Vol d'information : une jurisprudence Bluetouff pour la gloire ? (tribune)

Le 20 mai 2015, la Cour de cassation a statué dans un arrêt très attendu concernant ce qui est devenu « l'affaire Bluetouff ». Avec cet arrêt, la Cour de cassation prend clairement position : pour elle, une information peut être volée, c'est-à-dire que l'article 311-1 du Code pénal réprimant la « *soustraction frauduleuse de la chose d'autrui* » est pleinement applicable à la copie et l'exfiltration depuis un extranet de fichiers informatiques.

Nous aurions pu parler d'évolution majeure de la notion, dont une affirmation aussi claire était attendue depuis près d'une quinzaine d'années, si elle était arrivée quelques mois plus tôt. Nous nous contenterons de **saluer ce principe qui va dans le bon sens,** tout en étant **loin de fournir un blanc seing à la non-sécurisation des systèmes d'information** comme certains ont pu le craindre.

Bref rappel des faits…

Nous renvoyons le lecteur intéressé par le récit détaillé des évènements aux articles qui ont pu être écrits sur le sujet, notamment ici et là.

Il nous suffira ici de reprendre les éléments essentiels à notre sens :

- En août 2012, un journaliste/blogueur/informaticien au surnom de « Bluetouff », recourant en toute légalité à un VPN lui fournissant une adresse panaméenne, utilise les fonctionnalités d'un moteur de recherche pour se rendre sur une page librement accessible de ce qui s'avère être l'extranet de l'ANSES (Agence nationale de sécurité sanitaire de l'alimentation, de l'environnement et du travail). Grâce à cette faille manifeste de sécurité, il accède à des documents qui y sont stockés, en télécharge 7,7 Go (8 000 fichiers) et en publie une partie (250 Mo) dont il utilise le contenu pour ses articles, indiquant être en possession des 7,7 Go.
- L'ANSES s'en aperçoit et porte plainte pour « *intrusion dans un système informatique et vol de données informatiques* ».
- Or l'ANSES est un Opérateur d'Importance Vitale (OIV). La Direction Centrale du Renseignement Intérieur est alors chargée de l'enquête (d'autant plus au vu de l'origine géographique supposée des téléchargements).
- Durant sa garde à vue, Bluetouff explique les faits (le moteur de recherche, le VPN, l'IP, l'accès non protégé, etc.). **Mais il précise également** « *qu'après être arrivé « par erreur » au cœur de l'extranet de l'ANSES, avoir parcouru l'arborescence des répertoires et être remonté jusqu'à la page d'accueil, [qu'] **il avait constaté la présence de contrôles d'accès et la nécessité d'une authentification par identifiant et mot de passe*** **».**
- Le ministère public engage les poursuites.
- En première instance, le Tribunal correctionnel de Créteil relaxe Bluetouff. Pour le Tribunal, l'intention de restreindre l'accès au serveur extranet n'étant pas manifeste, « *Monsieur Olivier L. (le vrai nom de Bluetouff, NDLR) a pu donc légitimement penser que certaines*

données sur le site nécessitaient un code d'accès et un mot de passe mais que les données informatiques qu'il a récupérées étaient en libre accès et qu'il pouvait parfaitement se maintenir dans le système ». Par ailleurs, il ne peut y avoir « vol », l'article 311-1 du Code pénal n'étant pas applicable à des choses immatérielles dont l'accès ne dépossède pas le propriétaire.

- La Cour d'appel de Paris a pris une position inverse et a condamné Bluetouff. Certes, il n'y avait pas d'accès frauduleux en raison de la défaillance technique ayant rendu le serveur extranet de l'ANSES accessible (l'informaticien ne pouvait connaître la volonté de l'ANSES de restreindre l'accès). Toutefois, il est **condamné pour maintien frauduleux**, étant donné qu'il a reconnu constater à un moment « *la présence de contrôles d'accès et la nécessité d'une authentification par identifiant et mot de passe ».* Dès lors, il aurait dû se déconnecter immédiatement. La Cour d'appel est par contre beaucoup moins diserte sur la qualification de vol, se contentant d'énoncer que des « *copies de fichiers informatiques inaccessibles au public* » ont été faites « *à des fins personnelles à l'insu et contre le gré de leur propriétaire*».

La Cour de cassation reconnaît enfin le « vol d'information »

L'arrêt de la Cour de cassation était donc très attendu par nombre de juristes et d'informaticiens. Et c'est un euphémisme. Cela fait en effet près d'une quinzaine d'années que la question se pose de la formulation de l'article 311-1 du Code pénal et de son application à la copie d'un fichier informatique : peut-on « voler » une information tel qu'un fichier alors même que son propriétaire aurait toujours le fichier à sa disposition et n'en serait donc pas dépossédé ?

La jurisprudence ne semblait pas aller dans ce sens, s'appuyant sur la formulation de l'article et sur le fait que l'interprétation des textes pénaux doit s'entendre strictement. Certains, comme d'ailleurs le rapporteur devant la Cour de cassation dans cette affaire, ont pu tracer un parallèle avec le vol d'électricité, admis par la Cour de cassation dès 1912, pour indiquer que l'interprétation du texte devait être en phase avec son temps. Certes, mais l'électricité n'étant ni immatérielle, ni exempt de dépossession, le parallèle pouvait être considéré comme un peu rapide.

Pourtant, la Cour de cassation répond ici très clairement à cette interrogation, en indiquant que la Cour d'appel avait justifié sa décision de condamnation pour vol, l'informaticien ayant « *soustrait des données qu'il a utilisées sans le consentement de leur propriétaire* **». Pour les magistrats, la copie et l'exfiltration de données** sont donc assimilables à une soustraction et **peuvent donc être qualifiées de « vol ».** L'importance de la décision est d'ailleurs marquée par la Cour, *via* une publication dans ses Bulletins mensuels et bimensuels comme tout arrêt de principe.

Il est dommage que cette position n'ait pas été aussi clairement tranchée à l'occasion d'arrêts antérieurs qui auraient pu l'accueillir (en 2008 et 2011 notamment), il aura fallu attendre une décision rendue quelques années plus tard pour ôter toute ambiguïté sur ce sujet…

Surtout, cette décision arrive quelques mois après que le législateur ait souhaité dissiper toute ambiguïté, très clairement là aussi. Ainsi, la **loi de lutte contre le terrorisme du 13 novembre 2014** a incidemment opéré une modification législative qui **a permis la répression du « vol**

d'information » en modifiant l'article 323-3 du Code pénal pour réprimer notamment l'extraction, la détention, la reproduction ou encore la transmission frauduleuse de données issues d'un système informatique (le droit parlant de « Système de Traitement Automatisé de Données » ou « STAD »)**.**

Sur le pourquoi et le comment de ce texte majeur, nous renvoyons le lecteur intéressé à l'analyse que nous en avions faite à cette occasion.

Précision qui a son importance : du fait de cette modification législative, la peine qui attend le « voleur d'information » n'est plus du tout la même !

Si Bluetouff a été condamné à 3 000 € d'amende, il faisait face théoriquement à une peine de 3 ans d'emprisonnement et de 45 000 € d'amende (art. 311-3 du Code pénal). Or, aujourd'hui les mêmes faits seraient **passibles de pas moins de 7 ans d'emprisonnement et de 100 000 € d'amende !**

En effet, la loi du 13 novembre 2014 a non seulement considéré que le vol de données informatiques devait être **plus durement puni que le vol « classique »** (5 ans contre 3 ans d'emprisonnement, 75 000 € d'amende contre 45 000 €), mais qu'en plus la commission « *à l'encontre d'un système de traitement automatisé de données à caractère personnel mis en œuvre par l'Etat* » devait être une circonstance aggravante (ce qui serait donc le cas pour l'ANSES).

De façon incidente, émettons toutefois une réserve de taille sur la répression du piratage informatique de façon générale : si les sanctions prévues sont importantes, et de plus en plus au gré des réformes, il existe un (très) fort décalage avec le petit nombre de décisions de condamnations rendues et avec la faiblesse des peines prononcées.

L'arrêt du 20 mai 2015 : quelles conséquences ?

Cette interprétation, arrivant après la bataille, ne présente-t-elle qu'un intérêt historique ? Pas forcément. Si cette décision met certes un terme à un débat historique entre juristes, elle peut surtout être **annonciatrice d'une lecture « modernisée » d'autres** textes du Code pénal, considérant que leur interprétation pourra là aussi être mise en phase avec l'époque actuelle.

De façon plus anecdotique, l'article 311-1 pourra théoriquement servir de texte « d'appoint » au cas où le texte spécifique (le 323-3 susnommé) pourrait ne pas s'appliquer aux faits réprimés. A la lecture des textes et au vu de la définition très large de la notion de STAD par la jurisprudence, gageons toutefois que ces cas seront peu nombreux.

Enfin, cet arrêt donnera peut-être lieu à une décision de la Cour européenne des droits de l'homme (CEDH), que l'informaticien condamné souhaiterait a priori saisir. Or les affaires de piratage informatique et les textes qui les répriment se retrouvent rarement devant la CEDH. Cette affaire pourrait donc fournir une grille de lecture intéressante à l'avenir. Si la France devait être condamnée, ce pourrait être du fait de l'interprétation « modernisée » d'un texte qui existait bien avant l'informatique… et qui est aujourd'hui remplacé par un texte spécifique.

Pas un blanc-seing à l'absence de sécurisation

Si l'on étudie les commentaires concernant les articles qui fleurissent depuis quelques jours sur la problématique, un axe se dégage : cette décision serait une forme de blanc-seing pour les entités, les incitant à ne pas sécuriser leurs systèmes d'information. Grâce à cette interprétation, tout internaute ou hacker prenant en faute leur sécurité à partir d'un simple moteur de recherche pourrait ainsi être poursuivi.

Rassurons-les, ce n'est pas (du tout) le cas. En premier lieu, pour une raison simple : aucune juridiction n'a considéré que l'informaticien devait être condamné pour intrusion. Ce n'est **pas l'accès sur un système apparemment non protégé qui est** sanctionné (et sanctionnable). Ce point est fondamental et s'inscrit parfaitement dans le cadre de la jurisprudence « Kitetoa » de la Cour d'appel de Paris du 30 octobre 2002.

La différence réside dans le fait que, dans cette dernière affaire, le journaliste qui avait accédé à des données normalement confidentielles avait prévenu à plusieurs reprises l'administrateur du site de l'existence de la faille pour que ce dernier agisse. Poursuivi, il avait logiquement été relaxé.

Dans la présente affaire, la condamnation porte notamment sur **le maintien dans un serveur extranet** en sachant très bien que le propriétaire de celui-ci avait marqué son intention d'en restreindre l'accès, ce que montraient les pages mentionnant les authentifications nécessaires.

Un internaute tombant « par hasard », au gré de ses navigations, sur un serveur aux données qui ne devraient pas être accessibles… devrait tout simplement cesser la navigation et le faire remarquer au propriétaire : il ne pourrait pas être condamnable pour cela.

Plus globalement, c'est le propriétaire du site qui serait plutôt dans une situation fâcheuse du fait de cette absence de sécurisation, pour au minimum 3 raisons :

- les **effets médiatiques et économiques** d'une telle négligence, avec ses effets sur sa clientèle notamment ;
- les **risques de sanction de la CNIL** si des données à caractère personnel sont concernées, d'autant que le futur règlement européen sur le sujet rendra la notification des violations de sécurité sur ces données obligatoires et que les sanctions pour défaut de sécurisation se compteront bientôt en millions d'euros au minimum ;
- l'arrêt du 19 mars 2014 de la même chambre criminelle de la Cour de cassation. N'oublions pas en effet qu'il y a à peine 14 mois, les magistrats avaient décidé de revenir sur une jurisprudence de plus de 40 ans pour établir qu'en cas de piratage d'un système d'information, la faute de la victime – et donc le défaut de sécurisation du système d'information – devait être prise en compte pour évaluer le préjudice subi. En résumé, le **défaut de sécurisation de la victime conduit à diminuer, voire à exclure, les dommages-intérêts dus par l'attaquant**.

Autant de bonnes raisons (loin d'être exhaustives) pour une entité d'assurer la sécurité de son système d'information, et de ne pas s'attarder sur cette décision qui, pour elle, ne change pas l'état du droit.

*Par **François Coupez**, Avocat à la Cour, Associé du cabinet ATIPIC Avocat et titulaire du certificat de spécialisation en droit des nouvelles technologies*

A lire aussi, les précédentes tribunes de F. Coupez :

Protection des données personnelles et Big Data : inconciliables, vraiment ?

Administrateurs des SI : pourquoi une charte spécifique s'impose

Encadrement juridique du Cloud : peut-on éviter l'orage ?

Hacker les hackers : la « légitime défense numérique » existe-t-elle ?

Crédit photo : © adike / shutterstock