Dalloz IP / IT

DROIT DE LA PROPRIÉTÉ INTELLECTUELLE ET DU NUMÉRIQUE

Numéro 10 - Octobre 2021

9 782997 521102

DOSSIER | P. 482
LA LUTTE CONTRE LA CYBERCONTREFAÇON

PRATIQUE
Le *hacking* éthique : votre meilleur ennemi ?
Geoffroy Goubin & Lisa Janaszewicz

TEXTES ET DÉCISIONS
Mise à jour des modèles de clauses contractuelles types par la Commission européenne le 4 juin 2021 : ce qu'il faut savoir (décis. exéc. UE 2021/914)
Fabrice Naftalski

TEXTES ET DÉCISIONS
Présentation rapide du Règlement (UE) 2021/784 du 29 avril 2021 relatif à la lutte contre la diffusion des contenus à caractère terroriste en ligne
Emmanuel Dreyer

Version numérique incluse*

DALLOZ

LE *HACKING* ÉTHIQUE : VOTRE MEILLEUR ENNEMI ?

Geoffroy Goubin
Avocat au barreau de Paris, associé, cabinet Bougartchev Moyne associés

Lisa Janaszewicz
Avocat au barreau de Paris, collaboratrice, cabinet Bougartchev Moyne associés

Depuis le milieu des années 2010, la transformation numérique de la société et de l'économie a conduit à une forte augmentation de la cybercriminalité[1]. La crise sanitaire du coronavirus a renforcé la tendance à la digitalisation des activités, tous secteurs confondus et, par la même occasion, le risque de cyberattaques.

En décembre 2020, l'Agence nationale de la sécurité des systèmes informatiques (ANSSI) alertait sur l'accroissement du niveau de menaces cyber, sur les conséquences critiques des cyberattaques sur de nombreuses activités et sur les pertes financières importantes engendrées pour les entités piratées[2]. Il faut dire qu'entre 2019 et 2020, le nombre de rançongiciels[3] traités par l'ANSSI a pratiquement été multiplié par quatre[4].

Les cybercriminels, aussi appelés *hackers*, se professionnalisent et se structurent[5]. Les attaques récentes contre les entités françaises se caractérisent par une sophistication et une furtivité accrues, ce qui les rend d'autant plus préjudiciables[6].

Le *hacker* est donc devenu une source de grande vulnérabilité pour les entreprises et les administrations. Et s'il était, par ailleurs, leur plus grand allié ?

Une nouvelle profession, déjà incontournable outre-Atlantique, connaît aujourd'hui un essor sur le continent européen : le *hacker* éthique.

Comme d'autres procédés plus classiques, tels que le scan automatique de vulnérabilités ou les audits de sécurité informatique, le *hacking* éthique est un moyen préventif de lutte contre la cybercriminalité, qui vise à se prémunir, en amont, contre le risque d'attaques.

Contrairement à son homologue mal intentionné, le *hacker* éthique – ou « *hacker* blanc » – n'entre pas par effraction dans les systèmes informatiques des entreprises. Ce lanceur d'alerte de sécurité n'a pas pour but ultime le piratage de données. Il travaille de concert avec les entités concernées afin d'identifier les failles de sécurité que peuvent présenter leurs systèmes.

Les *hackers* blancs interviennent sur demande des clients, entreprises ou institutions, par l'intermédiaire de plateformes spécialisées (*Hacker one*, leader mondial du secteur, *YesWeHack*, leader européen, etc.).

Les *hackers* éthiques sont généralement sollicités à l'occasion d'audits spécifiques

1 ANSSI, dossier de presse, Cybersécurité, faire face à la menace : la stratégie française, 18 févr. 2021.

2 ANSSI, comm. presse, L'ANSSI et le BSI alertent sur le niveau de menace cyber en France et en Allemagne dans le contexte de la crise sanitaire, 17 déc. 2021.

3 Logiciels malveillants qui bloquent l'accès à l'ordinateur ou à des fichiers en les chiffrant et qui réclament à la victime le paiement d'une rançon pour y accéder de nouveau.

4 ANSSI, comm. presse, Cybersécurité : le gouvernement renforce la protection des citoyens, des administrations et des entreprises, 18 févr. 2021.

5 *Ibid.*

6 ANSSI, dossier de presse, 18 févr. 2021, préc.

de type « Bug Bounty », qui consistent à rechercher les éventuels bugs et vulnérabilités d'un système informatique. Il ne s'agit pas de « remontées sauvages » de failles de sécurité, mais d'une pratique convenue, encadrée et organisée ; une attaque planifiée, en somme.

L'efficacité de cette pratique semble d'autant plus redoutable que les *hackers* sont tiers à l'entreprise et rémunérés en fonction du nombre de failles effectivement identifiées ainsi que de leur criticité. Ils sont parfois mis en compétition entre eux, ce qui accroît leur ténacité et leur détermination à identifier les failles les plus critiques.

Ils sont généralement rémunérés au « bug recensé ». Autrement dit, le client ne paye que si son système informatique présente des vulnérabilités.

Lorsqu'ils détectent une faille, les *hackers* rédigent un rapport qui permet au client de retrouver la faille, d'évaluer les risques y afférents et de la corriger.

Dans un contexte de sophistication de la menace, le recours aux audits de type Bug Bounty constitue un complément efficace aux autres outils plus traditionnels de cybersécurité. Il permet aux entreprises et institutions de recourir aux services d'experts en cybersécurité aux profils variés et, ainsi, de démultiplier les compétences mobilisées.

Les vulnérabilités décelées par ces « pirates légaux » sont autant de brèches dans lesquelles un *hacker* malveillant aurait pu s'engouffrer.

I – UNE PRATIQUE ENCOURAGÉE PAR LES AUTORITÉS

Depuis quelques années, les pouvoirs publics commencent à se saisir de ce nouvel outil de prévention et semblent vouloir lutter contre le stéréotype tenace du *hacker* dangereux.

En 2016, le législateur est intervenu afin d'exonérer de poursuites pénales, dans certaines conditions, la personne de bonne foi signalant auprès de l'ANSSI l'existence d'une vulnérabilité concernant la sécurité d'un système informatique[7]. Cela constitue une première reconnaissance de l'activité des *hackers* éthiques et témoigne d'une volonté de les protéger contre le risque de sanction, d'une part, et d'inciter à la remontée d'informations, d'autre part.

Par ailleurs, les autorités françaises ont confirmé leur souhait d'encourager le recours à un tel procédé à l'occasion de la crise sanitaire de la covid-19. Ainsi, l'ANSSI a explicitement recommandé la réalisation d'un « audit de type Bug Bounty » dans le cadre de la mise en place de l'application StopCovid[8]. L'équipe projet StopCovid a donc lancé un programme de Bug Bounty afin de « garantir la fiabilité de l'application, grâce à la mobilisation d'une communauté d'experts indépendants en cybersécurité »[9].

Début 2021, le gouvernement annonçait mobiliser un milliard d'euros, dont 720 millions de financements publics, dans l'optique notamment de « faire émerger des champions français de la cybersécurité »[10].

II – UNE POTENTIELLE SOURCE DE RESPONSABILITÉ POUR LES ENTREPRISES

Pour autant, les entreprises européennes restent parfois frileuses à l'idée de laisser un *hacker*, avant tout perçu comme une menace, s'introduire dans leur système.

La pratique du *hacking* éthique n'est effectivement pas sans risque, puisqu'il est envisageable qu'un *hacker* prétendument éthique utilise finalement à mauvais escient l'accès au système informatique

7 C. défense, art. L. 2321-4, (issu de la loi n° 2016-1321, art. 47).

8 ANSSI, comm. presse, Application StopCovid - L'ANSSI apporte à Inria son expertise technique sur le volet sécurité numérique du projet, 27 avr. 2020.

9 ANSSI et Inria, comm. presse, « Conformément aux recommandations techniques de l'Agence nationale de la sécurité des systèmes d'information (ANSSI), l'équipe projet StopCovid lance ce mercredi 27 mai un programme de Bug Bounty pour garantir la fiabilité de l'application, grâce à la mobilisation d'une communauté d'experts indépendants en cybersécurité », 26 mai 2020.

10 ANSSI, comm. presse, 18 févr. 2021, préc.

qui lui a potentiellement été octroyé, par exemple, pour extraire et diffuser des données sensibles ou des données à caractère personnel.

Dans un tel cas de figure, le *hacker*, sous réserve qu'il soit identifiable, pourra faire l'objet de poursuites, notamment sur le fondement des infractions d'atteinte au fonctionnement et aux données contenues dans un système de traitement automatisé de données (un système informatique)[11]. L'entité concernée par l'acte malveillant pourrait également se prévaloir, selon les circonstances, d'un abus de confiance commis à son préjudice[12].

Toutefois, il n'est pas exclu qu'une entreprise qui a sciemment laissé pénétrer un *hacker* dans son système informatique engage également sa propre responsabilité vis-à-vis des tiers et des autorités en cas de détournement des données qui y étaient contenues.

En effet, la loi Informatique et libertés (n° 78-17 du 6 janvier 1978) et le règlement général sur la protection des données (RGPD), entré en vigueur en 2018[13], obligent les entreprises à garantir une sécurité quasi absolue des données personnelles traitées. En particulier, l'article 32 du RGPD oblige les responsables d'un système de traitement des données à mettre en œuvre des « mesures techniques et organisationnelles appropriées pour assurer un niveau de sécurité adapté au risque ». Le non-respect de ces dispositions peut entraîner une sanction pénale, allant jusqu'à cinq ans d'emprisonnement et 300 000 euros d'amende[14].

Néanmoins, en l'absence de négligences graves, le risque que l'entreprise soit effectivement poursuivie dans de telles circonstances semble limité. Ces poursuites auraient nécessairement un effet dissuasif sur le recours à la pratique du *hacking* éthique et iraient à l'encontre de la dynamique d'encouragement de cette pratique qui a actuellement cours.

Par ailleurs, les risques liés à la pratique du *hacking* éthique doivent être mis en perspective avec ceux, bien réels, liés à l'existence de failles au sein des systèmes informatiques des entreprises et qu'elles ont le devoir d'identifier et de corriger.

Selon la directrice générale de la plateforme de *hacking* éthique Yogosha, avec laquelle nous avons pu nous entretenir[15], la problématique juridique continue toutefois de représenter, pour les clients, un frein au recours à cet outil.

III – LA NÉCESSITÉ D'UN ENCADREMENT TECHNIQUE ET JURIDIQUE ADAPTÉ

Le risque zéro n'existe pas, surtout dans le domaine de la cybersécurité.

Toutefois, il est aujourd'hui possible d'anticiper et de minimiser les risques liés à la pratique du *hacking* éthique, techniquement et juridiquement, en :

- recourant à une plateforme s'appuyant sur une communauté de *hackers* « fermée », localisés dans l'Union européenne, triés sur le volet, en fonction de leurs compétences mais aussi de leur éthique. Il est en effet souhaitable que la plateforme dispose de toutes les informations relatives aux activités du *hacker*, lequel exerce bien souvent, en parallèle de son activité de *hacking*, d'autres fonctions notamment salariées ;
- exigeant d'avoir accès à toutes les données relatives au profil des *hackers* amenés à intervenir et en prédéterminant des critères de sélection spécifiques (coût, nationalité, absence de conflits d'intérêts du fait d'activités exercées par ailleurs dans certains secteurs, etc.). En cas d'activité impliquant le traitement de données particulièrement sensibles (ministères, entreprises du secteur de la santé ou de la défense, etc.), il peut être envisagé d'exiger la mise à disposition d'une équipe attitrée de *hackers*, présentant des garanties supplémentaires

11 C. pén., art. 323-1, 323-2 et 323-3.

12 C. pén., art. 314-1, le *hacker* ayant « détourné » les données auxquelles l'entité lui a donné accès.

13 Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, en vigueur le 25 mai 2018.

14 C. pén., art. 226-17 : « Le fait de procéder ou de faire procéder à un traitement de données à caractère personnel sans mettre en œuvre les mesures prescrites aux articles 24, 25, 30 et 32 du règlement (UE) 2016/679 du 27 avril 2016 précité ou au 6° de l'article 4 et aux articles 99 à 101 de la loi n° 78-17 du 6 janvier 1978 précitée est puni de cinq ans d'emprisonnement et de 300 000 euros d'amende ».

15 Plateforme française spécialisée dans le Bug Bounty créée en 2015, qui repose sur une communauté d'environ 500 *hackers*.

CE QU'IL FAUT RETENIR

Le *hacking* éthique n'est pas spécifiquement encadré, à ce jour, sur le plan juridique. Afin de bénéficier pleinement de cet outil tout en limitant les risques de responsabilité en cas de fuite ou de détournement de données, il convient de sélectionner scrupuleusement les plateformes prestataires et d'exiger de leur part certaines garanties, techniques et juridiques.

et s'engageant à ne pas œuvrer pour le compte d'autres entités déterminées ;

- mettant en place des mécanismes permettant de s'assurer que les *hackers* sont juridiquement responsables de leurs actes, tels que la signature de conditions générales d'utilisation les soumettant à une obligation stricte de confidentialité, à une obligation de signaler à l'entreprise toute prise de connaissance ou toute extraction malencontreuse, par le *hacker*, de données (notamment de données personnelles) ;
- déterminant, dans le cadre de la signature d'un contrat avec la plateforme, une mission et un champ d'intervention matériel et temporel précis pour le *hacker* ;
- recourant à une plateforme proposant un *monitoring* et un enregistrement des activités du ou des *hackers* sélectionnés, afin de pouvoir, en cas de besoin, retracer l'intégralité du parcours du *hacker* au sein des systèmes informatiques testés ;
- prévoyant l'octroi d'un droit de propriété exclusif de l'entreprise sur tous les documents relatifs au Bug Bounty et, notamment, sur les rapports de faille rédigés par les *hackers*, afin d'éviter le risque de « *vulnerability disclosure* », pratique qui consiste à dévoiler publiquement les failles de sécurité d'une entreprise, portant préjudice à sa réputation.

Cet arsenal juridique et technique semble être à même d'éviter la survenance d'incidents.

Pour autant, une évolution législative serait bienvenue.

L'instauration d'un cadre réglementaire clair et spécifique à la pratique du *hacking* éthique permettrait d'encourager le recours à cet outil, de limiter les risques de dérives et donc, à terme, de rendre plus efficace et adaptée la lutte contre les cyberattaques.

Un tel encadrement légal serait cohérent avec l'objectif affiché des autorités de mettre tout en œuvre pour promouvoir la cybersécurité, décrite par Bruno Le Maire, ministre de l'Économie, des finances et de la relance, comme « un enjeu majeur du XXIe siècle » [16].

16 ANSSI, dossier de presse, 18 févr. 2021, préc.