Qualifier le téléchargement illégal de données : soustraire ou extraire, telle est la question

Tristan Berger

QUALIFIER LE TÉLÉCHARGEMENT ILLÉGAL DE DONNÉES : SOUSTRAIRE OU EXTRAIRE, TELLE EST LA QUESTION

Résumé : Dans un arrêt du 20 mai 2015, la Chambre criminelle de la Cour de cassation a considéré que le téléchargement frauduleux d'un document pouvait constituer un vol. Cette position, fort discutable d'un point de vue juridique, correspond néanmoins à la logique de la loi du 13 novembre 2014 sur le terrorisme – postérieure aux faits du dossier et donc inapplicable en l'espèce – qui pénalise notamment l'extraction frauduleuse de données dans un système de traitement automatisé. Occultant les questions de la liberté d'accès à l'information et du statut des lanceurs d'alerte, cet arrêt reflète une dynamique répressive aux conséquences inquiétantes.

Retour sur les faits : du simple blogueur au terrifiant « *hacker* »

Qualifié de « *pirate* », de « *hacker* » ou encore de « *quatrième cavalier de l'apocalypse* », le blogueur[1] Olivier Laurelli – alias « *Bluetouff* » – a défrayé la chronique. L'activité du blogueur « *Bluetouff* » consiste essentiellement à écrire des billets d'opinion – sur des sujets tels que l'affaire Snowden, l'accord commercial anti-contrefaçon[2] ou encore la loi Hadopi[3] – qu'il publie ensuite sur son blog (Bluetouff.com[4]). Afin d'enrichir et de préciser ses écrits, il effectue des recherches d'informations poussées sur internet, démarche plus proche du journalisme d'investigation que du « *hacking* ». Le « *hacking* » consiste à tester « *les systèmes d'information pour découvrir les vulnérabilités* » de manière licite ou illicite, dans un intérêt privé ou collectif[5] ; un hacker n'est donc pas systématiquement un pirate ou un cybercriminel. En dehors de son activité de blogueur, Olivier Laurelli est « *imprégné* » de la culture du « *hacking* »[6] mais ne présentait aucun lien avec la cybercriminalité avant cette condamnation.

[1] Un « *blogueur* » est entendu ici comme l'auteur d'un « *blog* », site Web personnel sur lequel il note, comme dans un journal, ses réflexions, analyses et impressions à l'aide d'articles ou de billets d'opinion sur des sujets sur lesquels il a une expertise et/ou une passion en vue de les diffuser et de susciter des réactions.
[2] Accord Commercial Anti-Contrefaçon signé le 26 janvier 2012.
[3] Loi n°2009-669 du 12 juin 2009 favorisant la diffusion et la protection de la création sur internet.
[4] URL : <http://bluetouff.com/>. Consulté le 14 juin 2015.
[5] ACISSI. *Sécurité informatique. Ethical Hacking. Apprendre l'attaque pour mieux se défendre*. France : ENI, 2009, p.15 et s.
[6] J.-M. Manach. « @Bluetouff : A force d'agresser leur environnement, les hackers sont entrés en politique ». *Le vinvinteur,* 45 mn. URL : <https://www.youtube.com/watch?v=6qDe35bBfrU>. Consulté le 14 juin 2015.

Dans cette affaire, le blogueur a fortuitement accédé à un répertoire de 7,7 Go[7] de documents scientifiques, visiblement relatifs à la santé publique, au cours d'une recherche d'informations sur Google – via l'adresse web[8] <https://extranet.anses.fr/Docs>. Ce répertoire était situé sur l'extranet de Agence nationale de sécurité sanitaire, de l'alimentation, de l'environnement et du travail[9]. En théorie, ce site était censé être protégé et inaccessible au public, néanmoins il était libre d'accès *de facto* car l'ANSES ne l'avait pas protégé comme elle l'aurait du. Après avoir constaté l'existence d'un portail d'authentification – <https://extranet.anses.fr/> – le blogueur s'est maintenu sur le site et a téléchargé les documents qu'il a fixés sur différents supports. Il a ensuite utilisé une partie des documents ainsi téléchargés pour co-rédiger un article sur « *les cas de légionellose à proximité des centrales nucléaires* » publié sur le blog reflet.info[10]. Cet article était illustré à l'aide d'extraits d'un PowerPoint et complété par des données brutes téléchargés sur l'extranet de l'ANSES. Suite à une plainte de l'ANSES, le blogueur fût poursuivi en justice ; l'ANSES s'est constituée partie civile. L'auteur des faits a été relaxé devant le Tribunal correctionnel de Créteil ; le parquet a ensuite fait appel (mais pas l'ANSES qui a reconnu une faille dans son système entre-temps). La Cour d'appel de Paris a condamné le prévenu à 3000 euros d'amende pour maintien frauduleux dans un système de traitement automatisé de données et vol ; ce dernier a ensuite formé un pourvoi de cassation[11].

Devant la Cour : le téléchargement, c'est le vol...

Selon le requérant, le fait d'utiliser un logiciel public pour pénétrer dans un système non protégé – sans mise en garde spéciale du maître du système – et de s'y maintenir, et ce bien qu'il y ait un contrôle d'accès sur la page d'accueil, ne peut

[7] Les « *giga-octets* » ou « *Go* » sont une unité de mesure en informatique indiquant la capacité de mémorisation des mémoires informatiques. Les 7,7 Go téléchargés représentaient en l'occurrence approximativement 8000 documents.
[8] Ou plus l'exactement le « *Uniform Resource Locator* », ou « *URL* ».
[9] Ci-après « *ANSES* ».
[10] Extrait : « [...] *Cette publication, un peu particulière, a pour but d'offrir tous les éléments d'évaluation aux personnes compétentes afin que ces dernières se fassent une idée précise de l'efficacité des mesures prises par les pouvoir publiques sur cette question de santé* [...] ». *Reflet.info*, « Cas de légionellose à proximité des centrales nucléaires », 29 août 2012. *Article retiré*. URL (texte partiel) : <http://seenthis.net/messages/84150>. Consulté le 14 juin 2015.
[11] Le coût du pourvoi en cassation était estimé par le blogueur à 10 000 euros. N'étant pas en mesure de supporter ce coût, il a effectué un appel à financement avec un projet Kiss Kiss Bank Bank. 10 233 euros de don ont ainsi été réunis en un peu plus de deux jours. Source : <https://reflets.info/merci/>. Consulté le 14 juin 2015.

constituer un maintien frauduleux dans un système automatisé de données. De plus, le téléchargement de fichiers informatiques accessibles non protégés – et sans soustraction frauduleuse – ne saurait constituer un vol. Ainsi, deux problèmes de droit sont soulevés ici. D'une part, la question se pose de savoir si le fait de se maintenir dans un système de traitement automatisé après avoir découvert que celui-ci aurait dû être protégé constitue un maintien frauduleux au sens de l'article 323-1 du Code pénal. D'autre part, il s'agit de savoir si le téléchargement de données sur le site d'un établissement public administratif, sans le consentement de l'établissement, constitue une soustraction de la chose d'autrui au sens de l'article 311-1 du Code pénal. La Chambre criminelle a finalement tranché à l'encontre du blogueur : le fait de découvrir qu'un système de traitement automatisé est protégé et de s'y maintenir constitue un maintien frauduleux dans un système automatisé de données. De plus, le fait d'extraire des données puis de les utiliser sans le consentement de leur propriétaire est constitutif de vol. Aussi, la Cour de cassation a-t-elle rejeté le pourvoi.

La question du maintien frauduleux : une simple interprétation des faits

S'agissant du maintien frauduleux, l'interprétation est casuistique. La difficulté résidait dans la qualification juridique de l'élément moral : le blogueur avait-il conscience de l'irrégularité de son acte ? La Cour de cassation – qui, comme chacun le sait, juge en droit et non en fait – s'en est tenue à l'interprétation des faits par la Cour d'appel : le blogueur s'est maintenu sur le site extranet après avoir « *parcouru l'arborescence des répertoires et être remonté jusqu'à la page d'accueil* » où il a « *constaté la présence de contrôle d'accès et la nécessité d'une authentification par identifiant et mot de passe* ». La Cour de cassation a ainsi retenu qu'il « *s'est maintenu dans un système de traitement automatisé après avoir découvert que celui-ci était protégé* », ce qui, en ces termes, caractérise une forme de conscience, de la part du blogueur, de l'irrégularité de son acte. On ne peut jusqu'ici qu'adhérer au propos. En revanche, la cohérence juridique s'estompe concernant le second motif avancé, plus farfelu d'un point de vue juridique.

La question du vol de données : une qualification juridique intrigante

S'agissant du téléchargement de données, la qualification de vol est intrigante à double titre. D'une part la qualification de vol a été admise bien qu'il n'y ait pas eu de soustraction *stricto sensu*. D'autre part, la Cour a considéré l'ANSES comme étant propriétaire des données en cause sans s'intéresser au caractère public ou privé de celles-ci. Cette décision a fait couler de l'encre, et suscité pléthore de jugements de valeurs ; il s'agit cependant ici de l'analyser juridiquement et ce sous deux angles : celui de la soustraction interprétée de façon fort extensive (I), puis celui du caractère potentiellement public des données en causes, aspect totalement occulté par la Cour de cassation (II).

I. LE CHOIX D'UNE INTERPRÉTATION FORT EXTENSIVE DE LA « *SOUSTRACTION* »

Aux termes de l'article 311-1 du Code pénal, « *le vol est la soustraction frauduleuse de la chose d'autrui* ». Pour soustraire, il faut prendre, enlever, ravir[12]. En ce sens, le *Vocabulaire juridique* défini la soustraction comme étant une « *action en général subreptice et frauduleuse de retirer d'un ensemble tel ou tel élément* », il s'agit de l'« *action de dérober* »[13]. Ainsi, n'est pas constitutif de vol l'agissement consistant à prendre connaissance, par un décodeur frauduleusement fabriqué, des émissions d'une chaîne codée, dans la mesure où le branchement opéré n'a pour effet ni de déposséder le propriétaire qui continue à diffuser, ni de troubler le téléspectateur abonné qui peut suivre la diffusion. Par analogie, dans l'affaire Bluetouff, l'ANSES n'a, à aucun moment, été dépossédée, pas plus que les utilisateurs de l'extranet n'ont subi de quelconque trouble. Le fonctionnement est resté normal en tout point, tant pour le possesseur des données consultées que pour les éventuels utilisateurs. Admettre le vol dans cette hypothèse revient à considérer qu'une écoute téléphonique ou une photographie pourrait potentiellement être qualifié de vol, en raison d'une « *soustraction-extraction* » d'information. Dans cette même logique, le parquet ne devrait-il pas poursuivre Facebook, Google et Amazon pour vols de données ? Pourtant, en dépit de cette incohérence juridique, des analyses

[12] Cass. Crim. 18 nov. 1837 : S. 1838.1.366.
[13] G. Cornu, *Vocabulaire juridique*, 8ème édition mise à jour. Paris : PUF, 2009, p.880.

contradictoires d'une grande partie de la doctrine[14] et du principe de l'interprétation stricte de la loi pénale[15], la Chambre criminelle a délibérément saisi l'opportunité offerte par la Cour d'appel de Paris. Cette dernière, connue pour le maintient de sa position consistant à admettre le vol de données (à propos de logiciels)[16], a contribué à l'ancrage d'une politique jurisprudentielle en construction par la Chambre criminelle[17]. En consacrant cette interprétation du droit, la Cour de cassation a fait un choix politique difficilement soutenable d'un point de vue juridique.

Toutefois, cette question ne devrait pas être amenée à se reposer puisque depuis l'entrée en vigueur de la loi du 13 novembre 2014 renforçant les dispositions relatives à la lutte contre le terrorisme – postérieure aux faits de l'affaire Bluetouff – il est désormais possible de condamner l'extraction, la détention, la reproduction ou la retransmission frauduleuse de données sur un fondement beaucoup plus sévère que celui du vol. En effet, précisément pour offrir un fondement solide à la pénalisation de toute extraction frauduleuse de données – indépendamment de toute forme de soustraction – cette loi a modifié l'article 323-3 du Code pénal qui dispose désormais que « *le fait d'introduire frauduleusement des données dans un système de traitement automatisé, d'extraire, de détenir, de reproduire, de transmettre, de supprimer ou de modifier frauduleusement les données qu'il contient est puni de cinq ans d'emprisonnement et de 75 000 euros d'amende* ». Ainsi, un simple blogueur effectuant un travail d'investigation dans le but affiché d'informer le public – et potentiellement lanceur d'alerte – est désormais susceptible d'être puni plus sévèrement qu'un voleur en tombant sous le coup d'une loi anti-terroriste. Cela semble témoigner d'une « *porosité des différents domaines du droit pénal* »[18] qui est d'autant plus inquiétante que le délit semble être apprécié indifféremment du caractère potentiellement public des données, autrement dit il serait possible d'être pénalement condamné pour avoir téléchargé des données publiques.

[14] Voir par exemple : P. Sargos et M. Masse, « Le Droit pénal spécial né de l'informatique » In *Informatique et Droit Pénal*. Paris : Cujas, 1983, pp.21 et s. ; P. Catala, « Les transformations du droit de l'information » In *Émergence du droit de l'informatique*. Paris : Parques, 1983, p.267 ; P. Corlay, « Réflexions sur les récentes controverses relatives au domaine et à la définition du vol », *J.C.P éd. G.*, 1984, I, n°3160 ?

[15] Article 111-4 du Code pénal.

[16] Voir notamment : CA Paris 13e ch. A, 25 nov. 1992 ; M. Chawky, « Le vol d'informations : quel cadre juridique aujourd'hui ? », *Droit-Tic*, juill. 2006, p.13.

[17] Voir par ex. : Cass. Crim., 27 avril 2011, n°10-86.233.

[18] F. Johannès. « Mirelle Delmas-Marty : la démocratie dans les bras de Big Brother ». *Le Monde*, 4 juin 2015.

II. LE CHOIX D'OCCULTER LA QUESTION DU CARACTÈRE POTENTIELLEMENT PUBLIC DES DONNÉES

Au-delà de la question de la soustraction, la question pourtant essentielle du caractère public ou privé des données a été totalement occultée. En effet, il est probable que ces données détenues par l'ANSES et visiblement relatives à la santé publique – l'arrêt mentionnant leur réutilisation dans un article sur la légionellose[19] – revêtent le caractère de « *document administratif* »[20], « *d'information relative à l'environnement* »[21] ou encore « *d'information publique* »[22]. Dans les deux premiers cas, il s'agirait alors de données en principe librement accessibles. Dans le troisième cas, ces données devraient être librement réutilisables en sus. En l'absence de toute observation de la Cour de cassation à ce sujet, doit-on considérer que les autorités publiques sont « *propriétaires* » (terme employé dans l'arrêt) de toutes les données qu'elles détiennent *de facto* ? Il s'agirait là d'une interprétation manifestement erronée puisqu'une donnée ne peut pas être l'objet d'un droit de propriété[23], seule la structure d'une base de donnée[24], ou la base de donnée elle-même – c'est-à-dire « *un recueil d'œuvres, de données ou d'autres éléments indépendants, disposés de manière systématique ou méthodique et individuellement accessibles par des moyens électroniques ou d'une autre manière* »[25] – peuvent ainsi être protégée. Les autorités sont simples détentrices de ces données.

Quand bien même le blogueur aurait téléchargé des bases de données dont l'ANSES – ou tout autre organisme public ou privé – serait propriétaire, qu'en est-il pour celles qui constitueraient des « *documents administratif* » dont la liberté d'accès est consacrée par la loi du 17 juillet 1978 ? Et pour celles qui seraient relatives à la santé

[19] La légionellose est une infection respiratoire grave due à l'inhalation d'un aérosol d'eau contaminée par la bactérie Legionella

[20] Titre 1 de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

[21] Le mot « *environnement* » incluant ici toutes les informations relative à « *l'état de la santé humaine* » et à « *la sécurité* » conformément à l'article L.124-1 et s. du Code de l'environnement et à l'article 2 al. 1 f) de la directive n° 2003/4/CE du 28/01/03 concernant l'accès du public à l'information en matière d'environnement et abrogeant la directive 90/313/CEE du Conseil.

[22] Titre 2 de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

[23] C.-F. Mélanie, R. Agnès, B. Serge *et al. La production et l'exploitation des données ouvertes.* Séminaire organisé par le laboratoire D@nte, avec la collaboration de l'Ercim, dans le cadre du projet ISIS, 29 mai 2015, Université de Versailles Saint-Quentin-en-Yvelines.

[24] CJUE, 1er mars 2012, C-604/10, Football Dataco : *Gaz. Pal.*, 1er août 2012, p.11 note L. Marino.

[25] Art. 1 al. 2 de la Directive 96/9/CE du Parlement européen et du Conseil, du 11 mars 1996, concernant la protection juridique des bases de données.

publique dont le principe de libre d'accès est consacré par le Code de l'environnement[26], la directive 2003/4[27] et la Convention d'Aarhus[28] ? Doit-on considérer que le téléchargement d'une donnée en principe librement accessible constitue un délit dès lors que le consentement de la personne qui les détient n'a pas été donné en amont ? En l'espèce, les informations réutilisées par le blogueur portaient sur la légionellose, et donc manifestement sur des questions de santé publique. Le principe de libre accès aux informations relatives à l'environnement – incluant l'état de la santé humaine – souffre déjà de nombreux facteurs d'ineffectivité[29] ; en considérant un organisme comme propriétaire de celles-ci, et en qualifiant ainsi le vol, la Chambre criminelle ne conduit-elle pas, consciemment ou inconsciemment, à fragiliser d'avantage ce droit d'accès ?

Cette fragilité est par ailleurs nettement aggravée par la sévérité de la loi du 13 novembre 2014 relative au terrorisme qui enfonce le clou en condamnant la simple extraction, reproduction ou transmission de données dès lors qu'elle est « *frauduleuse* ». Par voie de conséquence, une information publique ou en principe accessible au public est *de facto* inaccessible sans le consentement des autorités (à moins de prendre le risque de commettre un délit). Selon certains auteurs, « *Bluetouff est [à sa manière] un lanceur d'alerte, et les données téléchargées méritaient peut être d'entrer dans le débat public* »[30], mais les lanceurs d'alerte sont désormais prévenus : aucune donnée, quelle que soit son importance, ne doit être mise à disposition du public sans le consentement de la personne qui la détient. Alors que d'autres systèmes juridiques développent un régime protecteur des lanceurs d'alerte, le droit français réduit au contraire, consciemment ou inconsciemment, leurs moyens d'investigations.

[26] Articles L.124-1 et s. du Code de l'environnement.
[27] Directive 2003/4/CE du Parlement européen et du Conseil du 28 janvier 2003 concernant l'accès du public à l'information en matière d'environnement et abrogeant la directive 90/313/CEE du Conseil.
[28] La convention d'Aarhus sur l'accès à l'information, la participation du public au processus décisionnel et l'accès à la justice en matière d'environnement, 25 juin 1998.
[29] B. Aurélie. « Le droit de l'information environnementale est-il effectif ». *Cycle de conférences du Conseil d'État*. Paris : La documentation Française, 2013, p.185.
[30] Roseline Letteron. « Télécharger, c'est tromper ? ». *Droit et Justice*, 11 février 2014.