LIVRE BLANC
JANVIER 2024

La Divulgation Coordonnée de Vulnérabilités

Une application française incomplète, des textes européens à harmoniser

ACN
Alliance pour la confiance numérique

Michel SEJEAN

Professeur agrégé de droit
privé et sciences criminelles
Université Sorbonne Paris Nord

EDITO

Avec ce livre blanc sur la divulgation coordonnée de vulnérabilités, l'Alliance pour la Confiance Numérique montre qu'elle porte bien son nom, en chacune de ses initiales.
« A comme Alliance », tout d'abord : car l'ACN représente une filière. Or, la vulnérabilité d'une entité (État, administration, entreprise commerciale, association, collectivité) va bien au-delà du simple risque privé. La vulnérabilité concerne potentiellement tout l'écosystème dans lequel cette entité s'insère et auquel elle est numériquement connectée. La filière est donc l'échelon pertinent d'une réflexion qui porte sur les vulnérabilités de tout son écosystème.
« CN comme confiance numérique », ensuite : car s'il est bien un sujet qui détermine la confiance numérique, c'est la mise en place d'un système de protection des chercheurs de vul-nérabilités désireux de contribuer à la cybersécurité des entités dont les vulnérabilités ont été découvertes. Sans confiance numérique, les chercheurs de vulnérabilités ne seront jamais inci-tés à faire remonter le fruit de leurs recherches : qui risquerait des poursuites judiciaires, civiles et pénales, pour avoir simplement voulu lancer l'alerte, alors qu'il était tentant – mais illégal – de vendre ces vulnérabilités à prix d'or ?

À cet égard, les constats dressés dans les deux premiers chapitres de ce Livre Blanc sont éloquents : en France, le dispositif qui est censé organiser cette protection est mal paramétré en plusieurs points. En premier lieu, l'instrument législatif est moins agile que celui, utilisé avec succès dans d'autres pays, des bonnes pratiques. En deuxième lieu, la loi pénale française ne prévoit l'irresponsabilité pénale du découvreur de vulnérabilités dit « de bonne foi » qu'en cas de poursuites engagées par le procureur de la République sur dénonciation d'un agent public et non de celles qui résultent de la plainte par l'entité dont les vulnérabilités ont été mises au jour.

En troisième lieu, sur le plan de la gouvernance, le choix français d'un dispositif de recueil des signalements centralisé au niveau de l'ANSSI est appelé à montrer ses limites si, comme on l'espère, les remontées sont de plus en plus nombreuses. Or, d'autres pays comme les Pays-Bas et la Belgique pratiquent de manière efficace des dispositifs décentralisés. Nombreux sont donc les réglages qui pourraient utilement avoir lieu en France et en Union européenne.

Grâce à la qualité de ses analyses et à la force de ses propositions, cet ouvrage de l'ACN prend une position forte et claire en faveur des chercheurs de vulnérabilités qui se comportent de manière responsable. Si les lectrices et les lecteurs de ce Livre blanc lui accordent la forte attention qu'il mérite, l'ACN aura contribué à placer, en face d'un risque systémique, une pro-tection systémique à la hauteur des enjeux.

SOMMAIRE

INTRODUCTION

Un risque systémique. – Qu'il s'agisse d'un État, d'une administration, d'une entreprise, ou d'une association, le constat est le même : une vulnérabilité de cybersécurité ne fait pas courir qu'un risque privé, elle menace toute une chaîne d'entités connectées entre elles. C'est dire qu'elle représente un risque *systémique*.

Divulguer pour le meilleur ou pour le pire. – Divulguer cette vulnérabilité, c'est jouer un rôle décisif sur le sort de l'entité concernée et, potentiellement, de tout l'écosystème qui y est connecté. Car de deux choses l'une : soit la divulgation est récupérée à des fins malveillantes, et les attaques provoqueront les conséquences que l'on sait ; soit, au contraire, la divulgation intervient en renfort de sécurité, mettant l'entité concernée en position de corriger la faille avant les attaquants.
Dès lors, comment encadrer la divulgation de vulnérabilité ? La question est d'autant plus complexe à aborder que les textes européens et nationaux se multiplient dans des directions qui divergent.

Du défaut de sécurité à son exploitation. – Selon l'ANSSI, la vulnérabilité est une *« faute, par malveillance ou maladresse, dans les spécifications, la conception, la réalisation, l'installation ou la configuration d'un système, ou dans la façon de l'utiliser. [...] »*.

De récentes estimations suggèrent qu'un logiciel (software) compte en moyenne quatorze vulnérabilités, plus communément connues sous le nom de failles de sécurité. Une vulnérabilité est donc un défaut de sécurité, tandis qu'un exploit est un logiciel qui exploite une vulnérabilité.

Plus précisément, toujours selon l'ANSSI, un exploit est *« tout ou partie d'un programme permettant d'utiliser une vulnérabilité ou un ensemble de vulnérabilités d'un logiciel (du système ou d'une application) à des fins malveillantes. L'exploitation peut se faire directe-ment à partir du système ciblé si l'utilisateur malveillant possède un accès physique (local exploit), ou à distance s'il s'y connecte (remote exploit) »*.

Chaque point de connexion est une vulnérabilité potentielle. – Les cyberattaques contre les établissements publics de santé durant la pandémie de Covid-19, ou encore depuis le conflit russo-ukrainien ainsi que les attaques notamment contre l'Assemblée nationale au cours du mois de mars 2023, permettent d'illustrer le fait que les vulnérabilités sont présentes dans tous les systèmes d'informations et peuvent être exploitées tout autant à l'encontre d'individus, d'entreprises, d'infrastructure critiques que des États eux-mêmes. Pour atteindre ces cibles, comme les hôpitaux par exemple, l'attaque par *ransomware*[1] est le moyen la plus couramment utilisée par les acteurs malveillants.

Objet du rapport : les divulgations par un chercheur extérieur à l'entité. – Afin de réduire l'exposition générale aux attaques informatiques, il est donc essentiel de repérer les vulnérabilités et d'y remédier (les « patcher ») avant qu'elles ne soient exploitées par des personnes mal intentionnées. Les systèmes d'information seront d'autant mieux sécurisés que les failles seront découvertes et traitées en amont. Toutefois, s'il est vrai qu'une vulnérabilité peut être découverte par une personne interne à l'organisation qui gère le sys-tème d'information, la série de cas d'usage qui fait l'objet du présent rapport correspond à la divulgation effectuée par une personne extérieure à l'entité concernée.

Blanc, noir et gris : trois nuances d'intentions. – Or, la personne à l'origine de la découverte de la vulnérabilité peut être animée par des motivations diverses. Lorsque son objectif est de découvrir des failles de sécurité dans le seul but d'aider une organisation à se protéger, à la demande de cette dernière et dans un cadre juridique contractuellement défini, par exemple à travers le recours à des services de *pentest* (tests de pénétration) ou de *bug bounty*, l'on parlera alors de chercheur en vulnérabilité (« *white hat* »). À l'inverse, le pirate animé d'intentions malveillantes sera appelé « *black hat* ». Mais comme rien n'est « tout blanc ou tout noir », il existe des chercheurs de vulnérabilités qui sont dits « gris » (« *grey hat* »), et qui se trouvent entre ces deux cas de figure. Quoique les « gris » agissent à leur propre initiative, leur intention est de renforcer la sécurité informatique en découvrant des failles qu'ils peuvent ensuite faire connaitre à l'organisation qui gère le système d'information. Pour ces chercheurs « *grey hat* », se pose la question juridique de la légalité de leur action, ainsi que celle des conditions dans lesquelles ils peuvent, ou non, divulguer les vulnérabilités découvertes.

Divulgation au grand public. – En effet, la divulgation au grand public de la vulnérabilité d'un produit est souvent perçue comme nécessaire, car les utilisateurs des produits sont susceptibles de devoir entreprendre des actions pour corriger ou réévaluer les risques. En outre, la divulgation publique a pour avantage de faire perdre la valeur marchande d'une vulnérabilité sur le marché noir.

[1] Rançongiciel

Cependant, la divulgation publique a comme effet corollaire de faire connaître l'existence de la vulnérabilité à tous, y compris à des acteurs potentiellement malveillants. L'enjeu est donc d'amener un chercheur en vulnérabilités qui trouve une faille à la signaler au responsable du système pour que ce dernier puisse y remédier avant que l'existence de la vulnérabilité ne soit rendue publique. Il est donc nécessaire de mettre en place un système à même de permettre une divulgation des vulnérabilités qui ne porte préjudice ni au testeur ou au chercheur en vulnérabilités, si ces derniers sont de bonne foi, ni au responsable du système concerné par la vulnérabilité.

Nécessité de coordonner la divulgation de vulnérabilité. – C'est donc naturellement que l'on parle de « divulgation coordonnée de vulnérabilités », ou CVD (*Coordinated Vulnerability Disclosure*), c'est-à-dire d'un processus structuré de coopération au cours du-quel les vulnérabilités sont portées à la connaissance du propriétaire du système d'information. Cette divulgation coordonnée fournit à l'organisation l'occasion de remédier à la vulnérabilité avant que l'information détaillée concernant la vulnérabilité ne soit révélée à une tierce partie ou au grand public[2] , tout en permettant aux chercheurs en sécurité de signaler les failles de manière responsable, dans un cadre juridique adapté, et sans porter préjudice aux responsables des systèmes concernés.

Cadre juridique adéquat : loi ou bonnes pratiques ? – En France, le cadre juridique de l'article 47 de la loi pour une République numérique de 2016[3] instaure la possibilité de rapporter une vulnérabilité à l'Agence nationale de la sécurité des systèmes d'informations (ANSSI) sans craindre de poursuites de la part du Procureur de la République. Le divulgateur doit alors être de « bonne foi ». Néanmoins, au terme de plusieurs mois d'études, le présent rapport ne parvient pas à la conclusion que l'article 47 offre, à celui qui trouve la vulnérabilité, une protection complète. En outre, l'exemple d'autres pays, dont les Pays-Bas, suggère que la diffusion de bonnes pratiques produise des résultats tout aussi satisfaisants qu'une loi en termes de divulgation coordonnée de vulnérabilités.

Ces bonnes pratiques sont d'autant plus importantes que la législation de l'Union européenne brille par son absence en matière d'encadrement de divulgation des vulnérabilités, faute de définition harmonisée de ce qu'est un accès frauduleux à un système d'information, et en l'absence de protection minimale commune des chercheurs en vulnérabilités. Il en résulte des législations nationales très disparates entre les États membres, alors même que ce sujet est transfrontalier et appelle à une harmonisation minimale qui fournirait aux chercheurs en sécurité une protection lorsque ceux-ci contribuent à l'amélioration générale de la sécurité des systèmes.

[2] Règlement (UE) 2019/881 du Parlement européen et du Conseil du 17 avril 2019 relatif à l'ENISA (l'Agence de l'Union européenne pour la cybersécurité) et à la certification de cybersé-curité des technologies de l'information et des communications considérant 30
[3] LOI n° 2016-1321 du 7 octobre 2016 pour une République numérique

Obstacles à l'essor des processus de divulgation coordonnée. – Selon l'ENISA[4], quatre obstacles à la participation d'un chercheur en vulnérabilités dans un processus de divulgation de vulnérabilité ont été identifiés en 2023 :

1. L'insuffisance de la protection juridique des chercheurs en vulnérabilités, en plus des différences de régimes juridiques applicables entre les États membres de l'Union européenne et dans le monde ; par exemple, le régime juridique des Pays-Bas en la matière protège beaucoup plus les chercheurs qu'en France[5] ;

2. L'obscurité du cadre juridique en matière de responsabilités civiles, pénales, et administratives ;

3. La pauvreté du contrôle et du suivi des vulnérabilités, qui ne sont pas corrigées à temps ;

4. Le manque de communication entre les parties prenantes en la matière, en raison de la lourdeur administrative des procédures de divulgation coordonnée de vulnérabilités. De plus, les chercheurs ne sont pas toujours enclins aux inte-ractions avec les autorités publiques.

En somme, la divulgation coordonnée de vulnérabilités est un chantier majeur de la cybersécurité française et européenne. Au stade de l'état des lieux, il apparaît que les chercheurs de vulnérabilités sont face à des règles juridiques obscures (I), lorsqu'elles ne sont pas porteuses d'une dangereuse illusion de protection (II). Certains États membres de l'Union européenne ont pourtant adopté des modèles dont il serait bon de s'inspirer, que ce soit sur le plan national ou sur celui de l'Union européenne, où le cadre juridique est encore en construction (III).

[4] Développer des programmes nationaux sur la vulnérabilité, ENISA, 16 février 2023, page 21.
[5] V. en ce sens, prenant les Pays-Bas et la Belgique comme exemples de modèles à succès : John Morgan SALOMON & Nick KELLY, Protecting Responsible Cybersecurity Vulnerability Research, Lessons from the evolution of ethical hacking, and ensuring we can fix security holes before the bad guys get there, in European Cybersecurity Journal, vol. 9 (2023), Issue 1, p. 26 et s., spec. p. 34-35; v. également le rapport de l'OCDE sur ce thème, rendu public le 25 janvier 2023 : OECD, Good Practice Guidance on the Co-ordination of Digital Security Vulnerabilities, JT03511220, DSTI/CDEP/SDE(2021)9/FINAL.

LES CHERCHEURS DE VULNÉRABILITÉS FACE À L'OBSCURITÉ DU DROIT

Les motivations et les activités des chercheurs de vulnérabilité sont si nombreuses qu'il faut les ordonner si l'on veut, ensuite, traiter de manière adéquate les problématiques auxquelles ces chercheurs font face.

a) Pourquoi divulguer des vulnérabilités ? Un maquis d'intentions

On ne peut parler de divulgation de vulnérabilités sans s'intéresser aux motivations des chercheurs en vulnérabilités qui ont pénétré le système d'information. Les chercheurs en vulnérabilités étaient-ils motivés par la volonté d'accroître la sécurité d'un système ? Selon la réponse apportée à cette question, des sanctions judiciaires devraient s'appliquer ou non.

De manière générale, il convient de distinguer trois types d'acteurs[6] :

Les chercheurs en vulnérabilités ***« white hat »*** ou « hackeurs éthiques » agissent dans l'objectif d'améliorer la sécurité des systèmes d'information. Ils pratiquent des tests d'intrusion avec la permission du responsable du système et l'informent des vulnérabilités qu'ils découvrent.
Par exemple, le chercheur en vulnérabilités réalise des tests de sécurité par le biais de programmes de *bug bounty* établis par contrat entre une organisation et un organisateur de *bug bounty* qui autorise, définit et encadre le périmètre de la recherche. De tels programmes récompensent les chercheurs qui trouvent et signalent une vulnérabilité[7].

Plus la faille remontée est critique, plus la rémunération du chercheur en vulnérabilités, autrement appelée *bounty*, sera conséquente.

[6] « What's the difference between black, white and gray hat hackers?", [24] février [2022], Norton
[7] Guide de l'ENISA sur la divulgation de vulnérabilités, avril [2022], page [26].

Les chercheurs en vulnérabilités indépendants s'inscrivent sur une plateforme en ligne où les organisations peuvent établir le cadre contractuel des programmes qu'ils souhaitent lancer. Un processus de sélection est mis en place par la plateforme, les chercheurs en vulnérabilités n'agissant nullement sous couvert d'anonymat et devant passer par les fourches caudines d'un processus de *Know Your Customer* (« KYC ») afin de rejoindre la communauté de la plateforme de bug bounty.

Dans ce cas, le chercheur en vulnérabilités n'encourt aucune poursuite judiciaire tant qu'il agit dans le périmètre défini par le client qui a préalablement donné son consentement par contrat. La légalité de l'intrusion est ici encadrée grâce au principe de la liberté contractuelle. À défaut de contrat néanmoins, le bug bounty ne pourrait pas être considéré comme légal.

À l'inverse, les chercheurs en vulnérabilités « ***black hat*** » agissent dans un cadre d'illégalité, de la création de logiciels malveillants à leur vente, du cyberterrorisme à la cybercriminalité. Les black hats n'ont pas la volonté de divulguer des vulnérabilités pour améliorer la sécurité des systèmes d'information mais cherchent plutôt à les vendre sur le marché noir.
Les chercheurs en vulnérabilités *black hats* sont tout particulièrement intéressés par les vulnérabilités dites *zero-day*, c'est-à-dire des vulnérabilités encore inconnues du concepteur, et qui n'ont été ni identifiées, ni répertoriées, ni publiées. Les vulnérabilités *zero-day* ont une valeur très forte, qui peut-être aussi bien stratégique que marchande.

Elles peuvent être vendues au prix fort, notamment à des gouvernements qui souhaitent les acquérir pour leurs activités de renseignement[8]. Selon l'ENISA[9], le prix de vente d'une vulnérabilité *zero-day* de choix à un gouvernement varie entre 50 000 et 300 000 dollars et peut, dans certains cas, aller bien au-delà.

A mi-chemin entre ces deux types de chercheurs en vulnérabilités, il existe une troisième catégorie : les chercheurs en vulnérabilités « ***grey hat*** ». Le *grey hat* n'agit pas toujours en faveur de la sécurité et peut parfois utiliser des moyens illégaux pour parvenir à ses fins.

[8] Guide de l'ENISA sur la divulgation de vulnérabilités, avril 2022, page 30.
[9] Guide de l'ENISA sur la divulgation de vulnérabilités, avril 2022, page 47.

L'exemple le plus parlant de chercheurs en vulnérabilités grey hat est celui qui pénètre et se maintient illégalement dans un Système de Traitement Automatisé des Données (STAD), découvre une vulnérabilité et en informe le propriétaire. Un autre exemple est celui du chercheur en vulnérabilités qui découvre une vulnérabilité dans un STAD et laisse une période de grâce à la personne responsable, avant de divulguer publiquement la vulnérabilité.

Le cas du chercheur en vulnérabilités *grey hat* est le plus complexe à appréhender d'un point de vue juridique car ce dernier peut commettre une infraction pénale (pénétrer de manière illégale dans un système informatique) pour atteindre un objectif louable (améliorer la sécurité d'un système). Selon les pays, les lois et les pratiques sont plus ou moins bienveillantes à l'égard des chercheurs en vulnérabilités *grey hats*.

En l'absence d'encadrement juridique, les réponses apportées à ces situations sont donc aléatoires et, en tout état de cause insuffisantes, dans la mesure où elles ne parviennent pas toujours à combiner à la fois une protection adéquate du chercheur, mais aussi celle du système concerné et les impératifs légitimes, notamment techniques, nécessaires à la correction de la vulnérabilité.

Il est donc nécessaire de mettre en place un système qui permette à tout chercheur en vulnérabilités bien intentionné de divulguer une vulnérabilité sans que cela ne crée de risque pour la sécurité du système concerné ou que cela n'implique de poursuites judiciaires à l'encontre du chercheur en vulnérabilités. Un système de divulgation coordonnée de vulnérabilités peut être mis en place au sein d'une entreprise ou d'un organisme public pour permettre un signalement de la vulnérabilité directement à l'entité concernée.

Il peut également impliquer un acteur intermédiaire. Certaines entreprises proposent ce service, à travers des Programmes de divulgation de vulnérabilités (*Vulnerability Disclosure Program « VDP »*) qui permettent de mettre en place un canal sécurisé en insérant un fichier texte à la racine de son site, afin de recueillir les rapports de vulnérabilités que pourraient transmettre des tiers.

Ce mécanisme permet de centraliser les remontées tout en réduisant les risques numériques. Sans ce processus, le chercheur pourrait abandonner l'idée de transmettre la vulnérabilité, ce qui empêcherait l'entreprise d'en avoir connais-sance afin de pouvoir y remédier. L'autre situation à risque serait que le chercheur tente de transmettre la vulnérabilité par l'envoi d'un simple courriel non sécurisé ou pouvant être adressé au mauvais destinataire, exposant ainsi l'entreprise à des violations de données ou des fuites de données si aucun chiffrement n'a préalablement été mis en place.

En ce sens, la directive européenne 2019/1937[10] a été adoptée afin de protéger davantage les lanceurs d'alerte (*whistleblowers*) qui contribuent à prévenir des dommages ou détecter des menaces ou des préjudices pour l'intérêt public. En raison d'une protection qui s'avérait insuffisante et inégale à échelle européenne, la crainte des représailles pouvait dissuader les lanceurs d'alerte.

Par la suite, la Commission Nationale de l'Informatique et des Libertés (CNIL) a mis en place un dispositif afin de recueillir les signalements des lanceurs d'alerte. Ce mécanisme est réservé « *aux personnes physiques identifiées qui signalent ou divulguent, sans contrepartie financière directe et de bonne foi, des informations portant sur des données personnelles, et plus particulièrement (...) un crime, un délit, une menace ou un préjudice pour l'intérêt général* »[11]. Pour cela, le lanceur d'alerte peut suivre une procédure interne de signalement si celle-ci existe au sein de l'organisme qui comportent la vulnérabilité repérée.

Pour cela, le lanceur d'alerte peut suivre une procédure interne de signalement si celle-ci existe au sein de l'organisme qui comportent la vulnérabilité repérée. Cependant, si cette action expose le lanceur d'alerte à un quelconque risque qui engendrerait des mesures de représailles, le lanceur d'alerte peut émettre un signalement directement auprès de la CNIL.

[10] Directive (UE) 2019/1937 du Parlement européen et du Conseil du 23 octobre 2019 sur la protection des personnes qui signalent des violations du droit de l'Union
[11] « Lanceurs d'alerte : adresser une alerte à la CNIL », CNIL, 24 novembre 2022

Pour cela, le lanceur d'alerte peut suivre une procédure interne de signalement si celle-ci existe au sein de l'organisme qui comportent la vulnérabilité repérée. Cependant, si cette action expose le lanceur d'alerte à un quelconque risque qui engendrerait des mesures de représailles, le lanceur d'alerte peut émettre un signalement directement auprès de la CNIL.

Le dispositif CNIL protège le lanceur d'alerte, via notamment :

1. Une garantie de confidentialité de l'identité ;

2. Une irresponsabilité civile : à condition que le lanceur d'alerte ait des motifs raisonnables pour considérer que la procédure était pertinente à la sauvegarde des intérêts menacés ;

3. Une irresponsabilité pénale ;

4. Une protection contre des mesures de représailles.

Les chercheurs en vulnérabilités pourraient utiliser ce mécanisme de la même manière que les lanceurs d'alerte, puisqu'ils permettent également de signaler les risques de menaces que pourraient entrainer des vulnérabilités. Il y a donc un intérêt à uniformiser la protection de ces deux acteurs, ce qui permettrait de traiter également la question de l'éthique dans la divulgation de vulnérabilités.

Pour cela, il s'avère nécessaire de sensibiliser largement autour de l'apport de ces remontées de vulnérabilités, permise par les chercheurs actifs dans un cadre défini et sécurisé, en termes de protection et de sécurité des systèmes informatiques en général. Souvent perçus comme malveillants, les chercheurs en vulnérabilités sont parfois bien intentionnés et méritent que leurs travaux soient reconnus et pris en compte.
Une sensibilisation au niveau national semble alors nécessaire afin de dédiaboliser le rôle de ces chercheurs et d'entamer une impulsion étatique en faveur de l'adoption d'une politique nationale de divulgation coordonnée de vulnérabilités.

b) Comment divulguer des vulnérabilités ? La voie de la coordination

La divulgation publique a certains aspects positifs : le premier est l'information du public afin que celui-ci puisse prendre ses précautions, tel qu'en faisant les mises à jour dès que celles-ci sont proposées. Un autre point également important est que plus il y a de personnes au courant de la vulnérabilité, plus il y a de personnes qui cherchent à y remédier. Les membres de la communauté du logiciel libre sont très réactifs sur de tels sujets et peuvent travailler à plusieurs centaines voire plusieurs milliers sur le problème qui sera donc susceptible d'être résolu plus rapidement et de manière plus efficace grâce à l'aide des pairs. Par ailleurs, la menace d'une divulgation publique peut aussi être vue comme une manière d'accélérer sa prise en compte effective par l'organisation responsable du système d'information qui souhaitera y remédier avant qu'elle ne devienne publique.

À l'inverse, une divulgation publique complète sans correctifs de sécurité peut générer une très grande insécurité : si une importante faille est découverte, facilement accessible, et difficilement corrigeable, alors ce sont des millions de personnes, des entreprises voire des États qui sont susceptibles d'être victimes de personnes mal intentionnées.

Il peut être long et complexe d'apporter les correctifs de sécurité à une vulnérabilité d'un logiciel et cela est encore plus long lorsqu'il est question de matériel, ou si le logiciel ou système concerné s'insère dans un ensemble informatique plus large. Si une vulnérabilité est rendue publique alors qu'un correctif n'a pas été déployé, c'est une porte ouverte sur tous les systèmes d'information concernés. Si une faille qui était connue de quelques chercheurs en vulnérabilités devient publique, davantage de chercheurs en vulnérabilités *black hats* peuvent saisir cette opportunité pour compromettre le système d'information.

Il est donc nécessaire d'encadrer cette divulgation afin de parvenir à obtenir les résultats espérés en termes de sécurité et les effets contraires ou les intentions malveillantes. C'est la raison pour laquelle de nombreuses organisations de cybersécurité, telles que l'ENISA, prônent la divulgation coordonnée de vulnérabilités.

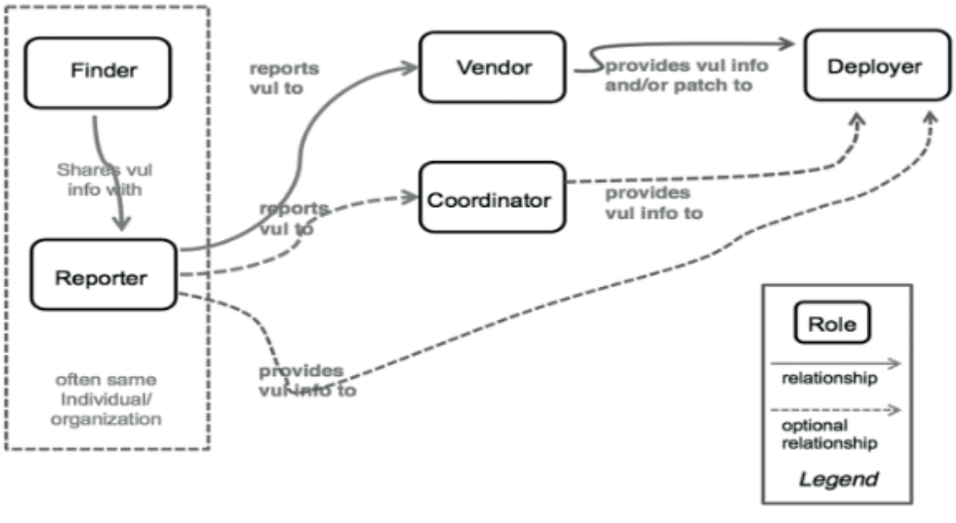
Ce processus permet une coordination entre le chercheur en vulnérabilité et le responsable du système, qui laisse le temps et la liberté au responsable de remédier à la vulnérabilité avant que celle-ci ne soit rendue publique, ou non, selon des critères définis et objectifs prenant en compte les circonstances, la criticité du système, le temps nécessaire au déploiement du correctif, etc.

Ce processus permet une coordination entre le chercheur en vulnérabilité et le responsable du système, qui laisse le temps et la liberté au responsable de remédier à la vulnérabilité avant que celle-ci ne soit rendue publique, ou non, selon des critères définis et objectifs prenant en compte les circonstances, la criticité du système, le temps nécessaire au déploiement du correctif, etc.

Cinq acteurs différents peuvent être identifiés dans le cadre de la divulgation coordonnée de vulnérabilités : le **découvreur** de la vulnérabilité, le **rapporteur** de celle-ci, le **vendeur** du produit vulnérable, le **déployeur** (qui déploie le correctif ou prends des mesures pour combler la vulnérabilité) ainsi que le **coordinateur**[12].

Le rôle de coordinateur peut être rempli par un CERT (*Computer Emergency Response Team*) ou CSIRT (*Computer Security Incident Response Team*), c'est-à-dire une équipe dédiée à la veille et aux réponses à des attaques informatiques. En France, c'est le CERTFR qui s'occupe de la sécurité des systèmes d'informations, en coopération avec l'ANSSI.

Figure 1. Relationships among actors in the CVD process



Source: Allen D. Householder, Garret Wassermann, Art Manion and Chris King, "The CERT Guide to Coordinated Vulnerability Disclosure", Software Engineering Institute, Carnegie Mellon University, August 2017.

[12] Le guide du CERT sur la divulgation coordonnée de vulnérabilités, Université de Carnegie Mellon, août 2017

Lorsque deux parties seulement prennent part au processus – le découvreur et le vendeur qui corrige la vulnérabilité – le schéma est assez simple. Cependant, dès lors qu'on se trouve confronté à une vulnérabilité qui implique de multiples acteurs, le processus de divulgation coordonnée est plus complexe car il faut réussir à synchroniser le développement, le test et la publication par les différentes parties. Le *Vulnerability Coordination Group* de l'organisation « *FIRST* » a publié un rapport à ce sujet, intitulé « *Guidelines and Practices for Multi-Party Vulnerability Coordination and Disclosure* »[13].

Selon la norme ISO/IEC 30111, il est possible d'identifier différentes phases dans la divulgation. Dans un premier temps, la faille est découverte, avant d'être rapportée, que ce soit au vendeur du produit ou à une tierce partie. Ensuite, vient la phase de la validation et du triage, durant laquelle la vulnérabilité est analysée et confirmée par le vendeur du produit, avant toute prise de décision en matière de délai et de réponse.
Puis un plan d'assainissement est développé et testé, tel un correctif de sécurité par exemple. Le public est ensuite informé de la vulnérabilité et du correctif, avant que ledit correctif ne soit déployé à tous les systèmes vulnérables. La vulnérabilité peut se voir attribuer un identifiant CVE (*Common Vulnerabilities and Disclosures*)[14] par le MITRE, organisation américaine à but non lucratif. Un identifiant CVE associé à une vulnérabilité suppose que celle-ci ait été identifiée et permet au MITRE de la classer dans une base de données de vulnérabilités recensées. La base de données inclut également les dates auxquelles ces vulnérabilités ont été découvertes, si l'alerte est toujours en cours ou si la vulnérabilité a reçu un correctif.

La divulgation coordonnée de vulnérabilités est le système le plus à même de protéger à la fois les intérêts du chercheur en vulnérabilités et ceux du responsable du système. La divulgation coordonnée de vulnérabilités peut cependant prendre de multiples formes, comme le démontre un simple tour d'horizon dans les pays européens. En France, la politique publique de divulgation coordonnée de vulnérabilités se focalise sur l'ANSSI comme point de contact pour le chercheur en vulnérabilités et intermédiaire. Parallèlement, certaines entreprises mettent en place leur propre politique de divulgation de vulnérabilités mais on ne peut à ce jour parler de pratique généralisée. Le système français a ses limites, notamment en termes de protection accordée au chercheur en vulnérabilités.

[13] *Lignes directrices et pratiques pour la coordination et la divulgation multipartite de vulnérabili-tés, FIRST, juillet 2017*
[14] *Page du MITRE sur les CVE*

II. LA PROTECTION DES CHERCHEURS EN DROIT FRANÇAIS : UN DANGEREUX TROMPE-L'ŒIL

La divulgation coordonnée de vulnérabilité est introduite par la loi pour une République numérique du 7 octobre 2016 mais reste encore insuffisante, dans la mesure où les chercheurs en vulnérabilités peuvent toujours faire l'objet de poursuites judiciaires, ce qui limite la prise en compte des vulnérabilités inconnues par les organisations mais connues de ces chercheurs. Pourtant, certains voisins fournissent des exemples de mise en œuvre de politique de divulgation coordonnée de vulnérabilités à la France, dont elle pourrait s'inspirer.

a) Une protection affichée

Les actions des chercheurs en vulnérabilités mal intentionnées sont illégales et considérées en France comme des infractions sanctionnées par l'article 323-1 du Code pénal. Cet article dispose que « [l]e fait d'accéder ou de se maintenir, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données est puni de deux ans d'emprisonnement et de 60 000 € d'amende.

Lorsqu'il en est résulté soit la suppression ou la modification de données contenues dans le système, soit une altération du fonctionnement de ce système, la peine est de trois ans d'emprisonnement et de 100 000 € d'amende.
Lorsque les infractions prévues aux deux premiers alinéas ont été commises à l'encontre d'un système de traitement automatisé de données à caractère personnel mis en œuvre par l'État, la peine est portée à cinq ans d'emprisonnement et à 150 000 € d'amende. »

Cet article est la transposition de l'article 3 de la directive « Cybercrime » (2013/40 UE)[15], qui pose un socle minimal en ce qui concerne la répression des cyber infractions. Ainsi, l'article 3 dispose que « [l]es États membres prennent les mesures nécessaires pour ériger en infraction pénale punissable l'accès sans droit, lorsqu'il est intentionnel, à tout ou partie d'un système d'information, lorsque l'acte est commis en violation d'une mesure de sécurité, au moins lorsqu'il ne s'agit pas de cas mineurs. »

[15] Directive 2013/40/UE du Parlement européen et du Conseil du 12 août 2013 relative aux attaques contre les systèmes d'information et remplaçant la décision-cadre 2005/222/JAI du Conseil

La directive « *Cybercrime* » ne mentionne aucune exemption de poursuites judiciaires pour les chercheurs en vulnérabilités bien intentionnés. Les États membres de l'Union européenne ne sont donc pas tenus d'introduire une telle exemption dans leur législation nationale.
Néanmoins, les chercheurs en vulnérabilités *grey hats* peuvent échapper à la qualification d'infraction grâce à l'article 47 de la Loi pour une République numérique[16] du 7 octobre 2016. Cet article dispose que « [l]e chapitre Ier du titre II du livre III de la deu-xième partie du code de la défense est complété par un article L. 2321-4 ainsi rédigé :

« Art. L. 2321-4.-Pour les besoins de la sécurité des systèmes d'information, l'obligation prévue à l'article 40 du code de procédure pénale n'est pas applicable à l'égard d'une personne de ***bonne foi*** *qui transmet à la seule autorité nationale de sécurité des systèmes d'information une information sur l'existence d'une vulnérabilité concernant la sécurité d'un système de traitement automatisé de données. « L'autorité préserve la confidentialité de l'identité de la personne à l'origine de la transmission ainsi que des conditions dans lesquelles celle-ci a été effectuée.*
« L'autorité peut procéder aux opérations techniques strictement nécessaires à la caractérisation du risque ou de la menace mentionnés au premier alinéa du présent article aux fins d'avertir l'hébergeur, l'opérateur ou le responsable du système d'information. » »

L'article 47 protège donc un chercheur en vulnérabilités « de bonne foi » des poursuites engagées par le procureur de la République au titre de l'article 40 du Code de procédure pénale.
Une personne qui découvre une vulnérabilité ne sera pas poursuivie si elle transmet à l'ANSSI l'information de l'existence d'une vulnérabilité. À cette fin, le site internet de l'ANSSI contient une rubrique spéciale dédiée à la divulgation de vulnérabilités.

La promulgation d'une loi en la matière a entraîné une prise de conscience de l'importance de ce phénomène et de la nécessité de l'encadrer pour que les personnes bien intentionnées ne soient pas sanctionnées. L'article 47 de cette même loi instaure ainsi un processus de divulgation coordonnée de vulnérabilités mais nécessite tout de même d'être complété pour aboutir.
En effet, l'État en la matière devrait impulser aux entités le composant (ministères, collectivités territoriales, établissements publics, ...) la mise en œuvre de canaux dédiés à la remontée de vulnérabilités en leur sein pour les chercheurs en vulnérabilités.

[16] *LOI n° 2016-1321 du 7 octobre 2016 pour une République numérique*

Ainsi, ces canaux permettraient d'accroitre la protection juridique des chercheurs et présentent un avantage considérable pour les organisations qui peuvent bénéficier des travaux des chercheurs en vulnérabilités de bonne foi et corriger la faille.

b) Une protection illusoire

Lors de la discussion de ce texte à l'Assemblée nationale, plusieurs députés souhaitaient une protection accrue, ce qui les avait amenés à proposer « *l'amendement Bluetouff* »[17] en janvier 2016. Cet amendement visait à ajouter un nouvel alinéa à l'article 323-1 du code pénal, ainsi rédigé :

« Toute personne qui a tenté de commettre ou commis le délit prévu au présent article est exempte de peine si elle a immédiatement averti l'autorité administrative ou judiciaire ou le responsable du système de traitement automatisé de données en cause d'un risque d'atteinte aux données ou au fonctionnement du système. »

Cet amendement tirait son nom de l'arrêt Bluetouff de la chambre criminelle de la Cour de cassation du 20 mai 2015[18]. Olivier Laurelli, blogueur connu sous le pseudonyme « Bluetouff », est condamné en février 2014 par la Cour d'appel de Paris pour maintien frauduleux dans un STAD, ainsi que pour vol de fichiers à l'Agence Nationale de Sécurité Sanitaire de l'Alimentation, de l'Environnement et du travail (ANSES).

Olivier Laurelli a accédé à des fichiers confidentiels par le biais d'un moteur de recherche, l'ANSES ayant un défaut de sécurisation de son site internet et donc de ses données. En remontant l'arborescence du site, Olivier Laurelli était tombé sur une page demandant une authentification : le blogueur savait donc qu'il se maintenait de manière irrégulière dans un STAD. Il a également fait une copie de plusieurs gigas de données, dont il a publié une partie sur son site. Relaxé en première instance, Olivier Laurelli est finalement condamné par la Cour d'appel à 3000 euros d'amende pour maintien frauduleux dans un STAD (article 323-1 du Code pénal) et soustraction de données (article 311-1 du Code pénal). Son pourvoi en cassation est rejeté.

[17] Amendement n°271, 15 janvier 2016. Disponible sur le lien suivant : https://www.assemblee-nationale.fr/14/amendements/3399/AN/271.asp
[18] Cour de Cassation, criminelle, Chambre criminelle, 20 mai 2015, 14-81.336

L'amendement Bluetouff a finalement été rejeté par l'Assemblée nationale. Les chercheurs en vulnérabilités bien intentionnés ne peuvent donc que bénéficier de l'article 47 de la loi pour une République numérique, qui est plus restrictif quant à la procédure à suivre par le chercheur en vulnérabilités. Celui-ci doit obligatoirement s'adresser à l'ANSSI et ne peut pas alerter le responsable du système directement.

En outre, l'article 47 ne protège que des poursuites engagées par le procureur de la République sur dénonciation d'un agent public et non de celles engagées par le responsable du système concerné par la vulnérabilité. Ce dernier peut engager des poursuites à l'encontre d'un chercheur en vulnérabilités, même si celui-ci est bien intentionné. L'article 323-1 du Code pénal est donc toujours applicable aux chercheurs, même s'ils sont de « *bonne foi* ». L'immunité pénale totale a été refusée par les législateurs français, de même que les propositions d'une immunité concernant uniquement les infractions d'accès et de maintien frauduleux dans un STAD et non les infractions de modification ou de suppression des données (afin d'éviter qu'un chercheur en vulnérabilités mal intentionné ne s'introduise dans un système, n'injecte des charges malveillantes - *malwares* - et se targue ensuite d'avoir découvert une vulnérabilité).

Les chercheurs s'exposent donc à des poursuites dans le domaine pénal, mais sont également susceptibles d'être poursuivis, notamment sur le fondement du droit civil, du droit des contrats et de la propriété intellectuelle.

Dans les faits cependant, l'ANSSI négocie avec le vendeur si celui-ci a l'intention de se retourner contre le chercheur, afin qu'il n'y ait pas de dépôt de plainte, pour encourager la remontée des failles et leur correction.

L'expression « *qui transmet à la seule autorité nationale de sécurité des systèmes d'information* » sous-entend que le chercheur ne doit pas divulguer la faille à qui que ce soit d'autre, s'il souhaite conserver la protection accordée par l'article L2321-4 du Code de la défense. Ainsi, toute divulgation publique faite par un chercheur en vulnérabilités est exclue de ce schéma.

c) Sortir de l'intermédiation : un tour d'horizon des alternatives

Le modèle français se caractérise par une politique de divulgation de vulnérabilités qui repose essentiellement sur l'intermédiation de l'ANSSI. Ce modèle vise à garantir l'anonymat du chercheur en vulnérabilités, sans doute adapté pour les cas les plus sensibles, même si l'étude des textes français a montré que le chercheur n'était pas à l'abri de poursuites judiciaires.

En outre, le modèle français présuppose un dimensionnement adapté des moyens et donc une réactivité adéquate de l'ANSSI afin que les vulnérabilités soient traitées dans les plus brefs délais. Le risque majeur est que l'ANSSI soit submergée par les signalements de vulnérabilités, ce qui ralentirait son temps de réaction. Tel est par exemple le cas au Japon, qui a également mis en place un système centralisé. En effet, au Japon les chercheurs en sécurité doivent signaler les vulnérabilités à une agence gouvernementale (*Information-technology Promotion Agency*). L'agence, conjointement avec le JPCERT, se charge de contacter le vendeur ou le développeur pour coordonner le processus de divulgation[19]. Ce système a été un succès depuis son origine, au milieu des années 2000. Cependant, depuis plusieurs années, le nombre de signalements a considérablement augmenté et le système se retrouve engorgé[20].

D'autres pays ont fait le choix de favoriser le contact direct entre les chercheurs en sécurité et les responsables de système. Cette alternative a le mérite de limiter le risque de poursuites judiciaires et de mettre en place une collaboration entre chercheurs et responsables de système.

L'exemple des Pays-Bas

En Union européenne, les Pays-Bas ont été l'exemple le plus flagrant de l'efficacité du modèle désintermédié de divulgation coordonnée de vulnérabilités. Dès janvier 2013, le *Nationaal CyberSecurity Centrum* (NCSC), l'agence néerlandaise de cybersécurité, a publié des lignes directrices relatives à la politique de divulgation de vulnérabilités. Une version révisée[21] du document est disponible depuis 2018. Ces lignes directrices sont essentiellement destinées aux responsables de systèmes d'information. Elles ont été conçues comme une série de recommandations pour aider une organisation à créer sa propre politique de divulgation coordonnée de vulnérabilités.

[19] *Lignes directrices sur la gestion des vulnérabilités, JPCERT CC, 11 mai 2019*
[20] *Protéger l'Europe des vulnérabilités des logiciels, Centre européen d'études politiques (CEPS), 28 juin 2018, p. 39*
[21] *« Divulgation coordonnée de vulnérabilités : les lignes directrices, Centre national de cybersécurité Néerlandais, 2 octobre 2018*

De nombreuses entreprises, notamment du secteur des télécommunications, ont publié leur politique de divulgation de vulnérabilités à la suite de la publication de ces lignes directrices. Le modèle néerlandais est souvent considéré comme une réussite en raison des nombreux signalements de vulnérabilités effectués dans le cadre des politiques de divulgation mises en place par les organisations (tant privées que publiques)[22].

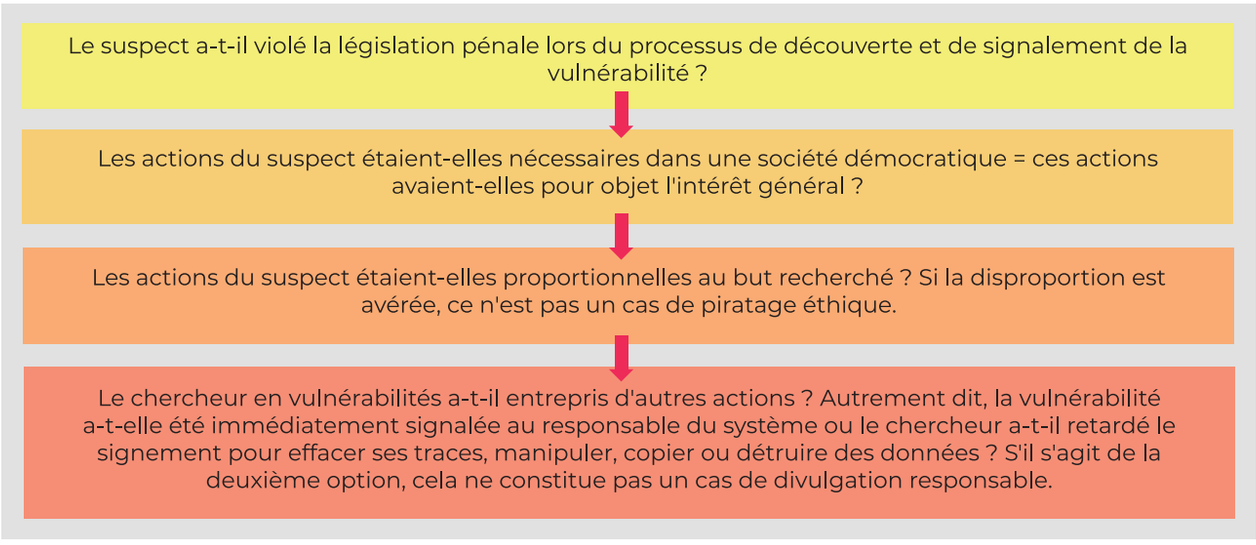
Il crée un environnement plus sûr pour les chercheurs car chaque politique de divulgation de vulnérabilités explique sous quelles conditions un chercheur n'encourra pas de poursuites judiciaires (pénales ou civiles). Cette volonté de « dédramatiser » la divulgation de vulnérabilités est parfaitement illustrée par la première page des lignes directrices du *Nationaal CyberSecurity Centrum*, qui montre le buste d'un jeune homme arborant fièrement un T-shirt sur lequel il est inscrit « j'ai piraté le gouvernement néerlandais et tout ce que j'ai eu c'est ce T-shirt minable » (« *I hacked the Dutch government and all I got was this lousy t-shirt* »). Ce modèle a également le mérite de sensibiliser les responsables de système au thème des vulnérabilités[23].

Les lignes directrices indiquent qu'il doit y avoir le moins d'intermédiaires possibles entre la personne qui signale une vulnérabilité et la personne chargée de résoudre le problème au sein d'une organisation. Néanmoins, si une vulnérabilité affecte plusieurs systèmes, il est judicieux d'informer plusieurs parties, précise le document. L'agence néerlandaise de cybersécurité ou d'autres acteurs de la communauté peuvent alors jouer un rôle de coordination[24].

À la suite de la publication des lignes directrices par le *Nationaal CyberSecurity Centrum*, le bureau du procureur néerlandais a envoyé une lettre à tous les départements judiciaires pour les informer de cette évolution. La lettre explique que, si le « *hacking éthique* » n'est pas reconnu en tant que tel dans la loi néerlandaise, la dimension éthique doit être un facteur de premier plan lorsqu'il s'agit de déterminer si une action constitue une violation de la législation pénale. Si un chercheur en vulnérabilités trouve une vulnérabilité et la signale au responsable du système, cela constitue a priori un acte de piratage éthique. En revanche, s'il y a des indices qui tendent à démontrer que le chercheur en vulnérabilités ne s'est pas contenté de signaler la faille, une enquête criminelle doit avoir lieu. Tel peut être le cas si le chercheur en vulnérabilités a copié des données sensibles[25].

En résumé, un procureur néerlandais doit se poser les questions ci-dessous[26] lorsqu'il aborde un cas de divulgation de vulnérabilité :

[22] *« Protéger l'Europe des vulnérabilités des logiciels, Centre européen d'études politiques (CEPS), 28 juin 2018, p. 23*
[23] *Idem.*
[24] *Divulgation coordonnée de vulnérabilités : les lignes directrices, Centre national de cybersécurité Néerlandais, 2 octobre 2018*
[25] *Guide de la divulgation de vulnérabilités, avril 2022, ENISA, p51.*
[26] *Protéger l'Europe des vulnérabilités des logiciels, Centre européen d'études politiques (CEPS), 28 juin 2018, p. 52*



L’exemple de la Belgique

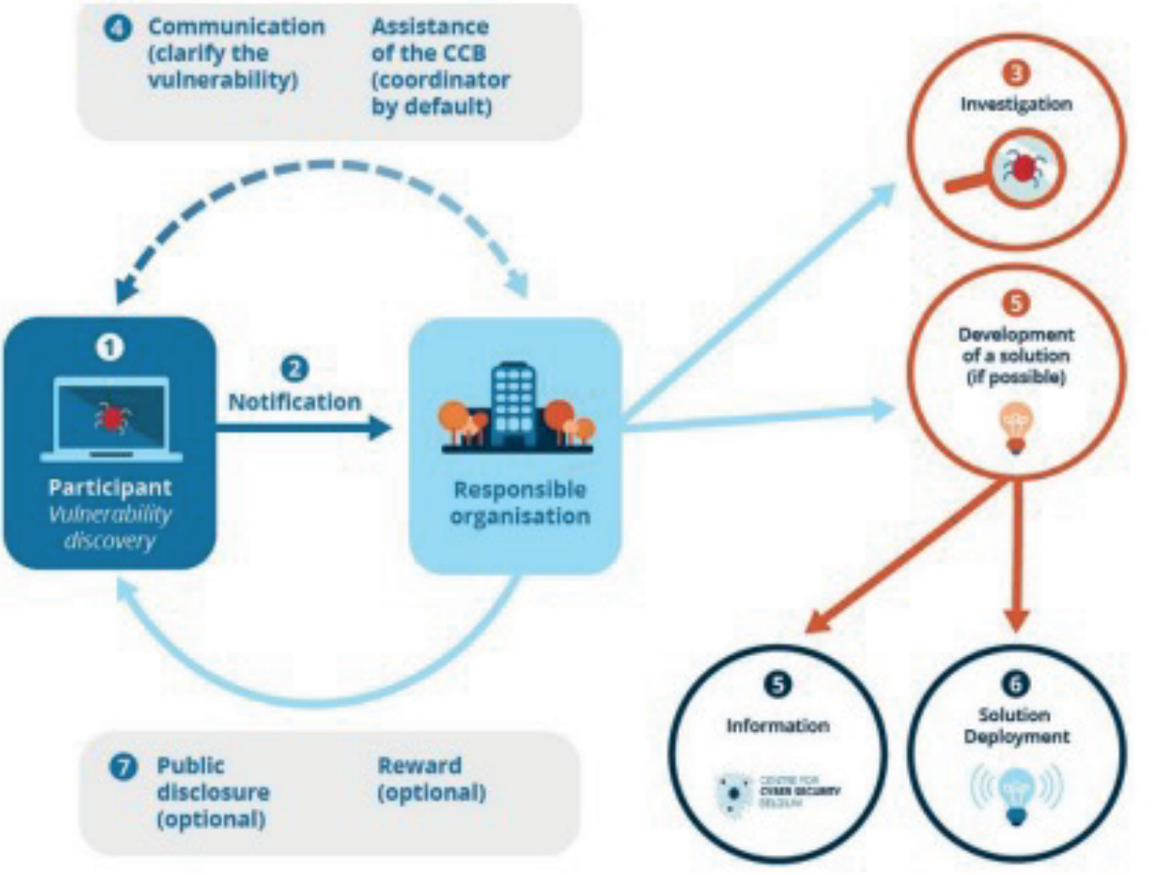
Au début de l’année 2023, la Belgique a adopté une loi portant sur le nouveau cadre juridique pour le signalement de vulnérabilités informatiques. À ce jour, le cadre juridique du Centre pour la Cybersécurité Belge (CCB) demeure celui qui se rapproche le plus d’une protection complète. Désormais, les chercheurs en vulnérabilités peuvent effectuer des recherches au sein de n’importe quelle entreprise, dans le but d’en vérifier la sécurité sans risquer d’être poursuivis. Précédemment, il était permis aux organisations d’autoriser les chercheurs en vulnérabilités bien intentionnés à réaliser des intrusions pour détecter des vulnérabilités. À présent ces derniers peuvent agir sans autorisation préalable, mais doivent cependant respecter quelques règles strictes. Le nouveau cadre juridique, placé sous le contrôle du CCB prévoit un processus de signalement des vulnérabilités qui protège les chercheurs bien intentionnés contre des poursuites judiciaires si :

- Le chercheur en vulnérabilités agit sur le territoire belge,
- Le chercheur en vulnérabilités informe le propriétaire du système vulnérable dès que possible (idéalement dans les 72 heures),
- Le chercheur en vulnérabilités, après avoir informé le propriétaire du système, soumet un rapport sur la vulnérabilité au CCB dès que possible si l’organisation concernée ne dispose pas de politique de divulgation de vulnérabilités ou si des difficultés entrent en jeu,

- Le chercheur en vulnérabilités a agi sans intention malveillante ou frauduleuse,
- Le chercheur en vulnérabilités a agi de manière nécessaire et proportionnée (la plupart des politiques de divulgation des vulnérabilités déclarent que les attaques par force brute, les DDoS, l'ingénierie sociale et le phishing sont inutiles et disproportionnées),
- Le chercheur en vulnérabilités ne met pas à la disposition du public les informa-tions acquises lors d'un piratage éthique sans l'approbation du CCB.

De plus, aucun paiement ne pourra être réclamé en échange, sauf dans le cadre d'un contrat conclu en amont.
Les pays européens ne disposant pas de politiques de divulgation coordonnée de vulnérabilités pourraient s'inspirer de cette loi en choisissant de limiter le nombre d'intermédiaires, tels que l'ANSSI, en signalant directement la vulnérabilité à l'organisation. Ce nouveau cadre juridique permettrait à la fois de renforcer la sécurité des organisations tout en assurant davantage de protection juridique aux chercheurs en sécurité.

Figure 3 – CCB CVD process (I)



1. Participant finds a vulnerability in the context of a CVDP.
2. Participant informs the responsible organisation based on the CVDP details.
3. The responsible organisation analyses the vulnerablity.
4. Communication between the participant and the responsible organisation continues to clarify the vulnerability. assistance from the CCB (as coordinator by default) can be asked if there is a lack of communication in this process.
5. A solution is developed (if possible). In case the vulnerability could affect also others organisations, the responsible organisation informs the CCB.
6. The responsible organisation deploys the solution to its users or customers.
7. Approval for public disclosure can be discussed and a reward can be given based on the CVDP.

Source: Centre for Cyber Security Belgium

L’exemple des États-Unis

Aux États-Unis, les entreprises ont commencé à publier leur politique de divulgation au début des années 2010. Les agences fédérales ont alors emboîté le pas pour faciliter la mise en place de politiques de divulgation tant dans les organisations privées que publiques. En 2015, l’Agence fédérale des télécommunications (*National Telecommunication and Information Administration*) a réuni les parties prenantes du processus de divulgation pour rédiger un modèle de divulgation coordonnée de vulnérabilités. Ce modèle visait à aider les organisations à entreprendre leur propre politique de divulgation coordonnée de vulnérabilités. D’autres agences fédérales ont suivi, telles que la Commission fédérale du commerce (*Federal Trade Commission*), l’Agence des produits alimentaires et médicamenteux (*Food and Drug Administration*) et l’Agence de la sécurité routière (*National Highway Transportation and Safety Administration*). Même le Département de la défense (*Department of Defence*) a rejoint la tendance en publiant en 2016 une politique de divulgation de vulnérabilités.

Les lois américaines n’ont pas été modifiées depuis l’émergence de ces politiques mais c’est plutôt leur interprétation et leur application qui diffèrent aujourd’hui. La loi *anti-hacking* (*Computer Fraud and Abuse Act – CFAA*) est toujours utilisée pour protéger les systèmes d’information américains. Néanmoins, le Département de la Justice a publié des orientations pour que les procureurs fédéraux s’assurent que les poursuites n’aient lieu que dans le cas où elles servent un « *intérêt fédéral substantiel* ». En mai 2022, le minis-tère de la Justice a précisé que dans ce cadre, la recherche de vulnérabilités de bonne foi ne devait pas être poursuivie par la Justice.

Les enseignements à tirer

Les exemples néerlandais, belge et américain présentent des systèmes décentralisés qui favorisent la divulgation coordonnée de vulnérabilités et protègent les chercheurs en sécurité d’éventuelles poursuites. Les exemples des Pays-Bas et des États-Unis sont la preuve qu’il n’est pas toujours nécessaire de légiférer pour créer un écosystème à même d’atteindre ces objectifs. Des réunions avec les parties prenantes et la rédaction de lignes directrices peuvent être des moyens tout aussi efficaces. La Belgique, quant à elle, démontre que la publication d’une loi reste une solution fiable. Elle offre la possibilité aux entreprises de se doter d’une politique de divulgation coordonnée de vulnérabilités qui leur est propre et à l’État d’intervenir de manière subsidiaire lorsqu’une telle politique n’existe pas.

S'il est essentiel d'encourager les entreprises à adopter leur propre politique de divulgation coordonnée de vulnérabilités, la création d'une obligation peut faire débat. Les politiques de divulgation coordonnée de vulnérabilités requièrent un niveau adéquat d'organisation et une maturité technique que n'ont pas tous les vendeurs. L'adoption d'une politique de divulgation coordonnée de vulnérabilités par une structure qui n'est pas encore assez mature pourrait engendrer des situations où une vulnérabilité signalée ne serait pas suivie ni fixée, ou une réaction hostile de la part des vendeurs, ce qui décou-ragerait les chercheurs en sécurité à prendre part à de tels processus[27].

D'autre part, l'exemple de la loi belge est inspirant, et démontre que la perception des chercheurs en vulnérabilités par les pouvoirs publics a évolué en Europe. Leurs travaux, corrélés à leurs intentions, sont désormais reconnus par les pouvoirs publics en Belgique. Cette évolution n'est pas à négliger et pourrait constituer une source d'inspiration et d'impulsion aux niveaux européen et français.

[27] L'économie de la divulgation de vulnérabilités, ENISA, 14 décembre 2018, p. 42.

III. UN CADRE EUROPÉEN EN CONSTRUCTION

L'absence de frontières dans le cyberespace entraîne une multiplication des facteurs de risques. Une vulnérabilité dans un système d'information peut entraîner des conséquences transfrontalières dramatiques. Ce caractère transfrontalier peut aussi rendre le choix de la juridiction compétente compliqué en cas de litige. Ainsi, aborder la divulgation de vulnérabilités sous un angle purement national semble insuffisant. Au niveau européen, l'élaboration d'un cadre pour la divulgation coordonnée de vulnérabilités est en construction depuis quelques années mais reste encore flou sur certains aspects, notamment au sujet des chercheurs en vulnérabilités. Ce flou entraîne une insécurité autant pour les organisations que pour les chercheurs qui ne trouvent pas toujours d'intérêt à la divulgation légale des vulnérabilités.

a) Le traitement des vulnérabilités inconnues par les organisations mis de côté par la législation européenne

Si la politique européenne en matière de divulgation de vulnérabilités est longtemps restée timide et tardive, il ne peut être nié que le thème de la divulgation coordonnée de vulnérabilités a fait progressivement son apparition dans l'arsenal juridique européen.

L'Union européenne a initié la mise en place d'outils d'incitation pour les acteurs privés et publics afin d'élaborer des politiques de divulgation de vulnérabilités. Dès 2015, l'Agence européenne de la cybersécurité, l'ENISA, a publié un guide sur les bonnes pratiques en matière de divulgation de vulnérabilités[28]. Ce guide encourage les entités publiques et privées à mettre en place leur propre politique de divulgation de vulnérabilités. Force est de constater que ce guide n'a pas eu l'impact qu'il aurait pu avoir. La faute peut être due à un manque de communication ou à un guide extrêmement détaillé (92 pages contre 28 pages pour le guide néerlandais).

En parallèle, le programme de financement européen Horizon 2020 soutient la recherche dans le domaine de la divulgation de vulnérabilités.

[28] Guide bonnes pratiques sur la divulgation coordonnée de vulnérabilités, ENISA, 18 janvier 2016

Au-delà de ces politiques incitatives non contraignantes, l'Union européenne a également à légiféré sur le sujet. Ainsi, le *European Cybersecurity Act*, règlement européen adopté au printemps 2019, marque une étape importante vers une diffusion plus large de politiques de divulgation coordonnée de vulnérabilités au sein des entreprises. Même si la divulgation de vulnérabilités n'est pas le thème central du règlement, le texte promeut le rôle de la divulgation coordonnée de vulnérabilités pour améliorer la cybersécurité (considérant 30). Le *European Cybersecurity Act* dispose que l'une des missions de l'ENISA est d'assister les États membres, institutions, organes et organismes de l'Union dans l'établissement de politiques de divulgation de vulnérabilités (article 6 paragraphe 1).

En outre, conformément au *European Cybersecurity Act,* tout nouveau schéma européen de certification de cybersécurité devra comporter des règles concernant le signalement et la gestion de vulnérabilités (article 54 paragraphe 1 point m).
Le fabricant ou fournisseur d'un produit, service ou processus certifié doit fournir les informations de contact ainsi que les méthodes acceptées pour la réception d'information sur les vulnérabilités de la part des utilisateurs ou des chercheurs en cybersécurité (article 55 paragraphe 1 point c). Ces dispositions signifient qu'un fabricant ou fournisseur doit au moins avoir une ébauche de politique de divulgation de vulnérabilités s'il souhaite certifier ses solutions. Le *European Cybersecurity Act* ne liste pas d'exigences claires relatives au type de politique de divulgation de vulnérabilités qu'une organisation doit mettre en place.

Plus récemment, le projet de règlement transsectoriel de *Cyber Resilience Act*, (CRA)[29] s'appliquant à tous les produits numériques, impose aux fabricants d'aller au-delà d'une politique de divulgation de vulnérabilités, et d'en assurer leur prise en charge afin de traiter les vulnérabilités, que la divulgation provienne d'une source interne ou externe à l'organisation (Article 10.6). Les chercheurs en vulnérabilité sont ici pris en compte par le règlement sans que ne soit précisé à qui le chercheur devra s'adresser.
Pour y remédier, l'organisation peut lancer des mises à jour de sécurité automatiques qui seront notifiées à l'utilisateur. Ces mises à jour doivent être gratuites et accompagnées, si besoin, d'instructions à destination des utilisateurs afin d'indiquer les actions à entreprendre. Les informations relatives aux vulnérabilités corrigées doivent ensuite être publiées en incluant la description de la vulnérabilité, les versions du produit affectées ainsi que l'impact potentiel de celle-ci. L'ENISA partage ensuite ces informations au réseau européen de CSIRT et à l'autorité de surveillance de marché.

[29] Proposition de règlement du Parlement européen et du Conseil du 15 septembre 2022 concernant des exigences horizontales en matière de cybersécurité pour les produits comportant des éléments numériques et modifiant le règlement (UE) 2019/1020

Les sanctions les plus importantes sur le CRA se concentrent sur la divulgation de vulnérabilité : jusqu'à 15 milliards d'euros d'amende ou 2,5% du chiffre d'affaires annuel mon-dial peuvent être imposés en cas de non-respect des dispositions du CRA en matière de divulgation coordonnée de vulnérabilités. De plus, le CRA précise que la notification d'une vulnérabilité doit être faite à l'ENISA dans les 24 heures qui suivent la découverte de cette vulnérabilité (Article 11.1).

Cependant, un récent rapport de l'ENISA (16 février 2023) sur le développement de programmes nationaux de vulnérabilités[30] relève que les textes applicables en la matière ne prennent pas en compte la réalité des infrastructures informatiques étatiques et privées[31]. En effet, il est techniquement inconcevable aujourd'hui pour un fabricant de connaître parfaitement ou en totalité ses produits à cause notamment de la complexification de la chaîne d'approvisionnement. Il est alors difficilement imaginable de penser la correction de vulnérabilités par un seul acteur désigné comme responsable sans coopération. Par conséquent, le décalage entre le développement rapide des infrastructures technologiques et la vitesse de construction d'un cadre réglementaire en la matière est une barrière à la mise en œuvre d'un cadre commun européen.

Par ailleurs, bien que certains acteurs privés se soient déjà dotés d'une politique de divulgation coordonnée de vulnérabilités, la multiplication de ces politiques vient complexifier le paysage en termes de responsabilité. Dans le rapport de l'ENISA mentionné plus haut, les industriels interrogés font part du manque de clarté sur la coopération gouvernementale et institutionnelle dans la divulgation de vulnérabilités. Les conséquences ont un effet qui dépasse les entités chargées de développer de telles politiques et qui retentit sur les utilisateurs finaux dont font partie les chercheurs en vulnérabilité de bonne foi. Ceux-ci ne trouvent pas toujours d'intérêt à divulguer légalement les vulnérabilités trouvées et les processus mis en œuvre sont souvent complexes et administrativement lourds. Il est aussi encore très fréquent que les vulnérabilités remontées ne soient pas corrigées, même lorsqu'un dispositif correctif existe et est mis à disposition.

[30] Développer des programmes nationaux de vulnérabilités, ENISA, 16 février 2023
[31] Développer des programmes nationaux de vulnérabilités, ENISA, 16 février 2023

b) Un manque de transparence qui impacte la protection juridique des chercheurs en sécurité

Dans un premier temps, bien que l'Annexe 2 du CRA aborde le sujet de la transparence pour les utilisateurs et impose désormais aux entités de fournir un point de contact dédié au signalement et à la communication de vulnérabilités, le CRA ne s'adresse qu'aux orga-nisations, ce qui contribue à l'insécurité juridique des chercheurs. Les questions de la responsabilité et de la transparence sont pourtant centrales pour la divulgation de vulnérabilités et ne sont pas clairement abordées, contribuant à un manque de clarté quant aux rôles de chaque partie prenante en la matière, comme le souligne le rapport de l'ENISA du 16 février 2023.

C'est ensuite la directive NIS2[32], publiée le 27 décembre 2022 et entrée en vigueur le 16 janvier 2023, ayant pour objectif d'harmoniser et de renforcer la cybersécurité du marché européen qui mentionne la divulgation coordonnée de vulnérabilités. Elle doit être transposée au sein des États membres d'ici le 17 octobre 2024[33] mais en la matière, la transposition de cette directive au sein des États Membres sans que plus de précisions ne soient apportées semble complexe.

Dans un premier temps, le considérant 60 de la directive dispose que *« Les États membres, en coopération avec l'ENISA, devraient prendre des mesures pour faciliter la divulgation coordonnée de vulnérabilités en établissant une politique nationale pertinente. 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 chercheurs en vulnérabilités, y compris leur exposition potentielle à une responsabilité pénale, conformément au droit national. (...) les États membres sont encouragés à adopter des lignes directrices concernant la non-poursuite des chercheurs en sécurité de l'information et une exonération de responsabilité civile pour leurs activités ».*

Dans le même élan, le considérant 62 soutient cette évolution : « *Afin d'encourager une culture de divulgation des vulnérabilités, la divulgation ne devrait pas avoir d'effets préjudiciables sur la personne physique ou morale déclarante.*

[32] Directive (UE) 2022/2555 du Parlement européen et du Conseil du 14 décembre 2022 concer-nant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union

[33] Développer des programmes nationaux de vulnérabilités, ENISA, 16 février 2023

L'ENISA devrait établir une procédure appropriée concernant le processus de publication afin de donner aux entités le temps de prendre des mesures d'atténuation en ce qui concerne leurs vulnérabilités et d'employer des mesures de gestion des risques de cybersécurité de pointe ainsi que des ensembles de données lisibles par machine et des interfaces correspondantes ».

Cette directive prévoit notamment que chaque État membre désigne l'un de ses CSIRT comme « *coordinateur aux fins de la divulgation coordonnée de vulnérabilités* » (Article 12-1). Il fait office d'intermédiaire entre la personne physique ou morale qui signale une vulnérabilité et le fabricant ou le fournisseur. Pour cela, il identifie et contacte les entités concernées, apporte une assistance aux personnes physiques ou morales signalant une vulnérabilité et négocie les délais de divulgation. Les rapports de vulnérabilités doivent ensuite être transmis à l'ENISA afin qu'elle élabore une base de données européenne de ces vulnérabilités (Article 12-2). Mais, il ne s'agit ici que de traiter les vulnérabilités connues par les administrations, tout comme pour le CRA. Comme pour le texte précédent, il serait opportun de permettre aux chercheurs de remonter les vulnérabilités inconnues des organisations concernées directement aux CSIRT.

Quand bien même la directive NIS 2 prévoit la possibilité pour le chercheur de rester anonyme en passant par un CSIRT, elle n'ancre pas la protection juridique des chercheurs en vulnérabilités dans son texte mais incite les États à le faire. Il apparaît alors difficile pour ces chercheurs de favoriser la voie de la divulgation légale quand le principe de protection de ceux-ci n'est pas clairement inscrit dans les textes. De plus, les chercheurs en sécurité ne sont pas toujours habitués, voire enclins à communiquer avec les administrations[34], ce qui ajoute une difficulté à ces processus.

Il apparait également que l'application juxtaposée des prescriptions de la directive NIS2 et du *Cyber Resilience Act* (CRA) ne soit pas toujours aisée. La première prévoit que le rapport de vulnérabilité soit transmis directement aux CSIRT nationaux avant qu'ils ne le transfèrent à l'ENISA. Le CRA, quant à lui, prévoit que le fabricant transmette le rapport de vulnérabilité à l'ENISA qui le transmettra ensuite aux CSIRT. Bien que ces textes n'aient pas les mêmes champs d'application (le premier concerne les entités importantes et essentielles et l'autre concerne les produits numériques), il semble tout de même difficile de percevoir le chemin de communication de référence dans le cas d'une entité soumise aux deux périmètres.
Les délais de transfert semblent également contradictoires : le délai prévu par la version publique du CRA prévoit un délai de 24 heures (article 11 .1), tandis que la directive NIS 2 prévoit que les rapports des CSIRT soient remontés tous les 3 mois à l'ENISA (article 23.9).

[34] Développer des programmes nationaux de vulnérabilités, ENISA, 16 février 2023, p ? 21.

Dans un second temps, il est déjà possible d'observer des initiatives en matière de gestion de vulnérabilités dans le secteur privé, que le rapport de l'ENISA du 16 février 2023 souligne et met en avant. Cependant, le rapport met en garde les États membres face au risque que, s'ils ne lancent pas un cadre en la matière, les initiatives privées induiront une forte hétérogénéité des politiques de divulgation de vulnérabilité qui sera plus difficile à appréhender *a posteriori*.

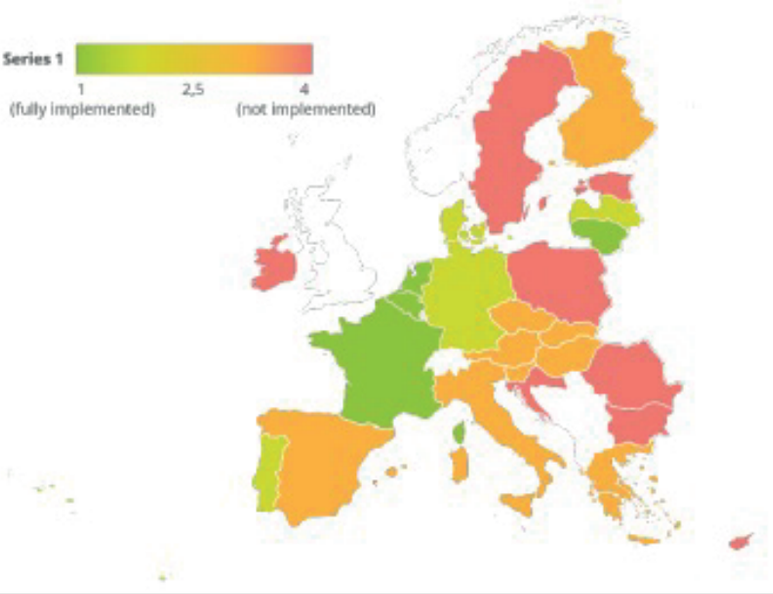
Ensuite, le problème de la transparence apparaît tout aussi important dans la chaîne de responsabilité au niveau des produits, notamment des produits en source ouverte. En effet, la chaîne d'approvisionnement étant de plus en plus complexe, implique des codes de différents auteurs, de différentes sources et de différentes natures. Et il est parfois difficile d'identifier le détenteur du code ou la personne à contacter dans le cadre de la divulgation coordonnée de vulnérabilités étant donné que n'importe qui peut publier, utiliser et modifier un code disponible en source ouverte. Dans ce contexte, la vulnérabilité ne peut être corrigée que par une approche collective encore difficilement appréhendée. Considérant la présence de produits en open source dans des logiciels et des produits utilisés partout dans le monde, un effort international, ou du moins européen, est nécessaire dans la gestion des vulnérabilités[35].

[35]La cybersécurité : Guide de divulgation coordonnée des vulnérabilités, ETSI, janvier 2022

c) Des politiques disparates de divulgation coordonnée de vulnérabilités en Union européenne

Globalement, très peu d'États membres ont mis en place une politique de divulgation coordonnée de vulnérabilités.

Figure 2: Implementation of coordinated vulnerability disclosure policy at national level in Europe, EU map[36]



Plusieurs États n'ont pas encore de politique de divulgation coordonnée de vulnérabilités : la Bulgarie, Chypre, la Croatie, l'Estonie, l'Irlande, Malte, la Pologne, la Roumanie et la Suède.
D'autres sont en cours d'élaboration d'une politique de divulgation coordonnée de vulnérabilités comme, l'Autriche, l'Espagne, la Finlande, la Grèce, la Hongrie, l'Italie, le Luxembourg, la République de Macédoine, la République Tchèque, la Slovaquie, la Slovénie et la Suisse (qui, bien que n'étant pas un États membre, fait partie du marché unique).
Enfin, quelques-uns sont sur le point d'adopter une telle politique comme l'Allemagne, le Danemark, la Lettonie et le Portugal. Seuls la France, les Pays-Bas et la Belgique ont déjà mis en place une politique de divul-gation coordonnée de vulnérabilités générales, valable pour tous les secteurs d'activité. La Lituanie est un cas particulier car elle a établi un cadre de divulgation de vulnérabilités pour un secteur en particulier : les fournisseurs de réseaux de communications publiques[37].

[36] Développer des programmes nationaux de vulnérabilités, ENISA, 16 février 2023, p. 11
[37] Protéger l'Europe des vulnérabilités des logiciels, Centre européen d'études politiques (CEPS), 28 juin 2018, p. 13

d) Des pistes d'amélioration possibles au niveau européen

L'Union européenne pourrait notamment :

1) Amender la Directive Cybercrime (Directive 2013/40/EU sur les attaques contre les systèmes d'information) afin d'intégrer la divulgation coordonnée de vulnérabilités, de promouvoir la protection des chercheurs en vulnérabilités et de les encourager à participer à des programmes de divulgation de vulnérabilités ;

2) Inciter les États membres à mettre en place des politiques qui encouragent les entités privées et publiques à établir leur propre politique de divulgation coordonnée des vulnérabilités, à l'instar des Pays-Bas. L'État doit impulser le mouvement en adoptant lui-même au sein de ses organisations (ministères, établissements publics, collectivités territoriales, ...) et montrer le bon exemple afin que les entités essentielles et importantes visées par la directive NIS 2 puissent se doter de politiques de divulgation coordonnée de vulnérabilités et être conforme à la directive au moment de sa prise d'effets ;

3) Mettre à jour le guide des pratiques en matière de divulgation de vulnérabilités de 2015 afin qu'il soit allégé et aligné aux initiatives européennes en la matière. L'ENISA dans son rapport du 16 février 2023, recommande notamment :

- L'usage des « *Software bill of materia*l » (SBOM) et des "*Software Composition Analysis*" (SCA) afin de faciliter l'appréhension des logiciels en source ouverte,

- L'utilisation de programmes de *Bug bounty* et les considérant comme complémentaires du *Security-by-design*,

- L'automatisation de la divulgation de vulnérabilités aux tâches répétitives qui ne nécessitent pas d'expertise humaine afin de créer des bases de données organisées selon une logique convenue et sans erreur humaine.

4) Sensibiliser la société européenne aux questions qui peuvent se poser dans le contexte de la divulgation coordonnée de vulnérabilités, que ce soit au niveau technique ou au niveau juridique. Un travail de pédagogie doit notamment être entrepris afin que les chercheurs en vulnérabilités et leurs activités soient dédiabolisés. Par exemple, l'État pourrait proposer une nomenclature uniforme à leurs activités afin qu'ils soient clairement distingués des acteurs malveillants en quête de profit. Une nomenclature à l'image de celle des lanceurs d'alerte semble être pertinente comme ces deux types d'acteurs apportent le même bénéfice sociétal.

CONCLUSION

La mise en place de politiques de divulgation coordonnée de vulnérabilités est désormais rendue obligatoire par les récents textes européens NIS2 et CRA. La question de la découverte et du traitement des vulnérabilités, en discussion depuis plusieurs années, est désormais un sujet central dans l'approche européenne de la cybersécurité. Toutefois, les premiers éléments de réponse juridiques, notamment européens, même s'ils constituent une base utile, mériteraient d'être homogénéisés, par une approche holistique permettant également de traiter la question de la place du chercheur en vulnérabilités de bonne foi.
Les législations nationales de chaque Etat-membre pourraient avoir en ce sens, un rôle d'aiguillon. En France, plusieurs pistes sont possibles, telles que la révision du Code pénal afin d'introduire un amendement qui protègerait les chercheurs en vulnérabilités de bonne foi d'éventuelles poursuites judiciaires engagées par le vendeur. Par ailleurs, la loi pourrait définir des obligations pour les organisations en matière de mise en place de processus dédiés permettant d'être informés en cas de découverte d'une vulnérabilité et assurant son traitement.
Nous manquons encore de recul sur l'utilisation du formulaire de lanceurs d'alertes sur le site de la CNIL, néanmoins, ce mécanisme pourrait servir de modèle voire de support aux chercheurs en vulnérabilités. La France pourrait également prendre exemple sur la loi belge et conditionner la protection des chercheurs en vulnérabilités bien intentionnés à des critères prédéterminés.

En Union européenne, les exigences issues du *European Cybersecurity Act*, de la directive NIS 2 ainsi que du *Cyber Resilience Act* concernant le sujet de la divulgation coordonnée de vulnérabilités gagneraient à être précisés et homogénéisés dans une approche holistique du sujet. Cela permettrait une harmonisation de la législation européenne, ce qui réduirait considérablement l'insécurité juridique à laquelle sont confrontés bon nombre de chercheurs en vulnérabilités, surtout dans des situations transfrontalières.
De plus, pour que la réponse européenne traite de la question de la place des chercheurs en vulnérabilités, les textes devraient également permettre à ces chercheurs de remonter leurs recherches directement aux CSIRT, et non pas simplement le permettre aux organisations.

Les bases de données de vulnérabilités connues seraient par conséquent complétées par les vulnérabilités inconnues des organisations mais connues des chercheurs et seraient alors plus exhaustives. L'ouverture de cette voie aux chercheurs serait aussi une garantie de leur protection juridique au niveau européen.

Ce serait en effet une réponse adaptée aux difficultés auxquelles font face à la fois les organisations et les chercheurs en vulnérabilités.
Le sujet de la divulgation coordonnée de vulnérabilités est donc un sujet multiforme. Aujourd'hui, sa prise en compte au niveau réglementaire est une réalité et atteste du fait que la divulgation coordonnée de vulnérabilités est conçue comme un outil supplémentaire dans l'arsenal dont nous disposons pour mieux protéger nos systèmes d'information.
Toutefois, afin d'optimiser l'efficacité de cet outil, ces initiatives réglementaires, qui aujourd'hui apportent des réponses à l'un ou l'autres des aspects du sujet, doivent être rassemblées dans une vision globale à même d'apporter les réponses opportunes à l'ensemble des acteurs de la chaîne. En effet, l'enjeu est de permettre à un maximum de vulnérabilités d'être connues et traitées : pour cela, il est essentiel de sécuriser le cadre juridique des chercheurs de bonne foi, d'organiser un système coordonné de remontées de ces vulnérabilités, auprès des organisations concernées et des pouvoirs publics, et de prévoir les conditions de leur traitement et de leur éventuelle divulgation publique.

En parallèle, il parait également opportun d'encourager toutes les organisations qui le peuvent à se doter de politiques privées de divulgation coordonnée de vulnérabilités : des solutions de confiance permettent d'ores et déjà de faciliter la mise en œuvre des politiques de divulgation coordonnée de vulnérabilités.
Cela peut passer par des mesures, telles que la mise en place d'une campagne et la publication de lignes directrices pour inciter les organisations privées et publiques à mettre en place leur propre politique de divulgation coordonnée de vulnérabilités et en préciser les grands principes.
L'information des magistrats et plus largement du personnel judiciaire aux enjeux spécifiques de ce sujet est également un élément décisif.
Ainsi, c'est une nouvelle approche, juridique, éthique et culturelle qui doit être mise en place afin de permettre à la recherche de vulnérabilités et à leur découverte de bénéficier pleinement à l'ensemble de notre société.

La compréhension de ce sujet et son appréhension à travers l'ensemble de ses domaines d'implication, de manière homogène, sont les clés du succès. Au-delà, les règles et bonnes pratiques, une fois définies doivent être partagées et s'intégrer de manière cohérente dans les édifices réglementaires nationaux, européens voire dans les instances internationales.

Les évolutions culturelles sont à l'œuvre. Les implications de la divulgation coordonnée de vulnérabilités sont nombreuses. Dans ce cadre, à la lumière des initiatives déjà menées en France et en Union européenne, une initiative nationale portant sur l'ensemble de ce sujet pourrait constituer un socle majeur pour dessiner le cadre juridique complet qui fait aujourd'hui défaut et augmenter ce faisant la protection et la résilience de notre pays et de l'Union européenne.

SITE :

https://www.confiance-numerique.fr/

@ACN_SecNum

ACN - Alliance pour la Confiance Numérique

ACN

Alliance pour la confiance numérique