Y-a-t-il une place pour les white hats dans la République numérique ? (tribune)

Les débats sur le projet de loi dit République numérique porté par Axelle Lemaire ont pris fin au Sénat le 3 mai dernier, ouvrant la voie à l'entrée en scène de la Commission mixte paritaire. Ce projet de loi, dont la gestation a été attendue plusieurs années et dont l'histoire a depuis été teintée de rédaction collaborative à bref délai et d'urgence, ne donne lieu pour cette dernière raison qu'à une seule lecture dans les deux chambres. A l'Assemblée nationale, le projet avait été retouché sur certains points alors qu'au Sénat, les modifications sont encore plus profondes, apportant son lot de surprises (voir par exemple l'obligation de localisation des traitements de données personnelles dans un centre de données situé en UE et sans aucun transfert vers un pays tiers). La majeure partie des apports du projet, toujours en discussion, est susceptible d'évolution lors de son passage en Commission mixte paritaire, notamment cette obligation de localisation, problématique au regard du règlement européen sur la protection des données.

Il est toutefois un sujet qui semble avoir recueilli un accord du gouvernement comme des sénateurs de tout bord, même si des discussions pourront porter sur la rédaction précise du texte : il s'agit de l'action des « *white hats* » quand ils signalent des failles de sécurité trouvées dans des conditions litigieuses.

Pour comprendre ces dispositions et leurs évolutions, un rapide historique s'impose…

A l'Assemblée nationale, protection maximale

Lors des discussions à l'Assemblée nationale, un débat a vu le jour sur l'affaire dite « de l'ANSES » et la publication par un journaliste/blogueur célèbre de centaines de Mo de fichiers extraits d'un site officiel censé être sécurisé (accès permis via une simple recherche de documents sur Google). Pour un rappel des faits plus détaillé, nous renvoyons le lecteur à notre précédente chronique sur le sujet. Il suffira d'indiquer ici que le procès-verbal de garde à vue dudit journaliste mentionne que celui-ci, poursuivi du fait du maintien frauduleux dans l'extranet de l'Agence nationale de sécurité sanitaire, de l'alimentation, de l'environnement et du travail, a reconnu constater l'existence de mesures de protection lors de son accès. En vertu des textes et de la jurisprudence, il aurait donc dû immédiatement se déconnecter et non poursuivre sa consultation (ni télécharger 7,7 Go de données). Il a donc été condamné par la Cour d'appel de Paris le 5 février 2014, la Cour de cassation n'ayant fait que confirmer cette position le 20 mai 2015.

Emu de cette situation et se livrant à une interprétation erronée de cette jurisprudence, un parlementaire a fait adopter un amendement dispensant de toute peine les « *lanceurs d'alerte des systèmes informatisés* » dans de telles situations[1]. Le but était ainsi, d'après le parlementaire, d'éviter une condamnation pour accès de bonne foi via un moteur de recherche à un serveur insuffisamment protégé.

La lecture et l'interprétation de cet article laissaient toutefois dubitatif et posaient nombre de questions, certaines d'importance. Faute de précision dans le texte, on pouvait comprendre que

l'information de n'importe quelle autorité administrative ou judiciaire était suffisante pour échapper à la peine du fait de l'intrusion ou du maintien frauduleux (ou de leurs tentatives). Un appel à police secours était-il suffisant ? Quid du fait d'adresser un courrier officiel à la Cour de cassation ? D'aborder un juge du tribunal d'instance de Digne-les-Bains pour lui en toucher deux mots ? D'envoyer un mél à la CNIL ? Et si le hacker éthique, souhaitant contacter l'entreprise, ne contactait en réalité qu'un de ses sous-traitants ne faisant pas remonter l'information ? Toutes ces questions ne faisaient que souligner la problématique du canal de remontée d'information et du temps que celle-ci prendrait, points essentiels de nature à permettre à la société objet de l'intrusion de ne pas déposer une plainte qu'elle pourrait considérer comme inutile en l'absence de condamnation effective du hacker. Encore faut-il qu'elle le sache à temps !

De même, que se passerait-il après cette information ? Cela donnerait-il la possibilité au hacker de prévenir l'opinion publique dans la foulée de la faille qu'il penserait avoir trouvée de bonne foi (alors même que ce ne serait finalement pas avéré) ? Comment décourager, à côté du *white hat* de bonne foi désireux d'aider, « l'opportuniste » laissant comprendre qu'il peut sécuriser le système contre rémunération, et brandissant un devis à valider dans la journée (avant qu'il ne s'adresse à l'opinion publique ou aux régulateurs) ?

Si l'intention était louable et que la rédaction de ce nouvel article 20 *septies* était visiblement le fruit d'un large consensus parmi les parlementaires, il n'en reste pas moins que le résultat pouvait aboutir à des situations problématiques. L'article a même été considéré par certains sénateurs comme constituant « *vraiment une porte ouverte, et même un encouragement, à la commission de délits, voire davantage* . Une solution était donc attendue afin de protéger les intérêts de tous, en conservant le principe de protection des *white hats,* tout en revoyant la rédaction du texte de fond en comble.

Au Sénat, protéger lanceurs d'alerte… et SI !

Ce projet d'article 20 *septies* a ainsi été profondément remanié au Sénat. Exit tout d'abord le placement de la disposition dans le Code pénal, et ce pour une excellente raison : le Sénat a souhaité placer l'Agence Nationale de Sécurité des Systèmes d'Information (ANSSI) au cœur du jeu, en complétant les articles dédiés à la sécurité des systèmes d'information au sein du Code de la défense.

En insérant un nouvel article L. 2321-4[2] à la suite de ces dispositions, les sénateurs prévoient ainsi non seulement des conditions très claires de « *lancement de l'alerte* » en matière de sécurité des SI, mais surtout un point d'entrée unique. En synthèse, cet article ouvre la possibilité d'avertir l'ANSSI de l'existence de vulnérabilités affectant un système d'information. Si le *white hat* est de bonne foi et n'a pas préalablement rendu l'information publique, l'ANSSI se charge alors de préserver son identité confidentielle, ainsi que les conditions d'obtention de l'information, et avertit l'hébergeur, l'opérateur ou le responsable du système d'information de la menace, une fois le risque caractérisé.

L'intérêt devient évident pour les *white hats* : contrairement à la rédaction de l'Assemblée nationale, qui conduisait à sa poursuite pénale (ce qui peut être long et éprouvant) et finalement à une exemption de peine, la version du Sénat permet au *white hat* d'échapper dans un grand nombre de

cas à la poursuite pénale… pour peu qu'il n'ait pas été identifié lors de ses actions sur le SI ciblé (hypothèse non discutée pendant les débats). Dans ce dernier cas, même si la rédaction ne change rien *stricto sensu* et que la jurisprudence sur la notion s'applique (la condamnation nécessitant une intention délictuelle), l'intervention de l'ANSSI pourra toutefois être de nature à tempérer les ardeurs de l'entreprise lors d'une éventuelle plainte et aboutir, là aussi, à une meilleure protection des *white hats*.

Restait un point problématique : en tant que fonctionnaires, les agents de l'ANSSI ne sont-ils pas tenus, dès qu'ils acquièrent « *la connaissance d'un crime ou d'un délit* », « *d'en donner avis sans délai au procureur de la République et de transmettre à ce magistrat tous les renseignements, procès-verbaux et actes qui y sont relatifs* » ? Et donc de dénoncer l'acte du *white hat* qui pourrait, selon les cas, être assimilé à un délit ?

Une exception à l'article 40 et tout est différent

Cette règle est en effet prévue dans l'article 40 du Code de procédure pénale et la rédaction du Sénat ne permet rien de moins que d'y prévoir une exception ! « *Pour les besoins de la sécurité des systèmes d'information* », l'obligation « *n'est plus applicable* ».

Qu'en penser ? Tout d'abord une évidence : ce n'est pas parce qu'ils ne sont pas tenus à cette obligation que les agents de l'ANSSI ne pourront pas dénoncer des faits après enquête. S'il s'avérait par exemple que le *white hat* était en réalité malveillant. Surtout, cette exception, qui a donné lieu à beaucoup de débats entre sénateurs, n'est rien de moins qu'une évidence dictée par la pratique. Elle s'inscrit par ailleurs en totale conformité avec le discours de l'ANSSI, qui se présente depuis plusieurs années comme un 'pompier' agissant pour sécuriser les SI en cas d'attaque, sans en tirer immédiatement un constat à charge contre l'entreprise.

Et maintenant : qu'attendre de la CMP ?

On pourrait penser que la Commission mixte paritaire (CMP), bientôt saisie du projet de loi, reviendra en grande partie sur la rédaction du projet dans son ensemble et détricotera le travail du Sénat. Néanmoins, cet article résistera peut-être, les discussions au Sénat ayant permis de gagner le soutien de la secrétaire d'État, Axelle Lemaire. Cette dernière indiquait lors des discussions qu'il lui semblait « *logique de soutenir cette proposition de recourir à l'ANSSI* » compte tenu du fait que « *l'ANSSI est composée des meilleurs informaticiens de notre pays, lesquels sont susceptibles d'un point de vue technique, du fait de leur expertise, de comprendre plus rapidement que ne pourrait certainement le faire le système judiciaire si la détection de la faille avait une intention malveillante ou s'il s'agit d'un signalement sincère et non frauduleux* ».

Reste à savoir ce qu'il adviendra de la précision concernant l'exception à l'article 40 du Code de procédure pénale (obligation de dénonciation des fonctionnaires), qui semble quant à elle sur la sellette. Surtout, les réflexions plus globales sur les « lanceurs d'alerte » pourraient, si elles restent

justement trop générales, avoir des effets de bord très importants sur la sécurité des SI. Sur cette question, nous ne pouvons qu'inviter le lecteur intéressé à suivre le devenir de la proposition de loi relative à la protection globale des lanceurs d'alerte du 29 mars 2016 aux définitions floues et à « l'Agence nationale de l'alerte » omnisciente…

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

1 « L'article 323-1 du code pénal est complété par un alinéa ainsi rédigé :

« *Toute personne qui a tenté de commettre ou commis le délit prévu au présent article est exempte 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*. »

2