal de saturer temporairement le standard téléphonique, est quant à lui directement passible de cinq ans d'emprisonnement et de 75 000 euros d'amende.

26 Enfin, un troisième aspect joue un rôle fondamental dans l'application disproportionnée du droit pénal de la criminalité informatique : l'insuffisante maîtrise des questions techniques par nombre de magistrats. Les délits prévus par la loi Godfrain sont légitimement réprimés, de même que l'usurpation d'identité numérique peut répondre à un réel besoin social et juridique. Le législateur, s'en tenant à des dispositions générales, n'a pas prévu tous les cas d'espèce qui justifieraient des exceptions ou des limites à leur application. Le problème est que dans ces affaires, les magistrats ne semblent pas non plus disposés à faire ce travail au plan jurisprudentiel.

27 La méconnaissance des réalités sociales et techniques d'Internet qui affecte certains magistrats tend en effet à renforcer certains de leurs préjugés et peut parfois laisser libre cours à quelques fantasmes de leur part. Elle les conduit à exagérer la nature et la gravité des faits reprochés et à voir dans des activités banales – par exemple le simple fait de participer à un salon de discussion IRC – un savoir-faire qui serait l'apanage d'une élite délinquante au sein du monde hacker. À l'image du juge madrilène qui, en décembre dernier, justifiait l'arrestation préventive de sept militants anarchistes en pointant leurs lectures subversives et le fait « *qu'ils utilisaient des mesures de sécurité extrêmes, telles que l'utilisation d'un serveur RISE UP* » (en fait de « *mesures de sécurité extrêmes* », le service mail de Riseup ne fait qu'appliquer les meilleures

pratiques en matière de confidentialité des communications). L'inculture numérique peut ainsi conduire les juges à une répression disproportionnée en les rendant aveugles à la réalité des faits dont ils doivent juger : l'usage par des citoyens d'outils Internet « grand public » dans un but de participation démocratique.

3°/- Aménager le droit ou aggraver la répression ?

28 Malheureusement, les dérives illustrées par ces trois affaires ne sont que les manifestations d'une tendance plus générale. Dès l'apparition du répertoire d'action hacktiviste dans les années 1990, la tentation des États était grande de considérer ces formes d'action politique comme relevant du « *cyber-terrorisme* »[24]. Aujourd'hui, cette perspective se confirme, dans un contexte où s'accumulent les mesures répressives visant à réguler Internet.

29 En janvier 2013, alors qu'Europol inaugurait son nouveau centre dédié à la lutte contre la cybercriminalité, le European Cybercrime Center, son directeur fraîchement nommé citait parmi les priorités du centre la lutte contre le « *cyberactivisme* » aux côtés des attaques informatiques étatiques et des activités terroristes. Dans les discours des décideurs, l'hacktivisme apparaît ainsi souvent comme une catégorie fourre-tout, mêlant toutes formes de criminalité informatique conduite à des fins politiques. Les actes de protestation comme les DDoS sont mis au même plan que les « *cyberattaques* » menées par des acteurs étatiques, ce qui conduit à l'activation des procédures et de sanctions d'exception (outre le rôle de la DGSI en France, voir les DDoS menés par le GCHQ britannique contre les serveurs IRC d'Anonymous, ou la condamnation par la justice de sa Majesté d'un jeune membre de la mouvance à 18 mois de prison ferme pour avoir hébergé les discussions IRC ayant permis l'organisation d'un DDoS contre Paypal en 2010).

30 Et pourtant, en 2011, quelques semaines après la révélation d'un rapport de l'OTAN consacré aux Anonymous, Jessica Vielhuber, membre du Conseil du renseignement national à la Maison Blanche, estimait lors d'une réunion avec ses partenaires de l'Alliance atlantique sur les « cyber-menaces » que la mouvance ne représentait pas une menace sérieuse. Dans un mémo préparé pour l'occasion, elle écrivait que « *bien que les groupes "hacktivistes" comme Anonymous aient fait récemment les gros titres en volant des informations de l'OTAN, la menace que représentent de telles activités est minime en comparaison de celle des États-nations* ». Un sens des proportions qui tranche avec nombre des discours publics sur la question. En fait, l'exagération de la menace semble avant tout destinée à justifier un traitement uniquement répressif de l'hacktivisme, et ce afin de l'exclure des formes de participation politique réputées légitimes.

31 La tendance législative est donc à l'aggravation de la répression. Aux États-Unis, après le vol de données retentissant dont fut victime le studio Sony en décembre dernier, Barack Obama a annoncé une réforme du Computer Fraud and Abuse Act[25]. Cette dernière risque d'aggraver les peines encourues tout en étendant le champ des infractions, ce qui pourrait avoir des conséquences désastreuses pour les journalistes[26].

32 En France, l'article 17 de la loi de novembre 2014 sur la lutte contre le terrorisme accentue également la portée répressive de la loi Godfrain. Les infractions prévues par cette dernière sont désormais susceptibles d'être reconnues comme étant commises « *en bande organisée* ». Cette réforme permet aux enquêteurs de mobiliser l'ensemble des procédures et moyens d'enquêtes propres à la lutte contre la criminalité organisée, et aux juges de prononcer des sanctions encore plus sévères. Même si peu après l'adoption du texte, des hackers liés à la mouvance djihadiste ont également perpétré des attaques DDoS contre de nombreux sites français au lendemain des attentats de janvier[27], les seuls actes récents susceptibles d'entrer dans le champ d'une telle disposition au moment de son adoption étaient les DDoS conduits par Anonymous dans l'opération Greenrights. Et de fait, en avril 2015, le Parquet a retenu la circonstance aggravante de faits commis « *en bande organisée* » contre deux militants se revendiquant de l'étiquette Anonymous. Ces derniers sont soupçonnés d'avoir pris part à des DDOS contre des sites institutionnels – ceux du conseil régional de Lorraine et de l'Agence nationale de gestion des déchets radioactifs – dans le cadre d'une campagne contre l'enfouissement des déchets nucléaires.[28] Ils encourent dix ans d'emprisonnement et 150 000 €

d'amende, et seront jugés le 9 juin par le tribunal correctionnel de Nancy. Enfin, dans le cadre de l'examen parlementaire du projet de loi sur le renseignement, le député Jean-Jacques Urvoas a argué de la récente cyberattaque contre TV5 pour défendre avec succès un amendement qui aggrave significativement les peines prévues par la loi Godfrain[29] (ce « cavalier législatif » est toutefois remis en cause au Sénat).

*

* *

33 Les affaires Rachida Dati et Greenrights sont encore en cours. Bluetouff et son avocat étudient quant à eux la possibilité de saisir le Cour européenne des droits de l'Homme. Les décisions à venir permettront peut être de ramener un peu de bon sens dans la jurisprudence afférente à la fraude informatique, et d'aménager dans le droit des espaces autorisant ces pratiques politiques tout en les encadrant. Pourquoi ne pas, par exemple, reconnaître la possibilité d'organiser sous certaines conditions des manifestations collectives dans l'espace numérique sous la forme de DDoS ? En 2006, une cour d'appel régionale allemande avait rendu une décision allant dans ce sens, dans une affaire où une action DDoS avait été orchestrée par des militants contre la compagnie aérienne Lufthansa dans le but de dénoncer sa participation à la déportation des sans-papiers. La jurisprudence Kitetoa, remise en cause dans l'affaire Bluetouff, amorçait quant à elle une évolution jurisprudentielle utile en proposant d'exonérer une personne mise en cause pour fraude informatique si le responsable du système informatique visé n'avait fait preuve d'aucune diligence en matière de sécurité. Enfin, et plus largement, il faudrait remédier au constat dressé en 2012 par la magistrate spécialiste de la cybercriminalité, Myriam Quéméner, qui dans une audition au Sénat avait regretté le *« manque de culture numérique »* de nombre de ses collègues[30].

34 Face au risque d'une nouvelle dérive répressive, des solutions doivent en tout cas être trouvées et il est urgent d'en débattre. Car si jusqu'à présent, le droit pénal de la criminalité informatique semblait éloigné de l'espace public et de la liberté d'expression – au delà en tout cas des questions touchant directement à la sécurité informatique –, il s'y trouve désormais largement mêlé. Les évolutions législatives et jurisprudentielles qui l'affectent constituent à ce titre un véritable enjeu démocratique

*

35 **Cass. crim., 20 mai 2015, no 1566 (Affaire Bluetouff)**
36 **Tribunal correctionnel de Paris, 18 décembre 2014 (Affaire Rachida Dati)**
37 **Tribunal correctionnel de Paris, 11 décembre 2014 (Affaire Greenrights)**

*

Notes

1 Conseil d'État, Ministère de l'Intérieur c/ Société Les productions de la Plume et M. Dieudonné M'Bala M'Bala, ordonnance du 9 janvier 2014.

2 Décret n° 2015-125 du 5 février 2015 relatif au blocage des sites provoquant à des actes de terrorisme ou en faisant l'apologie et des sites diffusant des images et représentations de mineurs à caractère pornographique.

3 Pascale Robert-Diard, « Des peines très sévères pour apologie du terrorisme », *Le Monde*, 19 janvier 2015.

4 Proposition de directive sur la protection des savoir-faire et des informations commerciales non divulgués (secrets d'affaires) contre l'obtention, l'utilisation et la divulgation illicites.

5 Damien Leloup, « Un journaliste condamné pour avoir signalé une faille de sécurité informatique » *Le Monde.fr*, 23 septembre 2009.

6 Cour d'appel de Paris, *Kitetoa c. Tati*, arrêt du 30 octobre 2002.

7 Jérôme Hourdeaux, « « Piratage » via Google : drôle de procès en appel pour un journaliste », *Mediapart*, 20 décembre 2013.

8 Idem.

9 Cass. crim., 20 mai 2015. no 1566.

10 Tribunal correctionnel de Paris, 18 décembre 2014.

11 Loi n° 2011-267 du 14 mars 2011 d'orientation et de programmation pour la performance de la sécurité intérieure**.**

12 Martin Untersinger, « Le « piratage » inédit du site de Rachida Dati au tribunal », *Le Monde.fr*, 17 novembre 2014.

13 Idem.

14 Electrohippies collective, « Client-Side Distributed Denial-of-Service: Valid Campaign Tactic or Terrorist Act? », *Electrohippies Occasional Paper* n° 1, 2000.

15 Richard Stallman, « The Anonymous WikiLeaks protests are a mass demo against control », *The Guardian*. 17 décembre 2010.

16 Tribunal correctionnel de Paris, 11 décembre 2014.

17 Marc Rees, « Opération GreenRights : le Parquet fait appel contre Triskel, l'éditeur d'irc.lc », *NEXT INpact*, 22 janvier 2015.

18 Idem.

19 Sur la liberté de critique politique, v. not. Cour EDH, 5e Sect. 14 mars 2013, *Eon c. France*, Req. n ° 26118/10 - ADL du 20 mars 2013.

20 Stéphane Tijardovic, « Le rôle de la DCRI en matière de cybersécurité », *Défense*, octobre 2010, n° 47.

21 Article 1er du décret n° 2014-445 du 30 avril 2014 relatif aux missions et à l'organisation de la direction générale de la sécurité intérieure.

22 Article 2 du décret n° 2014-445 du 30 avril 2014.

23 Thiébaut Devergranne, « Du plomb dans la loi Godfrain », *Données personnelles*, 26 mai 2012.

24 Mark Manion et Abby Goodrum. Terrorism or Civil Disobedience: Toward a Hacktivist Ethic. *SIGCAS Computer & Society*. juin 2000. vol. 30, p. 14–19.

25 Computer Fraud and Abuse Act, 1986, 18 U.S.C. § 1030.

26 Trevor Timm, « Barrett Brown's sentence is unjust, but it may become the norm for journalists ». *Boing Boing*, 26 janvier 2015.

27 Alain Ruello, « Vague de cyberattaques sans précédent en France », *Les Échos*, 15 janvier 2015.

28 AFP, « Deux Anonymous jugés pour des attaques contre des sites institutionnels », 10 avril 2015.

29 Voir aussi l'échelle des peines retenue dans la directive 2013/40/UE du 12 août 2013 relative aux attaques contre les systèmes d'information.

30 David Assouline, « Le contrôle et l'évaluation des dispositifs législatifs relatifs à la sécurité intérieure et à la lutte contre le terrorisme », compte rendu de l'état des travaux de la commission sénatoriale pour le contrôle de l'application des lois, Sénat, 2012, p. 28.

Pour citer cet article

Référence électronique

Félix Tréguer, « Le droit pénal de la fraude informatique, nouvel ami des censeurs ? », *La Revue des droits de l'homme* [En ligne], Actualités Droits-Libertés, mis en ligne le 02 juin 2015, consulté le 20 juillet 2015. URL : http://revdh.revues.org/1328

À propos de l'auteur

Félix Tréguer
Doctorant à l'EHESS et membre fondateur de l'association La Quadrature du Net

---

Résumé

Plusieurs décisions de justice rendues ces derniers mois en France – dont une décision de rejet de la Cour de cassation en date du 20 mai 2015 – s'appuient sur le droit de la criminalité informatique pour limiter les formes innovantes d'expression politique qui se déploient sur Internet. Or, ce mouvement jurisprudentiel qui s'inscrit dans un contexte d'abaissement tendanciel des garanties entourant la liberté d'expression risque encore de s'aggraver compte tenu des récentes évolutions législatives dans le domaine de la cybercriminalité. Face à ces dérives, il est urgent de trouver des mécanismes permettant une conciliation équilibrée entre les différents intérêts en présence afin d'assurer une protection efficace de la liberté d'expression dans l'espace public numérique.