Particularité et protection des « Hackers Blancs »

Fiche pratique publié le **25/08/2021**, vu **1591 fois**, Auteur : La zone du droit

Avec les « Hackers blancs », nous sommes passés de la « cybercriminalité » à la « cybersécurité ».

L'article 323-1 du Code pénal dispose que : *« Le fait d'accéder ou de se maintenir, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données est puni de deux ans d'emprisonnement et de 60 000 € d'amende.*

Lorsqu'il en est résulté soit la suppression ou la modification de données contenues dans le système, soit une altération du fonctionnement de ce système, la peine est de trois ans d'emprisonnement et de 100 000 € d'amende.

Lorsque les infractions prévues aux deux premiers alinéas ont été commises à l'encontre d'un système de traitement automatisé de données à caractère personnel mis en œuvre par l'Etat, la peine est portée à cinq ans d'emprisonnement et à 150 000 € d'amende. » [1]

Selon l'article 323-2 du Code pénal, *« le fait d'entraver ou de fausser le fonctionnement d'un système de traitement automatisé de données est puni de cinq ans d'emprisonnement et de 75000 euros d'amende.*

Lorsque cette infraction a été commise à l'encontre d'un système de traitement automatisé de données à caractère personnel mis en œuvre par l'Etat, la peine est portée à sept ans d'emprisonnement et à 100000 € d'amende. » [2]

La destruction de fichiers, de programmes, de sauvegardes, le flaming sont autant d'actes d'entrave susceptibles de provoquer des dysfonctionnements du système informatique.

« Le flaming » consiste à se livrer à des attaques via internet en ayant la volonté de perturber le système d'information de son interlocuteur et en suscitant un encombrement important de la capacité de la mémoire.

En outre, le Code pénal prévoit en son article 323-3 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 150 000 € d'amende.*

Lorsque cette infraction a été commise à l'encontre d'un système de traitement automatisé de données à caractère personnel mis en œuvre par l'Etat, la peine est portée à sept ans d'emprisonnement et à 300 000 € d'amende. » [3]

Les attaques informatiques fomentées par les cybercriminels ou *« hackers noirs »* font de plus en plus parti de notre vie quotidienne. En effet, depuis le début de la crise sanitaire les attaques informatiques ont connu une progression exceptionnelle. La majorité des attaques informatiques des *« cybercriminels »* ou *« cyber-délinquants »* visent à dérober les données de santé, données

bancaires, données des clients d'un opérateur téléphonique ou encore à prendre en otage les services informatiques d'un établissement en échange de rançons.

Par exemple, le géant de la téléphonie *« Orange »* a été victime d'une intrusion en avril 2014 suite à une défaillance technique de l'un de ses prestataires qui aurait conduit au vol des données personnelles de 1,3 millions de clients.

Sony Picture a été victime aux Etats-Unis, en novembre 2014 d'une opération de grande envergure menée par des pirates qui ont soustrait 100 téraoctets de données sensibles incluant l'annuaire de plus de 6500 salariés avec leurs adresses, dates de naissance, numéros de sécurité sociale, salaires, appréciations de l'employeur, mots de passe de compte twitter et de Facebook ou encore de comptes bancaires.

Plus récemment, des hackers ont réussi à dérober 600 millions de dollars de cryptomonnaies en exploitant une faille dans *Poly Network*, une plateforme de finance décentralisée qui connecte différentes blockchains entre elles. Alors que la société les exhortait de rendre le butin, les hackers ont finalement rendu 260 millions de dollars. L'attaque actuelle serait l'un des plus grands hacks de l'histoire de la crypto à l'heure actuelle. [4]

Par ailleurs, en fonction du risque représenté par le traitement, les responsables du traitement et les éventuels sous-traitants doivent mettre en œuvre les mesures techniques et d'organisation appropriées pour protéger les données contre la destruction illicite, la perte accidentelle, l'altération, la diffusion ou l'accès non autorisés aux données des personnes concernées.

Toutefois, sur internet, de nombreux sites web comportent des failles de sécurité, qui rendent possible l'accès à des données qui auraient normalement dû être protégées, et ce sans avoir besoin de disposer d'outils de piratage, uniquement en cliquant sur les liens publics du site ou en effectuant des requêtes sur un moteur de recherche.

Un internaute de bonne foi et dépourvu d'intention malveillante peut alors accéder à des données de manière non autorisée. Il arrive également que des internautes révèlent une faille de sécurité qu'ils ont repérée, et qu'ils veulent porter à l'attention des responsables du système ou de la communauté informatique : ce sont les *« hackers blancs ».*

I) Notion du *« Hacker blanc »*

Avec les *« Hackers blancs »,* nous sommes passés de la *« cybercriminalité »* à la *« cybersécurité ».* Le *« Hacker blanc »* est un spécialiste de l'informatique qui utilise ses connaissances de très haut niveau pour s'introduire dans les systèmes informatiques d'entreprises, d'agences bancaires, de centre hospitaliers par exemple sans le consentement de ces agents pour rechercher d'éventuelles failles dans lesdits systèmes. [5]

Contrairement aux *« Hackers noirs »,* ces *« Hackers blancs »* ne dérobent pas les données contenues dans les systèmes informatiques dans lesquels ils s'introduisent mais agissent comme *« des lanceurs d'alerte ».* Leur objectif est de prévenir contre les failles des systèmes informatiques et d'en alerter les autorités compétentes.

Son introduction dans les systèmes informatiques doit se faire de bonne foi dans un souci de détection de failles au niveau de la sécurité informatique contrairement au *« Hacker noir ou pirate »* qui lui agit dans tous les cas de mauvaise foi afin d'en tirer profit de son infraction.

La notion de *« bonne foi »* est celle qui doit être le commencement de toute intrusion des *« Hackers blancs »* dans les systèmes informatiques sans autorisation du maître des lieux.

La *"bonne foi"* est la croyance qu'a une personne de se trouver dans une situation conforme au droit, et la conscience d'agir sans léser les droits d'autrui. C'est une notion fréquemment utilisée dans notre législation pour atténuer les rigueurs de l'application de règles positives. [6]

Ainsi, toute intrusion de mauvaise foi dans un système informatique est une violation des droits des personnes concernées ou du maître des lieux. A titre d'exemple, un journaliste spécialisé ayant découvert une faille de sécurité relative à un produit Microsoft et ayant et ayant informé Microsoft, a été condamné en 2009 sur le fondement des textes du Code pénal sanctionnant les atteintes aux systèmes de traitement automatisé de données (Code pénal, article 323-1 s.). En effet, ce journaliste invoquant sa volonté d'information du public contre les dangers de l'informatique, avait ensuite publié sur son site internet des informations permettant d'exploiter cette faille de sécurité.

La Cour d'appel a rejeté l'excuse de la bonne foi en estimant qu'il y avait mise à disposition de moyens conçus pour commettre une atteinte à un système informatique, sans motif légitime, ce qui caractérisait l'infraction. Cette condamnation a été confirmée par la Cour de cassation. [7]

Il ne s'agit donc pas d'exonérer de sanction les « Hackers pirates » qui exploitent les failles au sein d'un système d'information et souhaiteraient se protéger a posteriori. [8]

II) Protection des « Hackers blancs »

La loi du 7 Octobre 2016 prévoit des dispositions spécifiques pour les *« Hackers blancs »* qui recherchent des failles de sécurité et qui préviennent les seules autorités (l'ANSSI).

Selon l'article L.2321-4 du Code de la défense, « *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'autorité 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.

L'autorité peut procéder aux opérations techniques strictement nécessaires à la caractérisation du risque ou de la menace mentionnés au premier alinéa du présent article aux fins d'avertir l'hébergeur, l'opérateur ou le responsable du système d'information. » [9]

Ainsi, pour bénéficier de cette protection, il faut avoir agi de « *bonne foi* » comme expliqué ci-dessus.

En 2015, la Cour de cassation a confirmé la condamnation à 3 000 euros d'amende du blogueur connu sous le nom de Bluetouff. [10]

Celui-ci, en effectuant des recherches sur Google pour un article, avait obtenu comme résultat de ses requêtes des liens vers des documents de l'Agence nationale de sécurité sanitaire de l'alimentation, de l'environnement et du travail (ANSES). Il avait suivi ces liens, était arrivé sur le site de l'ANSES, et avait téléchargé des documents qui lui avaient servi à rédiger un article. Or les documents en question étaient censés être confidentiels.

L'ANSES avait donc porté plainte, et l'enquête avait été confiée à la Direction Générale de la Sécurité Intérieure (DGSI). Celle-ci avait identifié Bluetouff d'autant plus facilement qu'il ne cherchait pas à se cacher et qu'il avait signé son article. Le domicile du blogueur avait été perquisitionné, son matériel informatique saisi, et il avait subi une garde à vue d'une trentaine d'heures.

L'enquête démontra que le système de sécurisation par mot de passe du site de l'ANSES était défaillant, et donc que l'on pouvait accéder à ce site directement depuis une requête sur le moteur de recherche Google. Estimant que, de ce fait, l'ANSES n'avait pas manifesté clairement son intention de restreindre l'accès aux fichiers en question, et que par conséquent Bluetouff avait pu légitimement penser que ces données étaient en accès libre, le Tribunal de Grande Instance de Créteil avait d'abord relaxé le blogueur.

Le Procureur de la République ayant fait appel, la Cour d'appel de Paris avait finalement condamné Bluetouff.

L'accès aux fichiers ayant été rendu possible par une défaillance de l'ANSES, la Cour a certes considéré qu'il n'y avait pas accès frauduleux au système. En revanche, le prévenu ayant reconnu qu'il avait constaté sur la page d'accueil du site la présence d'un contrôle d'accès par mot de passe, la cour a estimé qu'il avait conscience que son maintien dans le système était irrégulier : le délit de maintien frauduleux était donc constitué. En outre, la Cour a estimé qu'en faisant des copies de fichiers informatiques, « *à l'insu et contre le gré* » de leur propriétaire, Bluetouff s'était rendu coupable de vol de données (C. pén., art. 311-1).

Après le rejet de son pourvoi par la Cour de cassation, ce dernier a annoncé envisager de saisir la Cour européenne des droits de l'homme.

Pour éviter toute poursuite de la part de l’entreprise dont les failles du système informatiques ont été découvertes par le ou les « Hacker(s) blanc(s) », ces derniers doivent dans les plus brefs délais en informer l’autorité compétente citée ci-dessus (l’ANSSI). Son attitude désintéressée et sa bonne foi l’exemptera de ce fait de toute poursuite judiciaire. Son identité n’est pas divulguée, il reste donc dans l’anonymat.

Sources :

1- L’article 323-1 du Code pénal

2- L’article 323-2 du Code pénal

3- Code pénal, article 323-3

4- Les hackers restituent 260 millions de dollars à Poly Network sur les 600 millions piratés : https://www.usine-digitale.fr/article/les-hackers-restituent-260-millions-de-dollars-a-poly-network-victime-d-un-piratage.N1132129

5- AVEC LES HACKERS BLANCS, ON EST PASSÉ DE LA CYBERCRIMINALITÉ À LA CYBERSÉCURITÉ : https://www.labecedaire.fr/2019/04/16/avec-les-hackers-blancs-on-est-passe-de-la-cybercriminalite-a-la-cybersecurite/

6- Définition de Bonne foi : https://www.dictionnaire-juridique.com/definition/bonne-foi.php

7- Cass. Crim 27 Oct.2009, n°09-82.346.

8- (Christiane FERAL-SCHUHL, CYBERDROIT : Le droit à l'épreuve de l'internet, 8è édition. P.1084).

9- Article L2321-4 Code de la défense : L. n°2016-1321, 7 Octobre 2016 pour une République numérique, JO 8 oct., n°1

10- Faut-il dépénaliser les hackers blancs ? https://www.cairn.info/revue-de-science-criminelle-et-de-droit-penal-compare-2015-4-page-837.htm#:~:text=Selon%20Wikipedia%2C%20«%20Un%20white%20hat,%27information%20d%27une%2
.