White Hat Hackers :

Leur situation juridique, les risques qu'ils prennent et le rôle du PFPDT

I. Objet

1 Cette feuille d'information s'adresse avant tout aux White Hat Hackers. Elle vise à les sensibiliser sur la nature de leurs activités en regard du cadre juridique dans lequel elles s'inscrivent, en particulier du point de vue de la protection des données. Cette feuille d'information ne vise pas à porter de jugement sur ces activités, mais constate simplement que ces acteurs existent et que, dans cette mesure, il convient de les orienter quant à leurs comportements.

II. Contexte et définitions

1. White Hat Hackers (WHH)

2 Les annonces au PFPDT, ou bien auprès de médias, liées à la découverte de failles dans des systèmes informatiques se multiplient. Ces annonces sont souvent le fait de personnes se décrivant comme des hackers éthiques (*White Hat Hackers*, ci-après : « WHH »). Dans son expression idéale, un WHH s'emploie à détecter des failles dans une optique bienveillante : il ne cherchera pas à les exploiter pour en tirer un avantage, ni à les utiliser au profit d'une cause particulière (hacker activiste ou « hacktiviste »). Au contraire, il va mettre l'exploitant du système en position de corriger les failles et ainsi, d'améliorer sa sécurité informatique. À noter que les WHH peuvent intervenir dans le cadre d'un mandat reçu de l'exploitant du système, afin de le tester : ce cas de figure, où précisément ils agissent en accord avec la cible, ne pose *a priori* pas de difficulté et n'est donc pas l'objet de cette feuille d'information.

3 Les explications qui vont suivre visent ainsi les WHH qui agissent en dehors de tout cadre et à l'insu de l'exploitant du système, lequel n'en sera informé que si une faille est effectivement trouvée. Par leurs agissements, ils peuvent rapidement tomber dans l'illicéité. Sans prétendre à l'exhaustivité, cette feuille d'information vise à tracer quelques pistes de réflexion, pour que les WHH soient plus à même d'évaluer les implications de leurs actes. L'optique ici abordée est celle d'un WHH dans son expression idéale et voulant « faire juste » ; par définition, les activités des hackers qui visent un avantage direct (p. ex. exploiter les données à leurs propres fins) ou celles des activistes, qui utilisent ces failles à des fins protestataires (p. ex. bloquer le site internet d'une entreprise), sont *a priori* incompatibles avec les prescriptions qui vont suivre (cf. notamment la notion plus large de « hacktivistes », notion indépendante des questions de malveillance/bienveillance, employée dans le rapport technique du NCSC « Types de menaces, auteurs et outils » du 16.02.2021, ch. 3.4.).

2. Coordinated Vulnerability Disclosure (CVD)

4 La *Coordinated Vulnerability Disclosure* (CVD) désigne le processus de coordination et de partage des informations sur les vulnérabilités entre les *stakeholders* concernés (découvreurs des failles, entreprises concernées, Computer Emergency Response Teams [CERT] du gouvernement) dans le but de réduire les effets négatifs des vulnérabilités et d'informer le public ; une politique CVD implique la mise en place de plateformes d'annonce auprès desquels les WHH peuvent signaler les failles de sécurité découvertes sans crainte de poursuites judiciaires ; en outre, dans le cadre d'une telle politique, les exploitants sont généralement tenus de combler les failles ainsi signalées après un délai défini.[1]

5 La notion de CVD va essentiellement à l'encontre de la prémisse reconnue et codifiée à l'art. 2 de la Convention de Budapest du 23 novembre 2001 sur la cybercriminalité (SR 0.311.43), selon laquelle les États signataires prennent des mesures législatives pour ériger en infraction pénale l'accès intentionnel à un système sans autorisation. Cela pourrait expliquer pourquoi les Pay-Bas et la France sont les seuls pays membres de l'Union européenne qui disposent d'une politique CVD entièrement établie.[2]

3. La politique CVD mise en place par le NCSC

6 En Suisse, le Centre National pour la Cybersécurité (NCSC) a mis en place une plateforme d'annonce de CVD,[3] accompagnée d'une feuille de bonnes pratiques destinée à orienter les WHH. Ces règles sont pour l'essentiel aussi pertinentes du point de vue du droit de la protection des données ; la présente feuille d'information est complémentaire et se concentre sur des aspects plus spécifiques de la protection des données.

III. Situation juridique des White Hat Hackers sous l'angle de la LPD

7 L'accès à un système informatique à travers l'exploitation d'une faille permet souvent d'avoir accès aux données qu'il contient. S'il s'agit de données personnelles, la loi fédérale sur la protection des données (LPD)[4] s'applique. Toute opération – consultation, téléchargement, communication, enregistrement, etc. – que le WHH entreprend avec ces données constitue un traitement au sens de la LPD (art. 5 let. d LPD). La LPD pose plusieurs principes essentiels que chaque personne traitant des données doit respecter, y compris les WHH.

[1] Governance von 0-Day-Schwachstellen in der deutschen Cyber-Sicherheitspolitik - Stiftung Wissenschaft und Politik (swp-berlin.org), p. 32, consulté le 25.05.2023.

[2] Governance von 0-Day-Schwachstellen in der deutschen Cyber-Sicherheitspolitik - Stiftung Wissenschaft und Politik (swp-berlin.org), pp. 33-34, consulté le 25.05.2023

[3] Coordinated Vulnerability Disclosure (CVD) (admin.ch), consulté le 25.05.2023.

[4] Dans la présente feuille d'information, lorsque la LPD est citée, il est fait référence à la nouvelle loi, qui entrera en vigueur le 1er septembre 2023.

8 A défaut de s'y conformer, et même s'ils correspondent à l'expression idéale du WHH, ils doivent être conscients que le traitement opéré est *a priori* illicite. Ci-dessous sont exposés certains des principes les plus pertinents en regard des activités des WHH :

- Le principe de la licéité (art. 6 al. 1 LPD) implique le respect des règles juridiques, y compris celles hors de la LPD : un traitement est illicite s'il enfreint une règle de droit. Ce principe se réfère évidemment au droit pénal (p. ex. les art. 138 ss ou 179 ss du Code pénal [CP]), mais plus largement à l'ensemble de l'ordre juridique (p. ex. l'interdiction de la tromperie ou de la menace selon les art. 28 ss du Code des obligations [CO]).

- Le principe de la bonne foi (art. 6 al. 2 LPD) vise le comportement général de la personne traitant les données. Pour le WHH, cela implique en particulier de ne pas avoir d'agenda caché et de ne pas chercher à nuire à l'exploitant du système ou aux personnes concernées (soit les personnes dont les données sont concernées). Aussi, il ne doit notamment pas adopter un comportement qui entraverait les efforts de l'exploitant pour combler les failles découvertes et ainsi (r)établir un état conforme aux exigences de la protection des données (p. ex. proférer des menaces, fixer des deadlines temporelles irréalistes, bloquer les systèmes, etc.).

- Suivant le principe de finalité (art. 6 al. 3 LPD), les données ne doivent pas être utilisées à des fins incompatibles avec les buts indiqués lors de leur collecte. Le fait que les données soient traitées par une personne tierce telle qu'un hacker, même bien intentionné, n'est *a priori* pas compatible avec les buts initiaux de la collecte et rend donc le traitement par principe illicite. Le WHH doit donc avant tout s'abstenir de traiter les données personnelles auxquelles il a accès.

- Le principe de proportionnalité (art. 6 al. 2 LPD) impose de ne pas faire plus que ce qui est nécessaire pour atteindre le but visé – en l'espèce diagnostiquer et documenter la faille (*proof of concept*). Aussi, si nonobstant l'illicéité probable de ce comportement, un WHH estime qu'il est malgré tout nécessaire d'accéder aux données elles-mêmes pour mener ses investigations, il devra limiter ses traitements au minimum nécessaire – que ce soit en regard de la quantité de données ou du type de traitement. Cela implique aussi qu'il ne devra pas conserver les données plus longtemps que nécessaire. La recommandation du NCSC de ne mener des traitements que sur son propre profil est ici particulièrement pertinente (cf. *supra* no 6).

- L'ensemble de ces principes interdisent aussi de communiquer les données exposées, ou de divulguer l'existence de la faille (hormis aux autorités de surveillance), sous peine de porter atteinte aux personnes concernées. Ainsi, une divulgation dans les médias avant que la faille n'ait été comblée est a priori incompatible avec ces principes (en particulier lorsque l'exploitant s'efforce de remédier à la faille le plus rapidement possible). De même, ces principes commandent au WHH d'informer l'exploitant dès que possible de ses découvertes et de lui laisser suffisamment de temps pour corriger les failles.

IV. Risques juridiques pour les White Hat Hackers

1. Risques sous l'angle du droit civil (not. art. 32 LPD)

9 L'activité du WHH pouvant l'amener à enfreindre les principes évoqués ci-dessus, elle l'expose à des prétentions civiles de la part de l'exploitant du système ou des personnes concernées. S'il agit de bonne foi et limite ses traitements au minimum – autrement dit, s'il adopte un comportement de WHH idéal et tend au respect des principes de la LPD –, l'on peut supposer qu'il n'y aura cependant pas de réel intérêt à agir en justice : lorsque l'exploitant ou les personnes concernées seront informées de la faille, le WHH aura déjà supprimé les données éventuellement collectées ou sera sur le point de le faire ; elles n'auront pas non plus subi de dommage économique ou réputationnel, puisque le WHH n'aura pas divulgué d'information ; etc.

10 Un risque d'action civile ne peut être exclu – le choix appartient à l'exploitant et aux personnes concernées –, mais le fait d'adopter un comportement de WHH idéal minimisera ce risque.

2. Risques sous l'angle du droit pénal (not. art. 143, 143bis et 179^{novies} CP)

11 Parallèlement aux risques civils, le WHH s'expose à des risques de poursuite pénale, notamment fondés sur les art. 143, 143bis et 179^{novies} CP. Certains des comportements visés par ces articles sont par définition incompatibles avec un WHH (art. 143 al. 1 CP p. ex., où le hacker vise un enrichissement). D'autres infractions peuvent être commises même si le hacker se comporte de manière idéale (notamment art. 143bis al. 1 et 179^{novies} CP). Ces dernières infractions n'étant *a priori* poursuivies que sur plainte, les considérations faites en lien avec la mitigation des risques d'actions civiles s'appliquent ici également.

12 De surcroît, en présence de soupçon fondé d'infractions poursuivies d'office (soit même en l'absence de plainte), le personnel du PFPDT a une obligation de dénoncer (art. 22a de la loi sur le personnel de la Confédération [LPers]).

3. Risques sous l'angle du droit administratif (PFPDT ; art. 49 ss LPD)

13 Lorsqu'il traite des données, le WHH peut devenir lui-même un responsable de traitement au sens de la LPD. Aussi, si son comportement paraît problématique du point de vue de la LPD, en particulier s'il apparaît que le hacker n'a pas cherché à se conformer aux principes évoqués ci-dessus, le PFPDT peut être amené à ouvrir une enquête et à prononcer des mesures administratives à l'encontre du WHH lui-même (art. 49 ss LPD).

V. Rôle du PFPDT

14 Une annonce au PFPDT par le WHH n'est pas obligatoire et n'est d'ailleurs pas spécialement prévue par la LPD (à l'inverse du responsable du traitement, qui est tenu d'annoncer lorsqu'une faille entraîne un risque élevé pour les personnes concernées, notamment quand il est à craindre que celle-ci ait été exploitée ; cf. art. 24 LPD). Si une annonce est néanmoins envisagée, plusieurs éléments sont à considérer :

- Comme dit plus haut (cf. *supra* no 12), en présence de soupçon fondé d'infractions poursuivies d'office (soit même en l'absence de plainte : ex. art. 143 al. 1 CP), le personnel du PFPDT a une obligation de dénoncer (art. 22a LPers).

- En cas d'indices suffisants d'une violation des dispositions de protection des données, le PFPDT peut ouvrir une enquête (art. 49 ss LPD) contre le responsable du traitement au sens de l'art. 5 lit. j LPD (p. ex. l'exploitant du système). Si des dispositions de protection des données sont violées, il peut ordonner des mesures administratives pour remédier aux risques (cf. art. 51 al. 3 LPD). Cela étant, une annonce au PFPDT ne paraîtra pas toujours opportune. Si la faille ne résulte pas d'une négligence crasse, qu'il n'y a pas d'indice qu'elle ait été exploitée et que le l'exploitant du système y remédie à satisfaction, l'ouverture d'une enquête peut s'avérer superflue.

- Notons enfin que le PFPDT peut être amené à ouvrir une enquête (art. 49 ss LPD) contre le hacker lui-même. Il est également précisé que le PFPDT n'offre pas non plus la garantie d'anonymat au WHH – même si une divulgation du nom par le PFPDT s'effectuera toujours avec un but précis et dans le cadre de la loi.