Droit et Divulgation de Vulnérabilité

Université de Rennes 1
Master en Cybersécurité

Elvin Maubert, Baptiste Le Piouf, Luca Pourceau

16 Mai 2025

Résumé

Ce livre blanc examine le cadre juridique de la divulgation de vulnérabilités dans un contexte où la cybersécurité constitue un enjeu national et international majeur. Bien que la divulgation soit essentielle pour la protection des systèmes d'information, elle expose les chercheurs en cybersécurité à des risques juridiques significatifs, notamment en l'absence d'autorisations explicites. Ce travail analyse les enjeux techniques, éthiques et juridiques liés à cette pratique en explorant les méthodes d'anonymisation, les politiques de divulgation publique et privée, ainsi que les obligations légales imposées aux chercheurs. La deuxième partie se concentre sur les implications du droit pénal français, notamment les articles 323-1 à 323-8 du Code pénal, qui encadrent les risques encourus lors de la divulgation. En confrontant les aspects pratiques et les contraintes juridiques, ce livre blanc propose des pistes pour renforcer la sécurité juridique des chercheurs tout en soutenant les bonnes pratiques de divulgation.

Abstract

This white paper examines the legal framework surrounding vulnerability disclosure in a context where cybersecurity is a critical national and international issue. Although disclosure is essential for the protection of information systems, it exposes cybersecurity researchers to significant legal risks, particularly in the absence of explicit authorization. This work analyzes the technical, ethical, and legal challenges associated with this practice by exploring anonymization methods, public and private disclosure policies, and the legal obligations imposed on researchers. The second part focuses on the implications of French criminal law, particularly Articles 323-1 to 323-8 of the Penal Code, which govern the risks associated with disclosure. By comparing practical aspects and legal constraints, this white paper proposes ways to enhance legal security for researchers while promoting best practices in disclosure

Table des matières

Introduction

Chaque jour, des failles de sécurité critiques sont découvertes dans les systèmes informatiques que nous utilisons. Certaines sont rendues publiques, d'autres gardées secrètes, et beaucoup sont corrigées dans l'ombre, parfois sans qu'on sache par qui, ni comment. Pourtant, derrière chaque faille signalée se trouve une personne ou une équipe confrontée à un dilemme : comment divulguer une vulnérabilité sans se mettre en danger ? En 2024, c'est plus de 40 000 vulnérabilités qui ont été recensées dans la base CVE, soit une hausse de 38 % en 1 an. Mais combien de failles, bien que découvertes, restent dans l'ombre, par crainte de poursuites judiciaires ou à cause d'un cadre légal trop ambigu ? C'est toute la complexité et l'importance de la divulgation de vulnérabilités.

Dans un environnement où la cybersécurité représente un enjeu national et international, la divulgation des vulnérabilités devient cruciale pour le monde du numérique. Ce geste pourtant généreux et de bonne volonté peut néanmoins avoir des conséquences légales sévères pour les chercheurs en l'absence d'autorisations et de directives précises. Entre les incompréhensions juridiques, les responsabilités peu claires et des pratiques de sécurité à la limite du légitime, la divulgation reste un domaine délicat mêlant l'aspect éthique, juridique et technique.

L'objectif de ce livre blanc est donc de proposer une analyse de ces multiples aspects en associant les processus techniques au cadre juridique. Il est destiné aussi bien aux chercheurs en cybersécurité qu'aux juristes, aux entreprises et aux autorités publiques. Certains termes utilisés dans ce livre blanc peuvent prêter à confusion. Ils sont définis ici pour clarifier leur usage. Le signalement désigne l'acte de transmettre l'existence d'une vulnérabilité à une autorité ou une entité concernée. La divulgation, quant à elle, englobe plus généralement le processus du signalement, qui implique une mise à disposition plus large de l'information, qu'elle soit publique ou privée. Enfin, la déclaration renvoie à une obligation légale de notifier certaines vulnérabilités, souvent imposée à des éditeurs de logiciels.

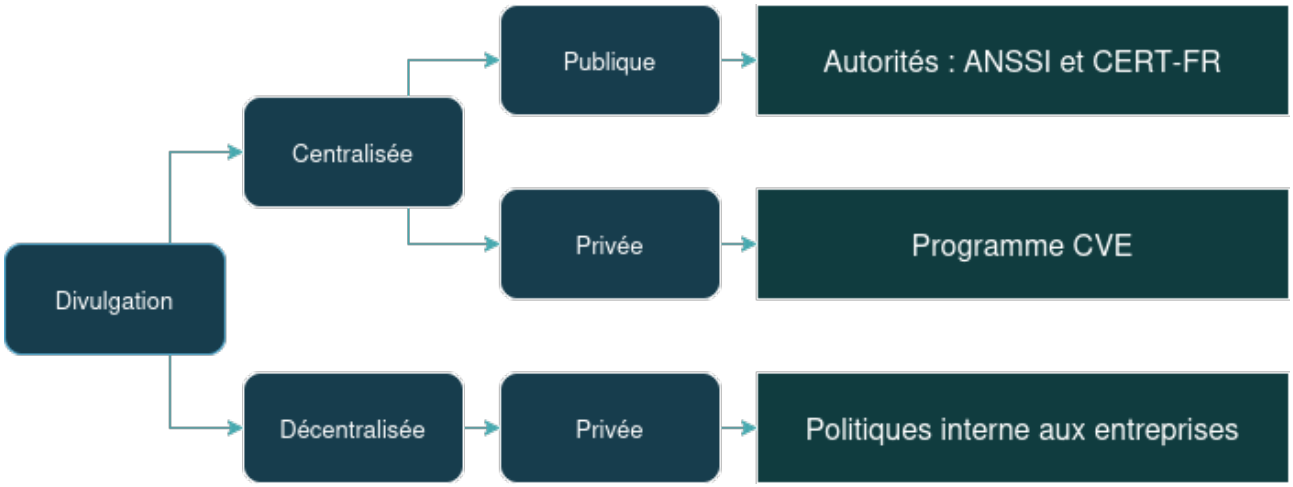
La première partie s'intéresse aux aspects pratiques et techniques du processus de divulgation. Elle commence par une exploration des différentes méthodes d'anonymisation utilisées par les chercheurs, à partir de la recherche jusqu'à la transmission d'une documentation technique. Elle se poursuit sur les principales structures, publiques comme l'ANSSI et le CERT-FR, ou

internationales comme les CNAs du programme CVE, qui permettent un accompagnement et une centralisation des divulgations. Enfin, elle analyse la manière dont les politiques internes aux entreprises, bien que sans valeur juridique, influencent le processus de divulgation des chercheurs tout en définissant une limite aux opérations sur leurs systèmes d'informations.

Dans un second temps, la seconde partie explore le cadre juridique qui entoure la divulgation de vulnérabilités en France. Elle met d'abord en avant les risques encourus par les chercheurs en sécurité lorsqu'ils agissent dans l'objectif de trouver des vulnérabilités. En effet, un chercheur se doit potentiellement de s'introduire sur des systèmes sans autorisation lors de sa recherche. Il est donc primordial d'analyser ce qu'en dit le droit français. Pour ce faire, il est nécessaire de bien comprendre quelles peines peuvent s'appliquer à des chercheurs lors de leurs activités et de comprendre comment fonctionne le droit lorsqu'il doit qualifier une infraction. Enfin, il est important d'aborder le fonctionnement de la responsabilité qui peut varier en fonction de si le chercheur agit seul ou dans un cadre professionnel.

1 Les coulisses de la divulgation des vulnérabilités

Lorsqu'un chercheur en cybersécurité identifie une faille, plusieurs circuits de divulgation s'offrent à lui. Ces circuits peuvent être classés selon leur degré de centralisation. Comme l'explique Teodora Curelariu, doctorante en Droit international public[1], trois grandes approches existent aujourd'hui dans le domaine de la divulgation en cybersécurité.



La première est celle de la centralisation publique, où la vulnérabilité est transmise à une autorité, principalement l'ANSSI ou le CERT-FR en France. L'État devient alors l'intermédiaire entre le chercheur et l'entité concernée. Cet échange est (souvent) encadré par un cadre légal, visant à protéger le chercheur (lorsqu'il agit de bonne foi) tout en assurant un accompagnement et une confidentialité du signalement.

La seconde approche repose sur une centralisation privée, où la vulnérabilité est remontée à une structure non gouvernementale, tel que les CNAs dans le cadre du programme CVE. Ces acteurs assurent la gestion et le recensement des failles selon des procédures standardisées.

Enfin, une troisième approche correspond à la décentralisation des divulgations. Ici, le chercheur contacte directement l'entité vulnérable sans passer par un intermédiaire. Cette approche repose sur les politiques de divulgation propres à chaque entreprise mais ne garantissant aucune protection juridique.

Ces trois approches reposent sur différentes logiques de confiance, de responsabilité et de gestion du risque dans le processus de divulgation.

Avant de présenter les différentes méthodes pour faire remonter une vulnérabilité, l'anonymisation doit faire l'objet d'une présentation détaillée. Divulguer une vulnérabilité peut se faire

[1] Curelariu, *Défis juridiques de la divulgation des vulnérabilités*.

par plusieurs moyens, impliquant plus ou moins d'acteurs, et avec un certain degré de responsabilité et de risque. En effet, face à la défiance plus ou moins justifiée envers les acteurs de la cybersécurité, l'anonymisation est un processus permettant de préserver son identité et garantir une divulgation de vulnérabilité sans répression. Que ce soit par une autorité publique ou un programme privé, le recensement centralisé ou décentralisé offre une meilleure communication dans l'ensemble de la communauté cyber. Cependant, certaines procédures dépendamment du moyen de divulgation entraînent certains risques pour les chercheurs.

Dans le cadre d'une divulgation de vulnérabilité, l'anonymisation est un processus essentiel à maîtriser aujourd'hui. (1.1). Dans le cadre d'une centralisation par des organismes publics des vulnérabilités, une procédure existe visant à garantir l'anonymat d'une personne auprès de l'ANSSI (1.2) ou auprès du CERT-FR (1.3). Cependant, il existe également une centralisation d'organismes privés auprès d'organismes comme l'organisation MITRE dans le cadre des CVE (1.4). Enfin, une dernière option, peu répandue aujourd'hui mais dont l'intérêt est certain : une décentralisation de vulnérabilité avec les politiques de divulgation des entreprises (1.5).

1.1 Anonymiser une divulgation de vulnérabilité

L'anonymisation dans un domaine aussi délicat que la divulgation de vulnérabilité est un acte stratégique qui reflète un choix mûrement réfléchi entre protection personnelle et reconnaissance professionnelle. D'un côté, préserver son anonymat permet d'éviter tout risque de représailles, qu'elles soient légales ou personnelles, et de focaliser l'attention sur la faille elle-même plutôt que sur l'auteur de la divulgation. De l'autre, rendre son identité publique constitue une marque d'honnêteté et de transparence, valorisant le chercheur dans son parcours professionnel aux yeux de la communauté.

Il est important, avant toute divulgation, de trouver un équilibre entre le risque encouru par les auteurs de la divulgation et le bénéfice attendu d'une divulgation publique et transparente. Dans un contexte juridiquement instable, le degré d'anonymisation reflète un choix relativement éclairé dont dépend la légitimité et l'impact de la divulgation. Cet anonymat peut représenter un choix, une recommandation ou une nécessité, selon les circonstances de la découverte de la vulnérabilité. Lorsqu'une faille touche des infrastructures critiques ou sensibles sans autorisation explicite d'accès, l'anonymisation devient fortement recommandée. À l'in-

verse, dans des contextes plus ouverts et collaboratifs, la reconnaissance publique peut devenir un atout essentiel pour construire sa réputation, prouver son expertise et obtenir une crédibilité professionnelle.

1.1.1 Rompre les liens d'identification

S'anonymiser lors de la divulgation d'une vulnérabilité ne consiste pas uniquement à adopter un pseudonyme [2]. Il s'agit d'un processus global qui vise à éliminer tout lien identifiable entre la personne qui découvre la faille et les informations qui seront rendues publiques ou transmises à des tiers. Ce processus d'anonymisation repose sur 3 principes : la prudence durant la phase de recherche, la suppression de toute information technique dans les preuves fournies, et l'utilisation de canaux de divulgation anonymes. Chacune de ces étapes est d'une grande importance dans la préservation de l'anonymat, un moindre détail peut suffire à remonter, même involontairement, jusqu'à l'auteur.

1.1.2 Protéger son anonymat pendant la recherche

Lors de la phase de recherche, l'objectif est d'éviter que le système d'information ciblé conserve des traces pouvant être reliées à l'identité du chercheur. Pour cela, il est courant de masquer son adresse IP réelle à l'aide de techniques de routage réseau. Une adresse IP peut être reliée à un fournisseur d'accès, un lieu géographique, voire à une session d'activité spécifique dans les logs, ce qui constitue une donnée identifiable. L'utilisation d'un réseau privé virtuel (ou "VPN" pour "*virtual private network*") permet par exemple de rediriger le trafic Internet via un serveur distant, chiffrant également les communications et camouflant l'adresse IP réelle par celle du serveur VPN.

Pour améliorer le niveau de confidentialité, il est fréquent de passer par des réseaux plus complexes et sécurisés comme Tor[3], qui font passer les données à travers plusieurs serveurs chiffrés, rendant alors l'identification de l'auteur plus difficile. Ces approches sont souvent accompagnées par l'utilisation de systèmes d'exploitation conçus pour la sécurité et pour l'anonymat, tels que Tails ou Whonix, qui fonctionnent comme des programmes en mémoire, sans laisser de trace sur un ordinateur et sur internet de par l'utilisation systématique d'outils d'anonymisation tel que Tor. Ces outils, bien que parfaitement légaux dans leur utilisation légitime, souffrent d'une

[2] Ce dernier constituant un processus réversible et identifiant

[3] Project, *Tor Project*.

mauvaise réputation par la communauté juridique. Tor notamment, est particulièrement associé à une utilisation malveillante comme la navigation sur le dark web. Au contraire, dans la communauté informatique, Tor est avant tout un outil légitime de préservation de la vie privée, garantissant la confidentialité et la sécurité des utilisateurs dans un milieu à haut risque.

1.1.3 Les preuves techniques, un nid d'information

Dans le processus global d'une divulgation de vulnérabilité, la documentation de celle-ci est de plus en plus préconisée. Elle est constituée principalement de rapports PDF, de fichiers de logs, de captures d'écran, ainsi que d'archives contenant des éléments techniques annexes (scripts, extraits de bases de données, dumps mémoire, etc.). Ces documents ont pour objectif de structurer la preuve, de détailler l'exploitation de la faille, et de guider l'entité vulnérable dans une correction efficace.

Destinée à l'entité vulnérable pour démontrer la faille, la documentation peut cependant introduire des informations pouvant compromettre l'identité du chercheur. Les captures d'écrans, les fichiers de logs ou encore les rapports techniques contiennent souvent des métadonnées invisibles sur le rendu standard du document. Un fichier PDF peut enregistrer l'identifiant de l'auteur, la version du logiciel utilisé ou même le nom de l'ordinateur[4]. Une simple capture d'écran peut révéler l'heure exacte de la prise, les détails du système ou des éléments d'environnement propres à un utilisateur. Les fichiers de logs, quant à eux, peuvent contenir des timestamps (indice d'horodatage) pouvant être associés à d'autres activités détectées sur le système d'information vulnérable.

Chaque type de fichier supporte ainsi des risques spécifiques de fuite d'informations rendant l'anonymisation encore plus consciencieuse. Il est donc important d'analyser, voire d'éliminer systématiquement toutes les métadonnées avant la divulgation, afin d'éviter toute identification parallèle aux activités passées.

1.1.4 Assurer une divulgation anonyme

Pour conserver son anonymat au moment de la divulgation, il est préférable d'éviter le simple recours à un pseudonyme, qui peut être réutilisé ou correspondre à d'anciennes activités. Les

[4] Adobe, *Suppression de contenu confidentiel dans les fichiers PDF*.

divulgations se faisant dans la plupart des cas par mail, l'utilisation d'une simple adresse mail peut mettre un terme à cette stratégie si elle est associée à des informations personnelles. Il est donc conseillé de posséder ou de créer une adresse e-mail indépendante, voire temporaire. Certaines plateformes comme ProtonMail ou Tutanota, en plus de leur politique de non-conservation des logs, permettent l'échange de mails chiffrés sans authentification liée à une identité réelle. Lorsque la vulnérabilité présente une certaine sensibilité comme des systèmes critiques ou gouvernementaux, certaines autorités de sécurité comme l'ANSSI ou le CERT-FR mettent à disposition des clés PGP. L'utilisation de PGP permet de chiffrer les envois de messages et garantit leur authenticité tout en assurant que seul le destinataire propriétaire de cette clé pourra accéder au contenu.

En résumé, l'anonymisation lors d'une divulgation de vulnérabilité est une démarche autant technique que stratégique. Malgré une méthodologie rigoureuse, il peut subsister un risque résiduel de correspondance involontaire entre une activité virtuelle et une identité réelle. L'anonymisation repose sur une suite de bonnes pratiques, mais un simple oubli, une métadonnée négligée ou une activité mal dissimulée peut suffire à compromettre l'ensemble de la démarche. Cela appuie sur le fait que l'anonymisation est un processus exigeant, nécessitant une prudence constante et rigoureuse, et notamment dans un cadre juridique instable. Ce dernier prévoit d'ailleurs la possible conservation de l'anonymat par l'Agence Nationale de la sécurité des systèmes d'information.

1.2 L'ANSSI, autorité nationale en cybersécurité

La transparence et l'honnêteté, un état d'esprit au premier abord contradictoire à l'anonymisation, mais grandement utile pour montrer une image de bienveillance à l'entité et prouver sa bonne foi lors de la divulgation.

L'Agence nationale de la sécurité des systèmes d'information (ou "ANSSI") est l'autorité nationale en matière de cybersécurité et de cyberdéfense en France. Créée en 2009, elle est placée sous l'autorité du Secrétariat général de la défense et de la sécurité nationale (SGDSN) . Ses missions principales incluent la protection des systèmes d'information sensibles de l'État, des opérateurs d'importance vitale (OIV) et, plus généralement, des entités stratégiques françaises[5].

[5]ANSSI, *Histoire et modèle*.

1.2.1 Rôle dans la divulgation de vulnérabilités

Dans le contexte de la divulgation de vulnérabilités, l'ANSSI joue un rôle d'accompagnement dans la gestion d'incidents et de vulnérabilités au sein d'une entité victime. Elle est également chargée de communiquer les vulnérabilités signalées aux entités concernées, afin d'aider à la correction de ces failles. Cette centralisation publique des vulnérabilités est une source fiable et de confiance au sein de la population. Elle permet à la fois aux sociétés utilisant des ressources et outils numériques d'être accompagnées et informées sur l'actualité de la cybersécurité en France et par la même occasion d'informer les utilisateurs potentiellement concernés par une divulgation de leur vie privée.

1.2.2 Cadre juridique et protection du signalant

Du côté des chercheurs, l'ANSSI offre une protection juridique qui offre une protection nuancée dans le cadre de la divulgation de vulnérabilité.. L'article L.2321-4 du Code de la défense prévoit que toute personne découvrant une vulnérabilité peut la signaler à l'ANSSI sans être tenue de la déclarer au procureur de la République, à condition que ce signalement soit effectué de bonne foi. Autant en juridique qu'en informatique, la notion de "bonne foi" n'est pas explicitement définie dans la législation. Elle est globalement interprétée comme une absence d'intention malveillante dans le respect de l'intérêt général et est appréciée par l'ANSSI, qui pourrait déclarer l'infraction au procureur à son bon vouloir. Ce jugement peut notamment se baser sur les méthodes utilisées pour accéder au système, sur la potentielle réalisation d'attaques de type déni de service, ou encore sur la conservation de données confidentielles ou le maintien non autorisé dans le système d'information.

Dans le cas où le chercheur choisit de ne pas anonymiser sa divulgation, l'ANSSI est légalement obligée de garder son identité confidentielle et de ne pas signaler au Procureur de la République la commission d'un crime ou d'un délit, comme précisé dans l'article L.2321-4 : "L'autorité préserve la confidentialité de l'identité de la personne à l'origine de la transmission". Cette protection demeure tant qu'aucune poursuite judiciaire n'est engagée. En revanche, si le procureur décide d'ouvrir une enquête après une plainte déposée par une entreprise concernée , l'identité du chercheur, s'il ne s'est pas anonymisé lui-même, pourrait alors être transmise aux autorités judiciaires dans le cadre de la procédure. Même si l'ANSSI ne transmet pas l'identité du chercheur au Procureur, l'entité concernée par la vulnérabilité peut de son côté, décider de

porter plainte si elle estime avoir subi un préjudice. La protection offerte par l'article L.2321-4 ne constitue donc pas une immunité totale, mais elle représente un cadre favorable pour les chercheurs agissant de manière bienveillante et responsable. Par conséquent, la confidentialité est garantie par défaut, mais demeure nuancée dans le cadre de potentielles poursuites.

Paradoxalement, l'ANSSI dispose d'un centre d'alerte permettant de signaler les vulnérabilités.

1.3 Le CERT-FR, point d'entrée pour les signalements

Le CERT-FR (Centre gouvernemental de veille, d'alerte et de réponse aux attaques informatiques) est le centre national de réponse aux incidents de sécurité informatique en France, rattaché à l'ANSSI. Il assure une veille constante sur les menaces émergentes et coordonne les actions nécessaires pour protéger les systèmes d'information des organismes publics et des opérateurs d'importance vitale (OIV). Cette mission inclut la réception et le traitement des signalements de vulnérabilités, permettant une réaction rapide et efficace face aux menaces identifiées. Il joue un rôle essentiel dans la coordination entre les chercheurs en sécurité, les entités concernées par des vulnérabilités et l'État.

En tant que bras opérationnel de l'ANSSI, le CERT-FR est chargé de la détection, de l'analyse et de la réponse aux incidents de cybersécurité. Il est le point d'entrée des signalements sous l'autorité de l'ANSSI, c'est donc à lui que revient ce rôle essentiel de communication entre les chercheurs en sécurité et les entités concernées par des vulnérabilités.

1.3.1 Procédure de signalement

Pour divulguer une vulnérabilité au CERT-FR en tant que chercheur, la seule méthode, du moins la plus recommandée, est de passer par courriel (cert-fr@ssi.gouv.fr), avec une possibilité supplémentaire de chiffrer l'échange grâce à la clé PGP publique. Bien qu'un formulaire en ligne soit également présent sur le site du CERT-FR, celui-ci est destiné aux éditeurs de logiciels concernés par l'article L.2321-4-1 du Code de la défense.

Le contenu de la divulgation n'est pas strictement défini, mais selon l'article L.2321-4, il doit être suffisamment complet pour que l'ANSSI puisse "procéder aux opérations techniques strictement nécessaires à la caractérisation du risque ou de la menace [...] aux fins d'avertir l'hébergeur, l'opérateur ou le responsable du système d'information." Autrement dit, l'ANSSI

se réserve le droit d'approuver l'existence de la vulnérabilité en procédant aux opérations techniques comme indiqué dans le signalement qui mènerait à cette vulnérabilité. Ainsi, bien que le format ne soit pas normalisé, il est courant de fournir un rapport détaillé, des preuves d'attaques, des logs, des captures d'écran, etc.

La procédure de signalement semble donc encadrée de manière à exiger un minimum de rigueur technique et de transparence, à travers la qualité des éléments transmis. Cette exigence permet à l'ANSSI non seulement de confirmer la réalité de la vulnérabilité, mais surtout d'apprécier la bonne foi du chercheur, en évaluant à la fois la pertinence des informations fournies, l'intention perçue et l'absence de comportement malveillant.

1.3.2 Coopération internationale

Membre du réseau international FIRST (Forum of Incident Response and Security Teams), le CERT-FR collabore avec d'autres équipes de réponse aux incidents à travers le monde. Cette coopération permet un échange d'informations sur les menaces et les vulnérabilités, renforçant ainsi la sécurité des systèmes d'information au niveau global. En cas de signalement concernant une entité étrangère, le CERT-FR peut transmettre le signalement à son homologue compétent dans le pays en question . Le CERT-FR peut également être amené à coopérer avec des entités similaires homologuées compétentes d'autres pays si le signalement impacte non seulement une entité française mais aussi une entité internationale.

1.4 CVE : L'encyclopédie mondiale des failles de sécurité

Fondé par l'organisation à but non lucratif MITRE et soutenue par le Département de la Sécurité Intérieure des États-Unis, le programme international Common Vulnerabilities and Exposures (CVE) vise à recenser de façon centralisée et unifiée les vulnérabilités touchant tous les logiciels, matériels et systèmes. Ce processus est d'une importance capitale. En effet, un grand nombre d'acteurs du secteur informatique peuvent ainsi collaborer afin de sécuriser leurs produits et protéger à la fois leurs propres intérêts et ceux de leurs utilisateurs en recensant et catégorisant les failles avant qu'elles ne soient rendues publiques, ce qui assure un équilibre entre sécurité et transparence. Cela permet d'éviter l'exploitation de failles critiques avant qu'un correctif ne soit disponible, tout en informant rapidement les utilisateurs. Ainsi, chaque vulnérabilité recensée dans la base CVE se voit attribuer un identifiant unique, qui permet aux entreprises, organismes de recherche et professionnels de la cybersécurité de dialoguer autour

de celle-ci, d'apporter les patchs et de se renseigner sur des risques potentiels.

1.4.1 Une organisation hiérarchisée

Le programme suit une hiérarchie bien précise qui est résumée sur le schéma suivant figure 1[6].

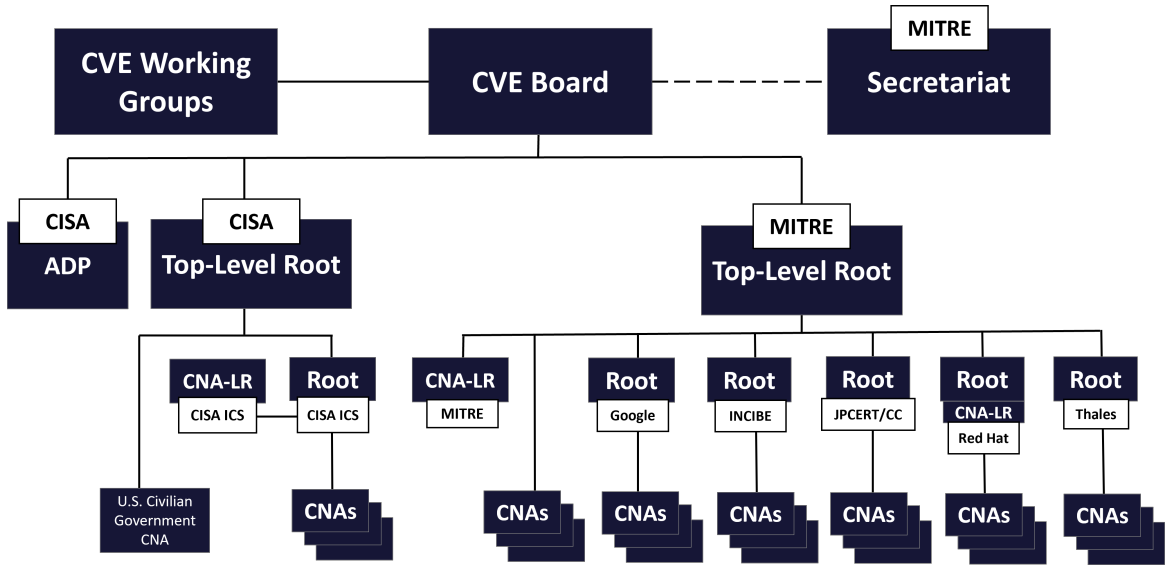


FIGURE 1 : Structure du programme CVE

Cette organisation permet de diviser les fonctions opérationnelles et de gestion en plusieurs entités ayant leurs propres portées. Au sommet on y retrouve trois entités :

- **CVE Board** : Supervise le programme CVE pour répondre aux besoins mondiaux en matière d'identification des vulnérabilités. Il regroupe des membres issus de divers secteurs : entreprises de cybersécurité, institutions académiques, agences gouvernementales, experts en sécurité et utilisateurs finaux d'informations sur les vulnérabilités.

- **Secrétariat** : Organisation mandatée par le programme CVE pour développer, héberger et maintenir l'infrastructure du programme, et fournir un soutien administratif et logistique au CVE Board, aux groupes de travail et aux autres composantes du programme.

- **CVE Working Groups** : Organisation créée par le CVE Board pour atteindre des objectifs spécifiques par la collaboration avec les parties prenantes du programme CVE et, si nécessaire, avec le public.

[6]CVE PROGRAM, *Program Organization Structure*.

Ensuite les rôles sont répartis sous la forme d'un arbre, composé de racines (les "Roots"), Top-Level Roots (TL-Roots), CVE Numbering Authoritiess (CNAs) et CVE Numbering Authorities of Last Resort (CNA-LR) ayant respectivement les compétences suivantes :

- **Top-Level Root** : C'est le niveau de gestion le plus élevé au sein d'une branche. Il rend compte au CVE Board et est responsable de la gouvernance et de l'administration de sa propre hiérarchie qui doit comprendre une CNA-LR et au minimum une CNA et un Root.
- **Root** : Assure les fonctions de gestion au sein de la hiérarchie qui lui sont délégués par le TL-Root dans une portée spécifique. Responsable, du recrutement, de la formation et de la gouvernance d'une ou plusieurs CNA, CNA-LR, ou d'autres Roots.
- **CNA (CVE Numbering Authority)** : Exécute les fonctions opérationnelles d'assignation d'identifiants CVE et de publication des enregistrements de vulnérabilités.
- **CNA of Last Resort (CNA-LR)** : Intervient lorsqu'aucune autre CNA n'est en mesure de traiter une vulnérabilité donnée.

Pour finir il existe un rôle particulier qui est endossé par la Cybersecurity and Infrastructure Security Agency (CISA), celui de Authorized Data Publishers (ADP)[7]. Il permet à cette entité d'agrémenter le contenu d'une CVE en y ajoutant des informations complémentaires comme le score Common Vulnerability Scoring System (CVSS)[8] qui mesure le niveau de risque associé à une faille, la décision issue du processus Stakeholder-Specific Vulnerability Categorization (SSVC) donnant une priorité aux correctifs à apporter aux différentes vulnérabilités[9] et les informations issues de la base de données Known Exploited Vulnerabilities (KEV)[10] permettant de connaître des cas d'utilisation réels de la faille. Toutes ces informations sont ajoutées dans une parties spécifiques et distinctes des données fournies par la CNA.

Comme il est possible de le voir avec la figure 2, bien que le programme existe depuis 1999, le nombre de CVE publiées n'a pas dépassé les 8000 jusqu'en 2016. Cependant, ce nombre a plus que doublé en 2017 et ne cesse d'augmenter depuis pour atteindre un record de 40,077 publications l'année passée. Ceci peut s'expliquer par la décision du programme d'étendre activement

[7]CVE Program, *Authorized Data Publisher (ADP)*.
[8]FIRST, *Common Vulnerability Scoring System (CVSS)*.
[9]CISA, *Stakeholder-Specific Vulnerability Categorization (SSVC)*.
[10]CISA, *Known Exploited Vulnerabilities Catalog (KEV)*.

le nombre de CNA en 2016[11].

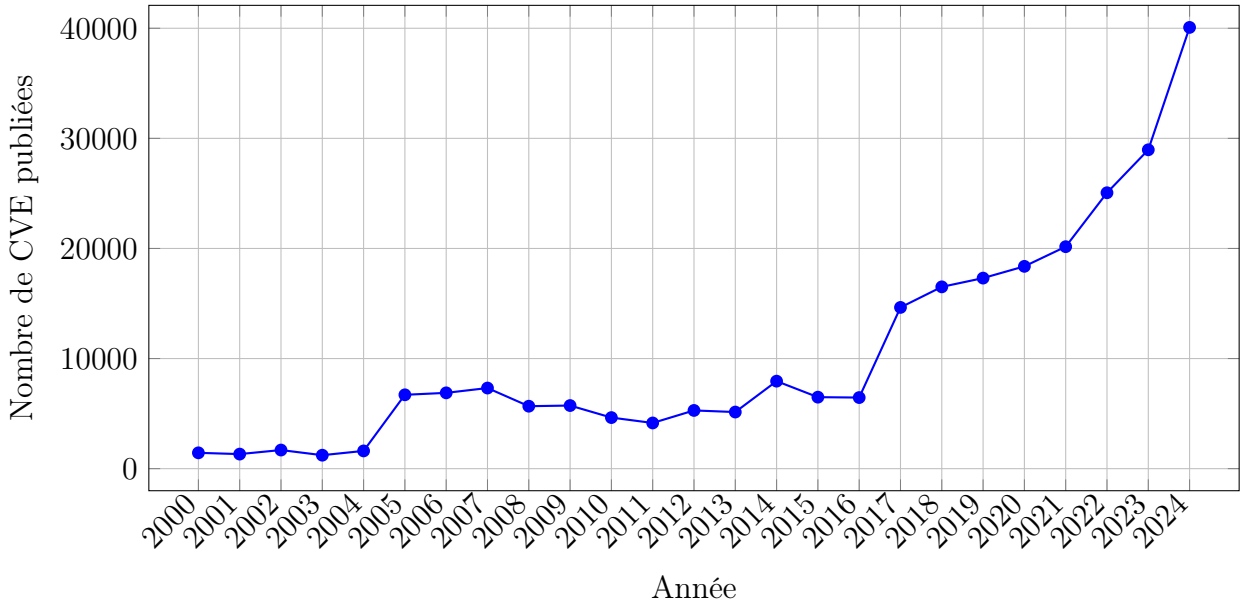


FIGURE 2 : Évolution annuelle du nombre de CVE publiées entre 2000 et 2024

1.4.2 CNAs : Les gardiens des vulnérabilités

Les CNA sont des organisations chargées d'attribuer des identifiants CVE. Ces entités, accréditées par la fondation MITRE, constituent le cœur du programme : elles valident, documentent et attribuent des numéros CVE aux vulnérabilités qui leur sont rapportées. La nature des CNAs peut être variée : éditeurs de logiciels (ex : Microsoft, Google), Computer Emergency Response Team (CERT), entreprises de cybersécurité ou encore chercheurs. Ces acteurs du programme CVE ne signent pas de contrat avec MITRE, ils peuvent candidater depuis le site cve.org afin d'être recontactés à ce sujet. Ils reçoivent alors un formulaire d'enregistrement à remplir avec des informations générales sur l'entreprise comme le nom, le pays d'origine, leurs secteurs d'activité, mais aussi des données prévisionnelles comme le nombre d'identifiants CVE nécessaires par an, qui sert uniquement de statistique pour le programme, l'étendue des produits qui serait sous leurs responsabilités ou encore leur politique de divulgation. Ensuite si les candidats respectent tous les exigences, à savoir disposer d'une politique publique de divulgation de vulnérabilités , disposer d'une source publique pour la divulgation de nouvelles vulnérabilités et accepter les "CVE terms of use", alors ils sont intégrés au programme. Ils sont également amenés à regarder des vidéos expliquant le fonctionnement du programme, le processus d'assignation des CVEs ou

[11]CVE PROGRAM, *About CVE - History*.

encore le suivi des correctifs à apporter[12]. Il n'existe aujourd'hui ni frais pour la candidature ou l'intégration finale, ni participation annuelle au programme. De même l'organisation MITRE ne rémunère pas les CNAs, elles gèrent elles-mêmes cette logistique supplémentaire pour leur propre bénéfice. Ils sont détaillés sur le site du programme comme étant les suivants[13] :

- **Renforcer la crédibilité** : Démontrer des pratiques de gestion des vulnérabilités matures et un engagement fort en cybersécurité, auprès des clients actuels et potentiels.
- **Valoriser l'information** : Fournir à la clientèle des informations enrichies et fiables sur les vulnérabilités.
- **Maîtriser la publication** : Contrôler le calendrier et le processus de publication des CVE pour les vulnérabilités relevant du périmètre de l'entreprise.
- **Protéger les données sensibles** : Assigner des identifiants CVE sans devoir partager d'informations confidentielles avec d'autres CNAs.
- **Optimiser les processus** : Rationaliser et accélérer la divulgation des vulnérabilités.

Cependant les CNA ne publiant pas au moins une CVE tous les six mois sont considérées comme inactive et, sauf justification, risque l'exclusion du programme CVE. Tous ces acteurs sont les moteurs du programme CVE et le nombre de publications annuelles montre qu'ils répondent à un besoin croissant. La figure 3 confirme la volonté d'expansion de l'écosystème CVE, il existe actuellement 453 CNA partenaires du programme et près de 90% d'entres eux l'ont rejoint après 2016.

Laquelle choisir ? Peut-on se tromper ?

Le choix d'une CNA se fait généralement en fonction de la nature de la vulnérabilité identifiée. S'il s'agit d'un produit d'un éditeur reconnu, le chercheur doit alors contacter directement la CNA concernée, la plupart du temps l'éditeur lui-même. La portée de chacune est indiquée sur le site cve.org[14]. Si aucune CNA n'est désignée pour le produit la vulnérabilité peut être soumise à une des trois CNA-LR suivantes qui agissent en tant que CNA par défaut :

[12]CVE Program, *CNA Onboarding Resources*.
[13]CVE Program, *CVE Terms of Use*.
[14]CVE Program, *List of Partners*.

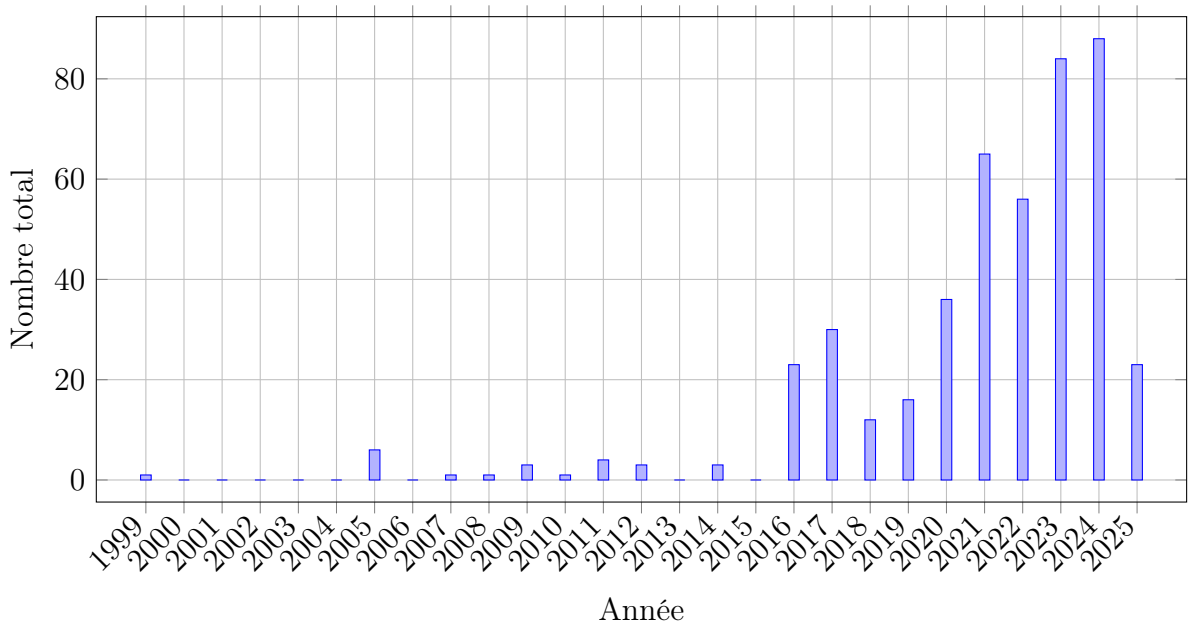


FIGURE 3 : Évolution du nombre de CNA ajoutées par années

- **Cybersecurity and Infrastructure Security Agency (CISA)**

  La CISA est une agence américaine spécialisée dans la protection des infrastructures critiques contre les cybermenaces, incluant les systèmes de contrôle industriels (ICS) et les dispositifs médicaux.

  - Couvre les vulnérabilités :
    - Signalées à CISA ou observées par CISA.
    - Affectant les systèmes de contrôle industriels (ICS) ou les dispositifs médicaux.
    - Non couvertes par le périmètre d'un autre CNA.

- **MITRE Corporation**

  La MITRE Corporation est une organisation américaine à but non lucratif qui administre le programme CVE et agit en tant que racine principale (Top-Level Root) pour la coordination de la divulgation des vulnérabilités.

  - Couvre les vulnérabilités :
    - non déjà couvertes par un CNA existant.
    - dans les produits open source.

- **Red Hat, Inc.**

Red Hat est une entreprise américaine spécialisée dans les solutions open source, jouant le rôle de CNA-LR pour les vulnérabilités liées aux projets open source, particulièrement ceux associés à ses propres produits.

- Couvre les vulnérabilités dans les logiciels développés par les CNAs sous la hiérarchie Red Hat.
- Remarque : Les organisations open source peuvent choisir Red Hat ou un autre Root.

Contacter une CNA n'ayant pas la compétence nécessaire au traitement de la vulnérabilité pourrait retarder le processus, un retard pouvant laisser la faille non corrigée et donc exploitable plus longtemps, mais généralement les CNAs réorientent les personnes qui souhaitent remonter une vulnérabilité.

Quelques CNAs françaises :

Jusqu'à aujourd'hui, il n'y a eu que sept CNAs enregistrées en France[15] :

- **ARC Informatique**
  Spécialisée dans ses propres produits et services, notamment dans le domaine de la supervision industrielle (comme PCVue).
- **Centreon**
  Traite uniquement les vulnérabilités liées à ses solutions de supervision informatique. Projet open source reconnu.
- **Dassault Systèmes**
  Couvre l'ensemble de ses sites web, services SaaS (comme 3DEXPERIENCE) et logiciels (incluant SolidWorks).
- **IDEMIA**
  Gère les vulnérabilités de ses produits (actifs ou obsolètes) ainsi que celles détectées dans des logiciels tiers hors du périmètre d'autres CNAs.
- **Schneider Electric**
  Responsable des CVE pour tous ses produits, incluant Proface, APC et Eurotherm, dans les domaines industriels et de l'énergie.

[15] CVE Program, *Centreon Added as CNA*.

- **Thales Group**

  CNA racine pour le groupe. Couvre les produits et technologies de Thales et de ses filiales, y compris les vulnérabilités tierces découvertes.

- **WPScan**

  Se concentre sur les vulnérabilités affectant WordPress : cœur, plugins et thèmes. Fortement impliqué dans la sécurité de l'écosystème WordPress.

Cependant, il semblerait que le pays indiqué pour chaque partenaire sur le site officiel du programme soit rempli par les partenaires. Pour cette raison, certaines entreprises ayant pourtant un siège social en France sont répertoriées dans d'autres pays sur le site. On peut citer l'exemple d'Airbus qui est officiellement basé aux Pays-Bas mais qui possède de nombreuses filiales en France :

- **Airbus**

  Responsable de l'attribution des CVE pour tous ses produits, y compris ceux en fin de vie ou de service. Couvre également les vulnérabilités découvertes dans des logiciels tiers, à condition qu'elles ne soient pas déjà couvertes par une autre CNA.

  Pays d'origine : Pays-Bas

- **Odoo**

  Gère les vulnérabilités affectant uniquement ses propres produits, notamment dans le cadre de sa solution open-source de gestion d'entreprise.

  Pays d'origine : Belgique

Aussi, comme indiqué dans les conditions pour devenir une CNA, chacune de ces entreprises dispose de politiques de divulgations internes accessibles au public. On s'intéressera plus particulièrement à l'exemple de Thales[16] dans une prochaine partie. Un point notable est l'absence de l'Agence nationale de la sécurité des systèmes d'information (ANSSI) et du Centre gouvernemental de veille, d'alerte et de réponse aux attaques informatiques (CERT-Fr). Cela pourrait s'expliquer par le rôle de ces organismes dans l'écosystème de la cybersécurité en France. En effet ils sont directement rattachés au Premier ministre et disposent de mission de défense nationale, avec des enjeux de confidentialité, voire même de secret défense. Ainsi, ne pas appartenir

[16] Thales Group, *Product Security Incident Response Team (PSIRT)*.

au programme CVE leur permet de ne pas être dépendant d'un organisme américain, ayant parfois des objectifs contraires. L'ANSSI collabore également avec l'Agence de l'Union européenne pour la cybersécurité (ENISA) et d'autres CERTs européens afin d'atteindre une souveraineté numérique européenne en matière de divulgation de vulnérabilité. Et même si l'ENISA est une CNA depuis janvier 2024, le récent lancement de la European Vulnerability Database (EUVD) semble confirmer cette volonté d'indépendance.

1.4.3 Autopsie d'une CVE : De la découverte à la publication

Chaque CVE suit un format standardisé[17] : `CVE-AAAA-NNNNN`, où :

- **AAAA** est l'année d'identification,
- **NNNNN** est un identifiant numérique unique.

Une fiche CVE comprend[18] :

- Le titre et l'identifiant,
- Une brève description de la vulnérabilité,
- Le produit concerné (avec version),
- Une référence vers la première divulgation publique,
- le type de vulnérabilité, le programme recommande d'utiliser le Common Weakness Enumeration (CWE)

Aussi, comme évoqué dans la partie sur les différents rôles au sein du programme, les ADPs peuvent rajouter du contenu divers pour chacune des entrées afin de les compléter.

Deadlines et publication

Une vulnérabilité peut être publiée immédiatement ou selon un calendrier de divulgation coordonnée, généralement de 90 jours. Cette période permet à l'éditeur du logiciel de corriger la faille avant sa publication. En cas d'absence de réponse ou de correctif, la CVE peut être rendue publique au terme du délai.

[17] CVE Program, *About CVE - Process*.
[18] CVE Program, *CVE Record Content*.

Cycle de vie d'une CVE

Le cycle de vie d'une CVE peut se résumer en plusieurs étapes[19] :

1. **Découverte** : un chercheur ou une organisation identifie une vulnérabilité dans un produit ou service.
2. **Contact du fournisseur** : le découvreur informe l'éditeur concerné (ou une CNA) de manière responsable.
3. **Assignation** : si la vulnérabilité est jugée légitime, un numéro CVE est assigné par la CNA.
4. **Période de correction** : un délai (souvent 90 jours) est accordé pour le développement et le déploiement d'un correctif.
5. **Publication** : une fois le correctif disponible (ou à la fin du délai), la CVE est rendue publique dans la base officielle.

1.4.4 Limite de l'organisation du programme

Même si ce programme est aujourd'hui une référence dans le monde de la cybersécurité, il présente certaines limites notamment en ce qui concerne ses financements. En effet ils proviennent du U.S. Department of Homeland Security (DHS) et plus précisément de CISA. Or, ils ont expiré le 16 avril 2025 et sont resté sans renouvellement pendant plusieurs heures avant d'être finalement rétablis pour onze mois. Même si cette période peut sembler courte, de nombreux acteurs du secteurs ont cru y voir la fin du programme CVE[20]. Cette situation souligne la fragilité du programme CVE, pourtant essentiel à la cybersécurité mondiale. Sa dépendance à une seule source de financement le rend vulnérable aux aléas politiques. Même une interruption brève peut perturber l'écosystème : retards dans l'attribution des identifiants, désorganisation des acteurs, perte de confiance. Pour assurer sa pérennité, le programme CVE cherche désormais à s'appuyer sur la CVE Foundation, créée pour renforcer la transparence et la diversification des financements. En élargissant la base au-delà de CISA, le programme cherche à éviter de revivre cette situation et garantir une continuité des services proposés[21].

[19] CVE Program, *About CVE - Process*.
[20] Kate O'Flaherty, *Article sur l'arrêt des financements du programme CVE*.
[21] CVE Foundation, *Présentation de la CVE Foundation*.

1.5 Les politiques de divulgation des entreprises

Après avoir étudié une manière centralisée de recenser les vulnérabilités, il est intéressant de voir un procédé décentralisé.

En effet, une autre méthode pour divulguer une vulnérabilité est de passer directement par l'entreprise. La plupart disposent d'ailleurs de politiques internes qui visent à établir un certain nombre de règles pour les personnes souhaitant remonter une faille, notamment sur les circonstances de la découverte ou le mode de contact. Rappelons que chaque CNA doit disposer d'une telle politique afin de faire parti du programme CVE. Ainsi on peut prendre l'exemple du groupe Hager[22] qui s'engage à ne pas poursuivre les chercheurs qui respecteraient certaines conditions comme par exemple : soumettre un rapport détaillé, collaborer avec les équipes du groupe, attendre de recevoir une autorisation avant de publier publiquement, ne pas demander de compensation financière ou ne pas modifier les données des systèmes vulnérables... À première vue ces consignes semblent acceptables et pourraient laisser croire aux chercheurs qu'ils seraient protégés de toute action en justice. Seulement ces politiques n'ont aucune valeur juridique. En effet si un procureur venait à obtenir des éléments justifiant une enquête alors le chercheur pourrait être poursuivi et ce même si l'entreprise ne souhaite pas engager de poursuite. Ce point n'étant pas évident, il pourrait induire en erreur un chercheur et le mettre en difficulté vis-à-vis de la justice et de l'entreprise. Cependant la plupart des instructions données par les entreprises étant souvent des interdictions qui font déjà partie du cadre légal, par exemple ne pas modifier les données des systèmes ou perturber l'accès à ces derniers, elles peuvent permettre de rappeler aux chercheurs certaines de leurs obligations.

[22] Hager Group, *Politique de divulgation de vulnérabilité du groupe Hager*.

2 Un cadre juridique incomplet

En droit français, il n'existe pas de définition du terme "divulgation de vulnérabilité". Tout comme en informatique, définir la vulnérabilité et la divulgation ne fait pas l'unanimité. À contrario, les instances européennes ont plus ou moins défini ces deux termes dans la directive NIS 2[23]. Cette directive, concernant les mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union européenne, fixe des obligations qui s'imposent aux États membres de l'Union et aux entreprises. Accompagnée d'autres directives, la directive NIS 2 impose un cadre coordonné pour la divulgation de vulnérabilités, mais se concentre sur les entités publiques et l'aspect institutionnel en charge de cette divulgation.

À l'article 12 de la directive NIS 2, le terme vulnérabilité est défini comme "une faiblesse, susceptibilité ou faille de produits TIC (ndlr. Technologies de l'Information et de la Communication) ou de services TIC qui peut être exploitée par une cybermenace."

Une définition du terme divulgation de vulnérabilité est également donnée dans le considérant 58 de la directive. Cette définition prévoit que "La divulgation coordonnée des vulnérabilités consiste en un processus structuré dans lequel les vulnérabilités sont signalées au fabricant ou au fournisseur de produits TIC ou de services TIC potentiellement vulnérables, de manière à leur donner la possibilité de diagnostiquer la vulnérabilité et d'y remédier avant que des informations détaillées à ce sujet soient divulguées à des tiers ou au public". Les considérants d'un texte européen ne sont pas aussi contraignants juridiquement que les articles du texte. Ils servent avant tout à introduire des éléments de contexte qui aident à la compréhension du texte et de ses enjeux. La définition illustre que la directive se concentre sur l'aspect institutionnel de la divulgation de vulnérabilité en tant que "processus structuré" permettant une remontée d'information et une remédiation. La protection des acteurs de la divulgation n'est pas encadrée, mais la directive prévoit au considérant 60 que "Dans le cadre de leur politique nationale, les États membres devraient s'efforcer de relever, dans la mesure du possible, les défis auxquels sont confrontés les experts qui recherchent les vulnérabilités, y compris le risque lié à

[23] Parlement Européen, *Directive (UE) 2022/2555 du Parlement européen et du Conseil du 14 décembre 2022 concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union, modifiant le règlement (UE) no 910/2014 et la directive (UE) 2018/1972, et abrogeant la directive (UE) 2016/1148*.

la responsabilité pénale potentielle, conformément au droit national".

L'absence de définition juridique à la divulgation de vulnérabilité et d'encadrement juridique des acteurs pose plusieurs problèmes, notamment pour les chercheurs en cybersécurité ou les hackers. La directive NIS 2 affirme qu'un risque de poursuites pénales pèse sur ces acteurs. Il est donc intéressant d'analyser les risques de poursuites potentielles (2.1) ainsi que les conséquences de l'engagement de la responsabilité des acteurs de la divulgation de vulnérabilité (2.2).

2.1 Quels sont les risques encourus ?

L'analyse ici porte sur deux cas d'usages concrets : la découverte d'une vulnérabilité dans le cadre d'un audit, ainsi qu'une découverte, par un chercheur en dehors de tout contrat (le droit civil, ou plus précisément le droit des contrats, ne sera pas analysé dans le cadre de ce rendu).

2.1.1 Les peines auxquelles s'exposent les hackers

Dans le cadre de la recherche de vulnérabilité, les principales peines auxquelles s'exposent les hackers sont décrites dans les articles 323-1 à 323-8 du Code pénal :

L'accès ou le maintien (article 323-1) est puni par une peine maximale de trois ans d'emprisonnement accompagnée de 100 000 euros d'amende. Cette peine pourra être portée à cinq ans d'emprisonnement et 150 000 euros d'amende s'il en est résulté soit la suppression ou la modification de données, soit une altération du fonctionnement du système.

Le fait d'entraver ou de fausser le fonctionnement d'un STAD est puni de cinq ans d'emprisonnement et de 150 000 euros d'amende. (article 323-2)

Le fait d'introduire frauduleusement dans un STAD, d'extraire, de détenir, de reproduire, de transmettre, de supprimer ou de modifier frauduleusement des données contenues par un STAD est puni de cinq ans d'emprisonnement et de 150 000 euros d'amende.

Les infractions définies ci-dessus sont punies de sept ans d'emprisonnement et 300 000 euros d'amende si elles sont commises à l'encontre d'un STAD mis en place par l'État.

Le chapitre concernant les infractions contre les STAD n'est pas le seul à définir des infractions pouvant causer du tort à un hacker dans le cadre de la divulgation de vulnérabilité. En premier lieu, les chercheurs peuvent enfreindre l'article 441-1 du Code pénal qui punit de trois ans d'emprisonnement et 45 000 euros d'amende le faux et usage de faux, notamment dans

l'usage de certificats. En informatique, un certificat est un fichier numérique qui authentifie l'identité d'une entité ou d'une personne en utilisant une signature électronique. À la manière d'une carte d'identité, il est tout à fait possible de créer un faux certificat permettant d'usurper l'identité d'une entité ou d'une personne. Faire usage d'un faux certificat dans le cadre d'une recherche de vulnérabilité est donc considéré comme de l'usage de faux.

2.1.2 La qualification de l'infraction

Afin de déterminer les risques encourus par les acteurs de la divulgation de vulnérabilité, il faut préciser qu'en droit pénal, afin de déterminer si un crime ou un délit s'applique au cas d'usage, il est nécessaire de déterminer la matérialité et l'intentionnalité de l'infraction :

- L'élément matériel vise le comportement réprimé par le texte de loi. A titre d'exemple, le vol est la soustraction frauduleuse de la chose d'autrui (article 311-1 du Code pénal). C'est donc l'action du vol qui est visé ici.
- l'élément intentionnel s'attarde sur l'intention de l'auteur. L'intention peut être démontrée différemment en droit (faute intentionnelle, non intentionnelle, d'imprudence ou de négligence).

L'objectif ici sera de montrer les infractions matérielles pouvant s'appliquer aux hackers cherchant des vulnérabilités et de voir leur traduction concrète. Puis, l'intentionnalité de l'infraction semble être un point de dissonance entre les juristes et les informaticiens. Il est donc nécessaire de clarifier cette dernière afin de pouvoir voir les risques liés à la responsabilité.

Analyse de l'élément matériel

L'élément matériel vise le corps du délit, à savoir l'action concrète qui peut être reprochée au hacker. Les articles 323-1 à 323-8 du Code pénal forment le socle juridique français en matière de pénalisation des atteintes aux systèmes informatiques, également appelés systèmes de traitement automatisé de données (STAD).

L'indéfinition du STAD De prime abord, il est nécessaire de préciser qu'aucune de ces lois n'a cependant pris la peine de définir la notion de STAD. La définition suivante avait pourtant été proposée par le Sénat lors de sa première lecture de la proposition de loi relative à certaines

infractions en matière de systèmes de traitements automatisés de données, aujourd'hui connue sous le nom de loi Godfrain (1988)[24] : "Au sens du présent chapitre, on doit entendre par système de traitements automatisés de données, tout ensemble composé d'une ou plusieurs unités de traitement, de mémoires, de logiciels, de données, d'organes d'entrées-sorties et de liaisons, qui concourent à un résultat déterminé, cet ensemble étant protégé par des dispositifs de sécurité".

Cette définition a été rejetée par l'Assemblée nationale par peur qu'elle ne se limite à l'état actuel de la technique, et ne couvre plus les équipements futurs développés par de nouvelles technologies.

Cette définition, malgré qu'elle ait été rejetée par l'Assemblée nationale, montre que la notion de STAD a pour objectif de recouvrir tout équipement informatique existant. Plus récemment, un rapport du groupe de travail interministériel a précisé que "en pratique, le STAD recouvre aussi bien une puce électronique (de carte de paiement, de téléphone mobile...), un site Web, une base de données ou un autocommutateur téléphonique électronique".[25]

S'agissant de la matérialité, les dispositions sur les infractions relatives aux STADs sont essentielles pour comprendre les risques juridiques encourus par les chercheurs en cybersécurité, même lorsqu'ils agissent à des fins de sécurité.

L'application de la matérialité des atteintes aux STADs À titre d'exemple, un chercheur identifie une potentielle vulnérabilité dans un système sur lequel il n'a aucune autorisation. Il tente donc d'exploiter cette faille pour vérifier ses soupçons. Il réussit et a donc accédé au système en exploitant cette vulnérabilité. À ce moment, la matérialité de l'infraction définie à l'article 323-1 du code pénal est remplie par l'accès ou le maintien dans le système en supposant qu'aucune atteinte au bon fonctionnement du système ni altération des données n'ont été effectuées. Dans ce cas, la matérialité de l'infraction est caractérisée par le fait que, pour identifier la vulnérabilité, le chercheur est entré dans le système, s'y est maintenu et a tenté d'exploiter la vulnérabilité pour vérifier sa trouvaille.

[24] Sénat, *Proposition de loi relative à certaine infractions en matière de systèmes de traitements automatisés de données modifiée par le Sénat.*

[25] Robert, *Protéger les internautes - Rapport sur la cybercriminalité*.

Qu'est-ce que la bonne foi en droit ? Analyse de l'élément intentionnel

Les termes de bonne foi, bonne intention ou éthique sont souvent mis en avant dans le cadre du travail des hackers ou des chercheurs en vulnérabilité. Si l'éthique a été suffisamment présentée dans le livre blanc des masters 1 cybersécurité sur les hackers éthiques de 2024[26], il est pertinent de revenir sur la bonne foi, la bonne intention et l'aspect intentionnel des infractions relatives aux STADs.

En langage juridique, la bonne foi peut être définie comme 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[27]. En droit français, le concept de bonne foi est quasi exclusivement utilisé en droit civil grâce à l'article 2274 du Code civil qui indique que "La bonne foi est toujours présumée, et c'est à celui qui allègue la mauvaise foi à la prouver."

S'agissant du droit pénal, le terme "bonne intention" ou "bonne foi" n'est pas utilisé. Il est cependant sujet d'intention dans l'article 121-3 du Code pénal qui indique "[qu]'il n'y a point de crime ou de délit sans intention de le commettre". Cet article traduit l'élément intentionnel de l'infraction. Cela signifie que, pour caractériser une infraction, l'auteur a dû avoir l'intention de la commettre. Cependant, la loi peut prévoir dans certains cas la pénalisation des infractions non intentionnelles (exemple : la mise en danger délibérée d'autrui de l'article 121-3 alinéa 2 du Code pénal). L'intention se distingue d'ailleurs du mobile qui est la raison de la commission de l'infraction. Le mobile est indifférent dans la caractérisation de l'infraction.

S'agissant des infractions concernant les STADs, le terme "frauduleusement" figure aux articles 323-1 et 323-3 du Code pénal. Ce terme est la traduction de la recherche d'intention en droit pénal. La jurisprudence, donc l'ensemble des jugements précédemment rendus par les juridictions, prévoit que l'intrusion frauduleuse se traduit par un défaut d'autorisation (Cass. Crim. 16 janv. 2018).

À titre d'exemple, une récente affaire jugée par le tribunal correctionnel d'Albi (TJ d'Albi, 6 juin 2024) fait état d'un pompier volontaire et ingénieur informaticien en cybersécurité qui

[26] Jules Cooper, Elyes Hakmouni, Titouan Le Blé, Leonie Maier, Mélanie Romano

[27] Braudo, *Définition de la bonne foi*.

a été jugé pour avoir pénétré le système informatique du Service Départemental d'Incendie et de Secours du Tarn. L'individu a toujours plaidé la bonne intention puisqu'il assure avoir simplement voulu tester la sécurité du système. Pourtant, le tribunal a bien reconnu que l'accusé n'avait pas agi avec de mauvaises intentions, mais cela n'a pas semblé avoir joué dans la décision de la cour. On le comprend notamment grâce à cette phrase issue du jugement : "Il importe peu que ces agissements ont été sans conséquence pour le système informatique du service départemental et que [l'individu] a entendu intervenir pour s'assurer de la protection effective du système, dès lors qu'il n'était pas habilité pour entrer dans l'intranet du système". Cette phrase montre que le manque d'habilitation, et donc d'autorisation, est le point clé qui a poussé vers la décision finale. Et donc, la lecture du jugement montre que ce qui différencie un hacker "malveillant" d'un hacker "bienveillant" est l'autorisation et non l'intention derrière l'acte.

En outre, il est également reproché à l'accusé de ne pas avoir réussi à "expliquer pour quelles raisons il n'avait pas averti ni en amont, ni en aval le SDIS de son action". Cela est évidemment un point noir dans sa défense car cela entrave la bonne intention qu'il louait alors jusque-là. Puisqu'il a réussi à pénétrer le système avec les identifiants par défaut "admin/admin" et que la sécurité était très faible, il aurait dû en avertir immédiatement le service pour qu'il puisse procéder à des modifications. Sans cette action, il devient alors plus difficile de statuer sur la bonne intention de l'accusé.

Les contours de la tentative et de la complicité

Il est également important de souligner que la tentative (article 121-4 du Code pénal) et la complicité (article 121-7 du Code pénal) sont punies au même titre que l'acte principal.

À ce titre, un individu qui tenterait de pénétrer un STAD à distance avec des identifiants par défaut, par exemple "admin/admin", sans y arriver pourrait être susceptible d'écoper de la même peine. Selon l'article 121-4 du Code pénal, la matérialité de la tentative se traduit par : le commencement d'exécution d'un crime ou d'un délit prévu par le Code pénal, et enfin une interruption par des circonstances indépendantes de la volonté de l'auteur. Dans le cas présenté, le commencement de l'exécution se traduit par l'individu qui rentre des identifiants pour se connecter à un système sans autorisation. L'interruption a lieu lorsque le système refuse l'accès au système à l'individu.

La complicité, quant à elle, pourrait être invoquée à l'égard d'une personne qui fournirait des détails privés concernant la sécurité d'un STAD dont elle a connaissance à une personne qui se servirait ensuite de ces informations pour compromettre le STAD en question. La matérialité de la complicité, selon l'article 121-7 alinéa 1er du Code pénal, se traduit par une "personne qui sciemment, par aide ou assistance, en a facilité la préparation ou la consommation". Dans l'exemple cité, la personne ayant fourni les informations au hacker a sciemment facilité la préparation et l'exécution du délit, elle est donc considérée comme complice.

L'analyse des éléments matériels et intentionnels des infractions relatives aux STADs permet de tirer une conclusion. Les acteurs de la recherche de vulnérabilité ne sont ni soumis à un cadre juridique inexistant, ni trop strict. L'état actuel de ce cadre montre qu'il est inadapté à la recherche du vulnérabilité car il ne prends pas en compte les actions nécessaires à la recherche de vulnérabilité, en plus d'être conditionnée à l'élément intentionnel de l'infraction, à savoir la nécessité d'obtenir une autorisation, ce qui est un frein énorme à l'activité de ses chercheurs.

2.1.3 Critique du cadre légal

Ces articles montrent la volonté du législateur de protéger les STADs contre les intrusions, mais leur application reste en réalité très floue. En effet, la loi oublie que toutes les actions qu'elle considère comme néfastes pour les STAD sont en réalité nécessaires dans le processus de recherche de vulnérabilité, et sont donc importantes pour la protection des STAD. C'est la raison pour laquelle les chercheurs en cybersécurité évoluent dans une zone grise où leurs contributions sont souvent perçues comme bénéfiques par la communauté, mais qu'elles sont perçues comme des délits par la loi.

Concrètement, dans le cadre d'une recherche de vulnérabilité, plusieurs actions sont nécessaires pour tester les différents types de vulnérabilités. Premièrement, en l'absence d'autorisation, la vérification de la robustesse d'un système d'authentification par mot de passe nécessite de tester un ou plusieurs mots de passe afin de vérifier si l'accès est permis ou non. Si le mot de passe testé donne accès au système, l'article 323-1 du Code pénal sur l'accès et le maintien frauduleux peut s'appliquer. Et comme vu précédemment, si le mot de passe testé ne donne finalement pas accès au système, la tentative peut tout de même être invoquée (article 121-4

du Code pénal). Ce simple test, en l'absence d'autorisation ou de politiques de divulgation de vulnérabilité encadrant la possibilité de le faire, peut permettre de poursuivre l'auteur du test, qui pourrait se limiter à cette manipulation et le signaler au propriétaire du système d'authentification.

Dans un système, les actions nécessaires à la recherche de vulnérabilités sont aussi concernées. L'exemple d'un chercheur qui aurait réussi à pénétrer un système sans autorisation est pertinent car, dans la plupart des situations, l'accès à un système ne permet pas l'accès à des données sensibles. Ce dernier doit alors chercher de nouvelles vulnérabilités qui pourraient lui permettre soit d'atteindre un autre système, soit de monter en privilège sur le système actuel. Quand on parle de privilège en informatique, il est fait référence à ce qu'un utilisateur a le droit ou non de faire sur un système. Ainsi, monter en privilège consiste à trouver et utiliser des vulnérabilités pour, soit modifier les privilèges accordés à l'utilisateur actuel, soit se connecter comme administrateur possédant davantage de privilèges. Ainsi, pour ce faire, le chercheur devra impérativement déposer sur le système des programmes d'analyse, des programmes de tests, ou d'autres fichiers lui permettant de trouver des vulnérabilités. Le chercheur a alors introduit des données dans le STAD, ce qui est interdit (article 323-3 du Code pénal). Cependant, il est important de rappeler que ces lois existent avant tout pour protéger les STAD des attaques malveillantes et qu'elles sont absolument nécessaires à ce but. Sans autorisation, il est difficile, voire impossible, de distinguer le hacker souhaitant vérifier la robustesse du système de celui souhaitant le compromettre. C'est la nuance entre les attaques malveillantes et les recherches bienveillantes et bénéfiques de vulnérabilités que ces lois, à ce jour, échouent à distinguer correctement.

Dans le jugement du tribunal d'Albi (TJ d'Albi, 6 juin 2024) cité précédemment, il est indiqué que l'homme a été reconnu coupable des trois chefs d'accusation dont il faisait l'objet : accès frauduleux, maintien frauduleux (article 323-2 du code pénal), et introduction frauduleuse de données dans un système de traitement de données automatisé (article 323-3 du code pénal). L'individu a donc été condamné à une peine de 9 mois d'emprisonnement avec sursis et à environ 4300 euros de dommages et intérêts. En effet, le jugement détaille, pour chaque infraction, l'action commise par l'individu :

- l'accès frauduleux se matérialise par une intrusion sur le serveur intranet du service en tant qu'administrateur
- le maintien frauduleux peut se traduire par une navigation afin de vérifier les autres

vulnérabilités. L'individu ayant lancé un scan de vulnérabilité, il devait se maintenir

- l'introduction de données se matérialise par le dépôt de 149 fichiers et 10 dossiers.

La matérialité de trois infractions a été constatée par les juges. La seule distinction que le droit fait du caractère malveillant ou non ne vise pas les considérations éthiques, ou la bonne intention du hacker, comme le disait le condamné du jugement du tribunal d'Albi. L'autorisation semble être l'élément déterminant de l'intentionnalité de l'infraction.

Après avoir vu les éléments de qualification de l'infraction et analysé le cadre légal, il est nécessaire de voir quels sont les risques en termes de responsabilité des auteurs.

2.2 A qui vont les responsabilités ?

Les deux cas présentés visent la découverte d'une vulnérabilité dans le cadre d'un audit (et donc d'un salarié employé dans le cadre d'une mission), ainsi qu'une découverte fortuite, par un chercheur en dehors de tout contrat. L'objectif ici est de voir s'il est possible d'engager la responsabilité des hackers en recherche de vulnérabilité, ainsi que celle des entreprises.

2.2.1 L'engagement de la responsabilité personnelle des hackers

L'engagement personnel des hackers en cas d'infraction se fait en vertu de l'article 121-1 du Code pénal qui dit que "Nul n'est responsable pénalement que de son propre fait.". Cela signifie qu'en droit pénal, on ne peut être poursuivi que pour une infraction commise soi-même et qu'il est, par définition, interdit de punir quelqu'un pour une infraction commise par un tiers, sauf exceptions.

Les tentatives d'élaboration d'une irresponsabilité en cas de bonne foi

Le législateur français a déjà tenté à plusieurs reprises de créer des exceptions pour protéger les hackers qui divulgueraient les vulnérabilités. En 2016, lors des débats concernant la loi pour une République numérique, l'Assemblée nationale avait voté un amendement qui indiquait que "toute personne qui a tenté de commettre ou commis le délit prévu au présent article (ndlr. article 323-1 du Code pénal) 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."[28]. Comme indiqué par les députés dans le document, cet amendement avait pour but de "protéger les lanceurs d'alerte lorsqu'ils veillent à avertir les responsables de traitement des failles dans leurs systèmes."

Plusieurs raisons ont poussé les sénateurs à rejeter cet amendement. Premièrement, il avait été argumenté que la rédaction de cet amendement permettait à toute personne qui accéderait frauduleusement et intentionnellement à STAD afin de supprimer des données ou d'en altérer son fonctionnement, par exemple, d'être exemptée de peine dès lors qu'elle aurait contacté, après son forfait, le responsable du traitement en cause[29]. Il avait également été noté qu'une telle mesure aurait pu encourager l'intrusion dans des STAD par des personnes n'ayant pas forcément l'intention de divulguer des vulnérabilités.

Une autre tentative a été effectuée, toujours en 2016, lors des débats parlementaires pour la loi Sapin 2[30]. Cette loi relative à la transparence, à la lutte contre la corruption et à la modernisation de la vie économique a posé les bases de la protection spécifique du lanceur d'alerte. Lors des débats parlementaires, le même amendement qui avait été proposé plus tôt dans l'année a de nouveau été proposé. Il a cette fois-ci été considéré comme hors sujet par la majorité parlementaire et a donc été rejeté[31].

Une alternative a été adoptée dans la loi pour une République numérique de 2016 où cet amendement avait été en quelque sorte remplacé par l'actuel article L.2321-4 du Code de la défense qui permet à l'ANSSI de ne pas signaler au procureur de la République une infraction qui aurait été commise dans le cadre d'une recherche de vulnérabilité si elle estime le chercheur de bonne foi. Cependant, cet article ne crée pas d'exception qui permettrait de déresponsabiliser un chercheur pour des infractions commises lors de sa recherche de vulnérabilité.

Pour résumer, toutes les propositions solides pour protéger davantage les divulgateurs de vulnérabilités ont été avortées. Ce manque de protection est évidemment critiquable au vu de

[28] Assemblée nationale, *Loi pour une République numérique de 2016 - Amendement n°271 (Rect).*

[29] Rees, *Il faut protéger les chercheurs de failles « zero day ».*

[30] Assemblée nationale, *Loi relative à la transparence, à la lutte contre la corruption et la modernisation de la vie économique - Amendement n°72.*

[31] Beky, *Loi Sapin 2 : les lanceurs d'alerte informatique non protégés.*

l'importance croissante de la cybersécurité aujourd'hui et de l'importance que peuvent avoir les hackers éthiques et les chercheurs dans ce milieu. Il est probable que ce manque de motivation du pouvoir législatif à appliquer une protection efficace soit en réalité dû au fait que les hackers sont en réalité très peu inquiétés par la justice quand ils divulguent des vulnérabilités, que ce soit à l'ANSSI ou même directement au propriétaire du système.

L'engagement de cette responsabilité reste rare

Bien que la responsabilité d'un divulgateur de vulnérabilités ne puisse pas être totalement écartée, cela ne signifie pas pour autant qu'il fasse systématiquement l'objet de poursuites judiciaires lors de la divulgation d'une vulnérabilité. En pratique, l'ANSSI ou les entreprises concernées engagent rarement des actions en justice lorsqu'il est clair que le chercheur a agi de bonne foi et n'a pas causé de tort au système. Ce serait contre-productif pour tous les acteurs du secteur, car les chercheurs en cybersécurité sont un élément important pour la sécurité des systèmes en général. Pour les entreprises plus importantes, cela constituerait également un risque, notamment en termes d'image publique, que de poursuivre en justice un chercheur de bonne foi qui a divulgué une vulnérabilité de manière confidentielle. Dans un monde où les données personnelles sont de plus en plus présentes et où leur sécurité est plus importante que jamais, cela pourrait renvoyer une mauvaise image de l'entreprise et de sa politique générale vis-à-vis de la sécurité informatique. Cependant, comme vu précédemment avec l'affaire jugée par le tribunal d'Albi, le manque de cadre juridique peut être un problème qui oblige les chercheurs à être irréprochables pour ne pas être inquiétés. De plus, le manque de cadre ne permet pas une uniformisation des règles à respecter, ce qui rend le travail des chercheurs encore plus difficile.

2.2.2 L'engagement de la responsabilité de l'entreprise et du chef d'entreprise

Dans la situation où une personne ayant divulgué une vulnérabilité est employée par une entreprise, la question se pose de savoir si la responsabilité doit être engagée envers l'employé ou l'entreprise.

Dans cette optique, il est important de noter que l'article 121-2 du Code pénal indique très clairement que les entreprises sont responsables pénalement des infractions commises, pour leur compte, par leurs organes ou représentants. Dans le cas où la responsabilité d'une entreprise est engagée, le chef d'entreprise peut être poursuivi en tant que personne physique.

Le principe de responsabilité pénale cumulative indique que pour une même infraction pénale, la responsabilité de plusieurs personnes peut être engagée. À titre d'exemple, si un ingénieur a pénétré un système informatique sans autorisation pour y rechercher une vulnérabilité dans le cadre de ses fonctions au sein de son entreprise, la responsabilité de l'ingénieur peut être engagée car il est la personne qui a commis les faits.

La responsabilité du chef d'entreprise peut également être engagée s'il est considéré, par exemple, que l'employé agit dans le cadre d'une délégation de pouvoirs, c'est-à-dire qu'il a accepté une mission précise, qui lui a été assignée et des moyens lui ont été fournis (ces critères sont d'ailleurs dégagés par la jurisprudence).

Enfin, la responsabilité de l'entreprise peut être engagée sur la base de l'article 121-2 vu précédemment. Ainsi, il existe un moyen pour un chef d'entreprise de déléguer certaines responsabilités à des personnes tierces, et ainsi éviter que sa responsabilité soit engagée pour des infractions commises par ses employés. Dans les entreprises d'une certaine taille, il est évident que le chef d'entreprise ne peut pas veiller à titre personnel à ce que tous les employés respectent la loi et ne mettent pas en danger l'entreprise. Pour cela, il existe la possibilité pour les chefs d'entreprise d'établir une délégation de pouvoir vers un subordonné. Le principe et les conditions de validité sont définis par la jurisprudence et ne sont donc pas définis par des lois[32].

En résumé, la responsabilité pénale des hackers est rarement engagée lorsqu'ils agissent de bonne foi, bien que la loi ne les protège pas sur ce point là. Lorsqu'ils agissent dans un cadre professionnel, la responsabilité peut être partagée entre l'employé, le chef d'entreprise et l'organisation elle-même, selon les circonstances et les délégations de pouvoir.

[32]Editions Tissot, *Définition de délégation de pouvoirs*.

Remerciements

Nous tenons à remercier notre encadrante Hermine Cappé pour son implication dans le projet. Son accompagnement a été très précieux et nous a permis de nous initier à un domaine dans lequel nous n'avions aucune connaissance mais qui s'est avéré être très intéressant et enrichissant.

Nous remercions également Christèle Jacq-Arnoult, Responsable des Relations Écosystème à la CyberSchool, pour son aide précieuse dans la mise en relation avec des professionnels du secteur. Son soutien a grandement facilité l'avancement de nos recherches.

Nous exprimons notre reconnaissance à Jérémie Dhune, ainsi qu'à Olivier Rollat, Simon Delayen et Lilian Marié de Sopra Steria pour la qualité de leurs échanges, leurs retours d'expérience et les exemples concrets partagés. Leur intérêt pour notre sujet a renforcé notre motivation et nous a conforté dans notre démarche.

Nous souhaitons également remercier Jean-Pascal Thomas d'Orange Cyberdéfense, pour le temps qu'il nous a accordé et sa disponibilité à répondre à nos questions.

Un grand merci également aux équipes de Synacktiv à Rennes pour leur expertise technique, ainsi qu'à YesWeHack pour leur éclairage sur les programmes de bug bounty et leur rôle dans l'écosystème de la divulgation responsable.

Enfin, nous remercions l'ANSSI pour les ressources mises à disposition, qui ont largement nourri notre réflexion sur le cadre réglementaire français.

À toutes et à tous, merci pour votre précieuse contribution à cette recherche.

Références

ADOBE. *Suppression de contenu confidentiel dans les fichiers PDF*. 2023. URL : https://helpx.adobe.com/fr/acrobat/using/removing-sensitive-content-pdfs.html (visité le 01/05/2025).

ANSSI. *Histoire et modèle*. 2025. URL : https://cyber.gouv.fr/histoire-et-modele (visité le 02/05/2025).

ASSEMBLÉE NATIONALE. *Loi pour une République numérique de 2016 - Amendement n°271 (Rect)*. 2016. URL : https://www.assemblee-nationale.fr/14/amendements/3399/AN/271.asp.

— *Loi relative à la transparence, à la lutte contre la corruption et la modernisation de la vie économique - Amendement n°72*. 2016. URL : https://www.assemblee-nationale.fr/14/amendements/3785/AN/72.asp.

BEKY, Arianne. *Loi Sapin 2 : les lanceurs d'alerte informatique non protégés*. 2016. URL : https://www.silicon.fr/Thematique/cybersecurite-1371/Breves/Loi-Sapin-2-les-lanceurs-d-alerte-informatique-non-proteges-438036.htm (visité le 01/05/2025).

BRAUDO, Serge. *Définition de la bonne foi*. URL : https://www.dictionnaire-juridique.com/definition/bonne-foi.php (visité le 12/04/2025).

CISA. *Known Exploited Vulnerabilities Catalog (KEV)*. URL : https://www.cisa.gov/known-exploited-vulnerabilities-catalog (visité le 15/05/2025).

— *Stakeholder-Specific Vulnerability Categorization (SSVC)*. URL : https://www.cisa.gov/stakeholder-specific-vulnerability-categorization-ssvc (visité le 15/05/2025).

CURELARIU, Teodora. *Défis juridiques de la divulgation des vulnérabilités*. 17 déc. 2024. URL : https://www.youtube.com/watch?v=tdAEuHgNQvI.

CVE Foundation. *Présentation de la CVE Foundation*. URL : https://www.thecvefoundation.org (visité le 15/05/2025).

CVE Program. *About CVE - History*. URL : https://www.cve.org/About/History (visité le 15/05/2025).

— *About CVE - Process*. URL : https://www.cve.org/About/Process (visité le 15/05/2025).

— *Authorized Data Publisher (ADP)*. URL : https://www.cve.org/ProgramOrganization/ADPs (visité le 15/05/2025).

— *Centreon Added as CNA*. 11 fév. 2025. URL : https://test.cve.org/Media/News/item/news/2025/02/11/Centreon-Added-as-CNA (visité le 15/05/2025).

— *CNA Onboarding Resources*. URL : https://www.cve.org/ResourcesSupport/Resources#cnaOnboarding (visité le 15/05/2025).

— *CVE Record Content*. URL : https://www.cve.org/ResourcesSupport/AllResources/CNARules%5C#section_5_CVE_Record_Content (visité le 15/05/2025).

— *CVE Terms of Use*. URL : https://www.cve.org/PartnerInformation/Partner (visité le 15/05/2025).

— *List of Partners*. URL : https://www.cve.org/PartnerInformation/ListofPartners (visité le 15/05/2025).

— *Program Organization Structure*. URL : https://www.cve.org/programorganization/Structure (visité le 15/05/2025).

Editions Tissot. *Définition de délégation de pouvoirs*. URL : https://www.editions-tissot.fr/guide/definition/delegation-de-pouvoir (visité le 15/05/2025).

FIRST. *Common Vulnerability Scoring System (CVSS)*. URL : https://www.first.org/cvss/ (visité le 15/05/2025).

HAGER GROUP. *Politique de divulgation de vulnérabilité du groupe Hager*. URL : https://hagergroup.com/fr/politique-de-divulgation-des-vulnerabilites (visité le 15/05/2025).

KATE O'FLAHERTY. *Article sur l'arrêt des financements du programme CVE*. URL : https://www.forbes.com/sites/kateoflahertyuk/2025/04/16/cve-program-funding-cut-what-it-means-and-what-to-do-next/ (visité le 15/05/2025).

PARLEMENT EUROPÉEN. *Directive (UE) 2022/2555 du Parlement européen et du Conseil du 14 décembre 2022 concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union, modifiant le règlement (UE) no 910/2014 et la directive (UE) 2018/1972, et abrogeant la directive (UE) 2016/1148*. 2022. URL : http://data.europa.eu/eli/dir/2022/2555/oj.

PROJECT, Tor. *Tor Project*. 2025. URL : https://www.torproject.org/about/history/.

REES, Marc. *Il faut protéger les chercheurs de failles « zero day »*. 2021. URL : https://next.ink/4905/il-faut-proteger-chercheurs-failles-zero-day/ (visité le 01/05/2025).

ROBERT, Marc. *Protéger les internautes - Rapport sur la cybercriminalité*. 2014. URL : https://www.vie-publique.fr/files/rapport/pdf/144000372.pdf.

SÉNAT. *Proposition de loi relative à certaine infractions en matière de systèmes de traitements automatisés de données modifiée par le Sénat*. 1987. URL : https://www.senat.fr/leg/1987-1988/ta1987_1988_0027.pdf.

THALES GROUP. *Product Security Incident Response Team (PSIRT)*. URL : https://www.thalesgroup.com/en/global/group/psirt (visité le 15/05/2025).