Projet de loi (n° 1033) relatif à la programmation militaire pour les années 2024 à 2030 et portant diverses dispositions intéressant la défense (articles 32 à 35)

Document faisant état de l'avancement des travaux de
Mme Sabine Thillaye, rapporteure

Mardi 9 mai 2023

EXAMEN DES ARTICLES 32 À 35 DU PROJET DE LOI

Article 32
(Art. L. 2321-2-3 *[nouveau]* du code de la défense)
Prescription par l'ANSSI de mesures affectant les noms de domaine en cas de menace susceptible de porter atteinte à la sécurité nationale

➢ **Résumé du dispositif et effets principaux**

L'article 32 permet à l'Agence nationale de la sécurité des systèmes d'information (ANSSI), en cas de menace susceptible de porter atteinte à la sécurité nationale, de prescrire plusieurs mesures graduelles affectant les noms de domaine, en particulier leur blocage ou suspension, ainsi que leur redirection vers un serveur sécurisé ou neutre contrôlé par l'ANSSI.

I. LE FONCTIONNEMENT DU SYSTÈME DNS

Consubstantiel au développement d'internet, le système DNS, qui permet concrètement de relier une adresse IP à un nom de domaine, et donc de réaliser des recherches sur internet, est un rouage fondamental de fonctionnement du web. Ce rôle central en fait une cible prisée des cyber-attaquants.

A. L'ÉTABLISSEMENT D'UNE CORRESPONDANCE ENTRE L'ADRESSE IP ET LE NOM DE DOMAINE

Chaque périphérique (ordinateur, tablette, téléphone, *etc*.) connecté à internet dispose d'une adresse IP (pour « *Internet protocol* »), composée d'une série de chiffres ou de nombres. Le **système de nom de domaine**, ou DNS (pour « *domain name system* ») permet de faire correspondre cette adresse IP à un nom de domaine, plus facile à retenir et à retranscrire qu'une suite de numéros. La correspondance est établie par des machines, les **serveurs de nom de domaine** (ou serveurs DNS).

Le nom de domaine permet ainsi de traduire de façon intelligible et mémorisable les adresses IP. Il est composé d'un préfixe (généralement, *www* pour

« *world wide web* »), ainsi que d'une chaîne de caractères (par exemple, assemblee-nationale) et d'une extension, qui peut être nationale (c'est le cas, en France, du *.fr* ou, au Royaume-Uni, du *.co.uk*) – ou générique, la plus connue étant *.com*.

L'ensemble de ces éléments rendent le nom de domaine unique.

LA STRUCTURE D'UNE ADRESSE IP

Source : site internet de l'Association française pour le nommage Internet en coopération

Concrètement, quand un internaute exécute une recherche internet, celle-ci est envoyée à plusieurs serveurs DNS successivement interrogés (1), jusqu'à obtenir une traduction de cette recherche en une adresse IP compréhensible par les ordinateurs et les réseaux.

L'étude d'impact annexée au projet de loi établit la liste des principaux acteurs du système DNS concernés par le présent article. Il s'agit :

– des **fournisseurs d'accès à internet** (FAI) : ce sont des entreprises ou personnes dont l'activité est d'offrir un accès à des services de communication au public en ligne, autrement dit à internet. Ces prestataires permettent de connecter les systèmes d'information de leurs clients au réseau internet, et donc de faire transiter tous les flux sur leurs réseaux ;

– des **hébergeurs de données** : ce sont des prestataires de service équipés de disques durs et de serveurs, qui proposent aux internautes le stockage de leurs contenus et leur diffusion sur internet. L'étude d'impact annexée au projet de loi précise que « *les hébergeurs peuvent, sans le vouloir, héberger des données malveillantes, telles que des centres de commande et contrôle qui permettent à un acteur malveillant de contrôler ses outils d'attaque à distance* » ;

– des **registres et les bureaux d'enregistrement des noms de domaine établis en France** : les registres maintiennent et gèrent les noms de domaine, c'est-à-dire la correspondance entre le nom de domaine et la personne ou l'organisation qui en est propriétaire, tandis que les bureaux d'enregistrement se voient déléguer par les registres la commercialisation des noms de domaine.

---

(1) Aucun serveur ne comprend l'ensemble des données du système DNS. Par exemple, seuls les serveurs de l'Afnic, chargée de l'enregistrement des noms de domaine en France, peuvent répondre aux sollicitations concernant des noms de domaine se terminant par .fr.

B. LE RECOURS FRÉQUENT AUX DNS LORS DE CYBER-ATTAQUES

Le rôle central des DNS en fait u**ne cible privilégiée par les cyber-attaquants** : ainsi, les noms de domaine sont fréquemment utilisés pour mener des attaques informatiques, permettant l'établissement d'une communication entre la machine compromise par l'attaque et celle de l'attaquant, ou le leurre d'un utilisateur vers un site malveillant dans le cadre d'attaques par hameçonnage.

L'ANSSI a traité **831 incidents en 2022**, dont la plupart impliquant l'usage du DNS. Le SGDSN a détaillé à votre rapporteure plusieurs cas d'espèce où une action sur le nom de domaine a, ou aurait pu, entraver une attaque :

– **WannaCry**, du nom d'un logiciel malveillant de type rançongiciel auto-répliquant qui, en mai 2017, a concerné des pays du monde entier. Une équipe spécialisée a pu reprendre le contrôle du domaine DNS attaqué par le *WannaCry*, désactivant ainsi l'ensemble des virus sur les machines affectées ;

– **APT31** : ce mode opératoire, associé en source ouverte à la Chine, a été mis en œuvre dans le cadre d'une vaste campagne d'espionnage à l'encontre d'organisations françaises en 2021. Il utilisait *Cobalt Strike*, une solution répandue de sécurité offensive, afin d'exfiltrer des données à travers le protocole DNS. Ce mode opératoire, qui a fait l'objet d'une publication sur le site du CERT-FR (1), le centre opérationnel de l'ANSSI, permettait la résolution des IP correspondant aux noms de domaine vers des routeurs compromis. Le blocage de ces noms de domaine aurait pu, selon l'ANSSI, permettre d'entraver la menace ;

– **Nobelium** : le mode opératoire d'attaquants *Nobelium* aurait été utilisé pour mener plusieurs campagnes d'hameçonnage contre des entités françaises entre février et décembre 2021. Cette campagne a permis de compromettre plusieurs comptes de messagerie d'organisations françaises et d'envoyer depuis ces comptes compromis des courriels piégés à des institutions étrangères. L'infrastructure de commande et contrôle des attaquants (2) comprenait des noms de domaines ressemblant à des noms légitimes de sites d'information et d'actualités. Leur blocage aurait pu permettre, selon l'ANSSI, d'entraver cette campagne.

---

(1) https://www.cert.ssi.gouv.fr/cti/CERTFR-2021-CTI-012/ (consulté le 28 avril 2023).

(2) Selon la définition transmise à votre rapporteure par le SGDSN, une infrastructure d'attaque est un ensemble d'éléments connectés à internet créant un « pont » entre l'attaquant et sa victime dans la perspective, le plus souvent, de garantir l'anonymat et la discrétion du premier. Ces infrastructures peuvent être composées de serveurs loués auprès d'hébergeurs ou de serveurs compromis, utilisés à l'insu de leurs propriétaires. Dans le dernier cas, l'attaquant s'appuie sur des vulnérabilités lui permettant d'y accéder.

Le déroulé classique d'une attaque informatique

Qu'il s'agisse d'une attaque d'espionnage pour obtenir des informations ou des cyberattaques criminelles, comme les rançongiciels, utilisés à des fins d'extorsion, l'organisation d'une cyber-attaque répond à des mêmes grands principes, plus ou moins sophistiqués et automatisés en fonction des cas, rappelés par le SGDSN et l'ANSSI au cours de leur audition :

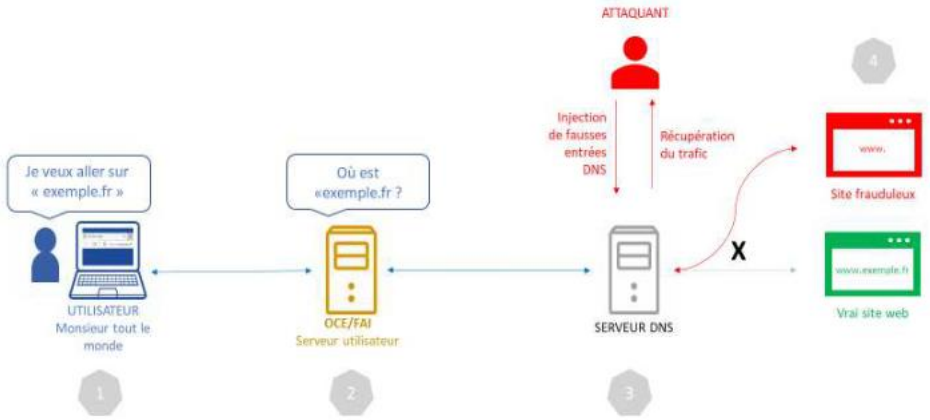
– **phase 1 (reconnaissance)** : l'attaquant cherche à obtenir des informations sur sa cible. Dans le cadre d'une opération d'espionnage, il s'agit d'obtenir des renseignements, et donc de déterminer les vulnérabilités du système d'information visé, pour mieux comprendre le fonctionnement de l'entreprise cible, les habitudes de son dirigeant, *etc*. Si l'opération est motivée par des fins criminelles, il s'agit surtout pour l'attaquant de rechercher les faiblesses à exploiter dans l'entreprise et de déterminer la cible la plus facile d'accès pour pénétrer dans le système d'information ;

– **phase 2 (intrusion initiale dans le système de la victime)** : il s'agit de « mettre le pied dans la porte » du système d'information de la victime déterminée par l'attaquant. La manière la plus classique de procéder est de recourir au procédé du *fishing*, par l'intermédiaire d'un email piégé à une victime. Plus la phase 1 a été préparée en amont, plus l'e-mail de *fishing* sera vraisemblable. L'attaquant peut aussi chercher des systèmes d'information mal configurés ou mal mis à jour, et donc vulnérables, qu'il pourrait exploiter techniquement pour les contrôler ;

– **phase 3 (escalade de privilèges)** : une fois entré dans le système d'information, l'attaquant doit encore obtenir les informations précises sur sa cible, qui ne sont généralement pas détenues par la première victime, simple « porte d'entrée ». L'attaquant va opérer une « escalade de privilèges », ce terme qualifiant les droits des utilisateurs sur le système d'information concerné. Se déplaçant d'utilisateur en utilisateur, l'attaquant va ainsi rechercher parmi les périphériques les informations qui pourraient *in fine* l'intéresser. Ce faisant, il prend peu à peu le contrôle de tout le système d'information. L'on peut penser à un attaquant qui, après avoir compromis le compte d'un député, cherchera à obtenir d'autres droits afin de maximiser le potentiel de son attaque, par exemple en ciblant un administrateur du système de l'Assemblée nationale ;

– **phase 4 (exploitation des accès obtenus)** : lorsqu'il s'agit d'une opération d'espionnage, l'attaquant va exfiltrer, en une fois ou de manière régulière, l'ensemble des informations qui l'intéressent (un email sensible, une information industrielle protégée par le secret des affaires, etc.) ; lors d'une attaque par rançongiciel, l'attaquant va déployer son logiciel malveillant sur le parc informatique, chiffrer les données qui y sont stockées et paralyser le système d'information de la victime, l'incitant ainsi à lui verser une rançon.

UN EXEMPLE DE DNS DÉFAILLANT



Source : étude d'impact annexée au projet de loi

II. L'EXISTENCE DE MESURES ADMINISTRATIVES ET JUDICIAIRES DE FILTRAGE DE CERTAINS CONTENUS EN LIGNE

Avec le déploiement et la généralisation d'internet, la circulation en ligne de certains contenus illégaux a contraint le législateur à faire évoluer le cadre légal.

Il existe ainsi déjà plusieurs mesures de filtrage, administratives ou judiciaires, de certains de ces contenus, qui reposent sur plusieurs techniques, comme le **retrait des contenus illicites**, le **blocage par adresse IP** ou le **blocage par DNS** (1). Ils ont notamment pour finalité de lutter contre le terrorisme et la pédopornographie, prévenir un dommage aux personnes, protéger la sincérité d'un scrutin, ou lutter contre la circulation de contenus illicites.

Ces dispositifs, qui constituent nécessairement une atteinte au principe de neutralité d'internet, sont néanmoins permis, sous certaines conditions, par le droit européen.

A. DIFFÉRENTES FORMES DE BLOCAGE EXISTENT DÉJÀ

1. Les procédures de blocage judiciaire

Plusieurs dispositions permettent d'obtenir le blocage judiciaire de contenus diffusés en ligne.

● La loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique (LCEN) comporte ainsi une disposition relative au **blocage judiciaire de certains sites**, permettant à l'autorité judiciaire de prescrire, en référé ou sur requête, toute mesure propre à prévenir un dommage ou à faire cesser un dommage occasionné par le contenu d'un service de communication au public en ligne. Le

(1) *Cette dernière technique étant définie dans l'étude d'impact annexée au projet de loi comme le fait de* « filtrer le nom de domaine *[ce qui]* empêche l'internaute de se connecter à la ressource associée au nom de domaine (principalement, les sites internet), ressource qui est rendue inaccessible pour l'ensemble des utilisateurs. »

juge judiciaire peut ainsi enjoindre au fournisseur d'accès à internet ou à l'hébergeur de retirer le contenu litigieux, voire de bloquer l'accès au site internet sur lequel ce contenu est diffusé [(1)].

● En matière de **violation d'un droit d'auteur ou d'un droit voisin**, le président du tribunal judiciaire peut, à la demande des titulaires de droits ou de leurs ayant-droits, ordonner en référé *« toutes mesures propres à prévenir ou à faire cesser une telle atteinte* (…) *à l'encontre de toute personne susceptible de contribuer à y remédier* » [(2)].

● L'article 706-23 du code de procédure pénale dispose par ailleurs que « *l'arrêt d'un service de communication au public en ligne peut être prononcé par le juge des référés pour les faits* [d'**apologie du terrorisme**] *lorsqu'ils constituent un trouble manifestement illicite, à la demande du ministère public ou de toute personne physique ou morale ayant un intérêt à agir. »*

● Créé par la loi n° 2018-1202 du 22 décembre 2018 relative à la lutte contre la manipulation de l'information, l'article L. 163-2 du code électoral permet au juge des référés de prescrire « *toutes mesures proportionnées et nécessaires pour* ***faire cesser*** **» la diffusion d'«** ***allégations ou imputations inexactes ou trompeuses*** *d'un fait* ***de nature à altérer la sincérité du scrutin*** *à venir diffusées de manière délibérée, artificielle ou automatisée et massive par le biais d'un service de communication au public en ligne* », pendant les trois mois précédant une élection.

● Enfin, il existe un **mécanisme dit « jeux en ligne »** permettant à l'Autorité nationale des jeux d'enjoindre aux hébergeurs de « *prendre toute mesure pour empêcher l'accès* [à un jeu d'argent et de hasard ne respectant pas la réglementation] *et les invite à présenter leurs observations dans un délai de cinq jours* ». À défaut, son président peut ordonner aux FAI, moteurs de recherche et annuaires d'empêcher l'accès ou de faire cesser le référencement des contenus illicites. Le non-respect de cette injonction est passible d'une peine d'emprisonnement d'un an et de 250 000 € d'amende [(3)].

2. Le blocage administratif

● La loi n° 2014-1353 du 13 novembre 2014 renforçant les dispositions relatives à la lutte contre le terrorisme a instauré, à l'article 6-1 de la LCEC, **une procédure de blocage administrative unique** des contenus faisant l'apologie ou appelant à commettre un acte terroriste, ainsi que des contenus à caractère pédopornographique, dont l'Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication (OCLCTIC) peut demander le retrait, le blocage ou le déréférencement.

---

(1) Article 6, I, 8 de la LCEN.

(2) Article L. 336-2 du code de la propriété intellectuelle.

(3) Article 61 de la loi n° 2010-476 du 12 mai 2010 relative à l'ouverture à la concurrence et à la régulation du secteur des jeux d'argent et de hasard en ligne.

● Par ailleurs, le code de la consommation permet aux agents de l'autorité administrative – en l'espèce, la Direction générale de la concurrence, de la consommation et de la répression des fraudes (DGCCRF) – d'enjoindre aux offices et bureaux d'enregistrement de noms de domaine de procéder au **blocage d'un nom de domaine, à sa suppression ou à son transfert** à cette autorité, en cas de manquement à certaines dispositions du code de la consommation [(1)].

B. EXCEPTIONS AU PRINCIPE DE NEUTRALITÉ DU WEB, CES DISPOSITIONS SONT PERMISES PAR LE DROIT EUROPÉEN

Le règlement (UE) 2015/2120 du 25 novembre 2015 [(2)] consacre, en droit positif, le **principe de neutralité d'internet**. L'article 3 dispose ainsi, visant à la fois les utilisateurs et les fournisseurs d'accès à internet :

« *1. Les utilisateurs finals ont le droit d'accéder aux informations et aux contenus et de les diffuser, d'utiliser et de fournir des applications et des services et d'utiliser les équipements terminaux de leur choix, quel que soit le lieu où se trouve l'utilisateur final ou le fournisseur, et quels que soient le lieu, l'origine ou la destination de l'information, du contenu, de l'application ou du service, par l'intermédiaire de leur service d'accès à l'internet.* (…)

3. Dans le cadre de la fourniture de services d'accès à l'internet, les fournisseurs de services d'accès à l'internet traitent tout le trafic de façon égale et sans discrimination, restriction ou interférence, quels que soient l'expéditeur et le destinataire, les contenus consultés ou diffusés, les applications ou les services utilisés ou fournis ou les équipements terminaux utilisés. »

Les fournisseurs d'accès à internet doivent ainsi **traiter de la même manière tous les usagers des services de communication au public en ligne**, fournisseurs de contenus et utilisateurs des réseaux, excluant ainsi l'idée d'un internet à plusieurs vitesses en fonction des services ou de leurs utilisateurs.

Ce principe a été décliné en droit français par la loi du 7 octobre 2016 pour une République numérique. Son article 40 dote l'ARCEP de prérogatives nouvelles de contrôle lui permettant de surveiller les pratiques des FAI, diligenter des enquêtes, voire prononcer **des sanctions pouvant aller jusqu'à 3 % du chiffre d'affaires des opérateurs** [(3)].

---

(1) Article L. 521-3-1 du code de la consommation.

(2) Règlement (UE) 2015/2120 du Parlement européen et du Conseil du 25 novembre 2015 établissant des mesures relatives à l'accès à un internet ouvert et modifiant la directive 2002/22/CE concernant le service universel et les droits des utilisateurs au regard des réseaux et services de communications électroniques et le règlement (UE) no 531/2012 concernant l'itinérance sur les réseaux publics de communications mobiles à l'intérieur de l'Union.

(3) L'Autorité de régulation des communications électroniques, des postes et de la distribution de la presse (ARCEP) est une autorité administrative indépendante dont la mission de réguler le marché des opérateurs de téléphonie, d'internet et des postes. Elle exerce aujourd'hui des missions relatives à la régulation du secteur postal, la protection de la neutralité du net, l'aménagement numérique des territoires, la distribution de la presse et la mesure de l'impact environnemental du numérique. Pour le secteur des communications, l'ARCEP définit ainsi la réglementation applicable aux opérateurs, attribue les ressources en fréquences, et

La neutralité d'internet n'est néanmoins **pas absolue**. L'article 3 du règlement européen de 2015 dispose ainsi que :

« *Les FAI* (…) *s'abstiennent de bloquer, de ralentir, de modifier, de restreindre, de perturber, de dégrader ou de traiter de manière discriminatoire des contenus, des applications ou des services spécifiques ou des catégories spécifiques de contenus, d'applications ou de services, sauf si nécessaire et seulement le temps nécessaire, pour : (a) se conformer aux actes législatifs de l'Union ou à la législation nationale qui est conforme au droit de l'Union, auxquels le fournisseur de services d'accès à l'internet est soumis, ou aux mesures, conformes au droit de l'Union, donnant effet à ces actes législatifs de l'Union ou à cette législation nationale, y compris les décisions d'une juridiction ou d'une autorité publique investie des pouvoirs nécessaires* » (1).

En droit français, l'article L. 33-1 du code des postes et des communications électroniques rappelle d'abord le principe de neutralité de l'internet, qu'il assortit de réserves, en particulier « a*) les conditions de permanence, de qualité, de disponibilité, de sécurité et d'intégrité du réseau* » et « *e) les prescriptions exigées par l'ordre public, la défense nationale et la sécurité publique* ».

Les restrictions mises en place par le législateur s'insèrent ainsi dans cette exception au principe de neutralité du web.

III. LE DISPOSITIF PROPOSÉ : DE NOUVELLES MESURES GRADUELLES APPLICABLES AUX NOMS DE DOMAINE QUI PERMETTENT À L'ANSSI DE MIEUX LUTTER CONTRE LES MENACES À LA SÉCURITÉ NATIONALE

L'article 32 du projet de loi créé un nouvel article L. 2321-2-2 au sein du code de la défense, qui permet à l'ANSSI de mettre en œuvre des mesures graduelles

---

conseille le Gouvernement. Pour le secteur des postes, elle délivre par exemple les autorisations aux opérateurs de services postaux d'envoi de correspondance, exerce un contrôle comptable et tarifaire du prestataire du service universel ou encore émet des avis relatifs aux aspects économiques des tarifs des prestations offertes à la presse. Pour mener à bien ses fonctions, l'ARCEP dispose d'un pouvoir de sanction qui comprend la possibilité d'attribuer des avertissements, des restrictions d'autorisations, des astreintes ou des amendes.

(1) Les considérants 13 et 14 de la directive précisent ce point. Ils disposent ainsi que : « (13) Premièrement, des situations peuvent se présenter dans lesquelles des fournisseurs de services d'accès à l'internet sont soumis à des actes législatifs de l'Union ou à de la législation nationale qui est conforme au droit de l'Union (par exemple, en ce qui concerne la légalité des contenus, applications ou services, ou la sécurité publique), y compris le droit pénal exigeant, par exemple, le blocage de contenus, d'applications ou de services spécifiques. En outre, des situations peuvent se présenter où ces fournisseurs sont soumis à des mesures conformes au droit de l'Union mettant en œuvre ou appliquant des actes législatifs de l'Union ou de la législation nationale, telles que des mesures d'application générale, des décisions de justice, des décisions d'autorités publiques investies des pouvoirs pertinents ou d'autres mesures visant à garantir le respect de ces actes législatifs de l'Union ou de cette législation nationale (par exemple, des obligations de respecter des décisions de justice ou des décisions d'autorités publiques exigeant le blocage de contenus illégaux) (…)

(14) Deuxièmement, des mesures de gestion du trafic allant au-delà de telles mesures raisonnables de gestion du trafic pourraient être nécessaires pour protéger l'intégrité et la sécurité du réseau, par exemple en prévenant les cyberattaques qui se produisent par la diffusion de logiciels malveillants ou l'usurpation d'identité des utilisateurs finals qui résulte de l'utilisation de logiciels espions. »

de filtrage, dès lors qu'elle constate une menace susceptible de porter atteinte à la sécurité nationale du fait de l'exploitation d'un nom de domaine.

L'appréciation des risques d'atteinte à la sécurité nationale par l'ANSSI

L'ANSSI a précisé à votre rapporteure comment ses agents apprécient concrètement le risque d'atteinte à la sécurité nationale. Celui-ci repose notamment sur trois critères :

– si les éléments à disposition de l'ANSSI permettent de **supposer que l'attaquant est de nature étatique**. Cela arrive lorsque le mode opératoire de l'attaquant est susceptible d'être rapproché de ceux exploités par des entités liées à des puissances étrangères ;

– si les **moyens de l'attaquant** sont d'une complexité ou d'un niveau particulièrement avancés, l'ANSSI citant en particulier le cas des attaques issues d'entreprises spécialisées dans la lutte informatique offensive privée, notamment le recours au logiciel Pegasus développé par la société NSO Group, dont les clients étaient des États ;

– **la nature de la (ou des) victime(s)** : si la cible d'une compromission est une entité étatique, un opérateur d'importance vitale (OIV) ou un opérateur de services essentiels (OSE) [(1)] ou si l'étendue de la compromission est telle qu'elle fait courir un risque particulier au tissu économique, sanitaire ou à l'ordre public sur une portion ou l'entièreté du territoire national.

Les mesures employées se distinguent selon que le titulaire du nom de domaine est de bonne foi ou est, au contraire, animé par des intentions malveillantes. Elles partagent un même objectif : neutraliser l'utilisation dévoyée d'un nom de domaine.

A. LES MESURES DE FILTRAGE APPLICABLES AU TITULAIRE DE BONNE FOI (ALINÉAS 2 À 6)

Lorsque la menace résulte « *de l'exploitation d'un nom de domaine à l'insu de son titulaire qui l'a enregistré de bonne foi* », le nouvel article L. 2321-2-3 du code de la défense prévoit une gradation des mesures susceptibles d'être demandées par l'ANSSI :

– dans un premier temps, l'ANSSI peut demander au titulaire du nom de domaine de **prendre « *les mesures adaptées pour neutraliser cette menace dans un délai qu'elle lui impartit* »**. À titre d'exemples, le SGDSN a précisé à votre rapporteure que le propriétaire pourrait être invité à **modifier son enregistrement dans l'annuaire d'internet**, de sorte qu'il ne soit plus associé à une machine contrôlée par un attaquant, ou choisir d'associer son nom de domaine à une machine non compromise qu'il contrôle, voire de l'associer à une adresse « vide » ;

(1) Ces deux derniers termes sont définis sous le commentaire de l'article 34, qui concerne directement ces opérateurs.

– si la menace n'a pas été neutralisée dans le délai imparti, l'ANSSI peut **ordonner aux fournisseurs d'accès à internet et aux hébergeurs (1) le blocage ou la suspension du nom de domaine**. Concrètement, le blocage consiste, plutôt que d'orienter l'utilisateur vers le nom de domaine malveillant, à ne pas lui fournir de réponse (« page introuvable ») ou à le renvoyer vers une page internet expliquant que le nom de domaine a été suspendu. Le SGDSN a précisé à votre rapporteur que le choix de l'une ou l'autre de ces options se fera en fonction des cas d'espèce.

B. LES MESURES DE FILTRAGE APPLICABLES AU TITULAIRE DE MAUVAISE FOI (ALINÉAS 7 À 9)

Le II de l'article L. 2321-2-2 du code de la défense prévoit, lorsque le nom de domaine représentant une menace a été enregistré à **des fins malveillantes** – c'est-à-dire, avec la volonté de l'utiliser aux fins de mener une attaque informatique – et que le titulaire est donc de mauvaise foi, **une procédure applicable sans délai**.

Dans un tel cas de figure, l'ANSSI peut en effet ordonner aux FAI et aux hébergeurs de **procéder au blocage du nom de domaine ou à la rediriger vers un serveur sécurisé de l'ANSSI ou vers un serveur neutre**. Cette opération permet en effet à l'ANSSI d'observer le mode opératoire de l'attaquant et d'identifier, le cas échéant, de nouvelles victimes.

L'ANSSI peut également demander à l'office d'enregistrement ou aux bureaux d'enregistrement des noms de domaine d'**enregistrer, renouveler, suspendre ou transférer le nom de domaine concerné par la menace**. L'objectif de telles dispositions est de s'assurer que le blocage du nom de domaine ne peut être contourné par l'attaquant, tout en préservant l'anonymat de l'ANSSI afin qu'elle puisse caractériser la menace sans que l'attaquant n'en soit informé.

L'étude d'impact détaille les avantages attendus de l'ensemble de ces mesures. Celles-ci vont ainsi « *contribuer à renforcer la sécurité des systèmes d'information en France par la sécurisation du système de noms de domaine contre les agissements d'acteurs malveillants en cas de menace susceptible de porter atteinte à la sécurité nationale.* [Elles permettront] *de neutraliser l'utilisation dévoyée d'un nom de domaine par un cyber attaquant, d'améliorer la compréhension des modes opératoires d'attaque et donc, d'agir en conséquence.* »

Votre rapporteure comprend que l'ensemble des procédures de blocage administratif déjà existantes, ainsi que celle prévue par le présent article, servent des intérêts distincts et concernent des périmètres d'acteurs différents. Elle regrette néanmoins qu'**une harmonisation de certaines d'entre elles** – en particulier, les blocages permis au titre de la LCEN et celui de l'article 32 – ne soit à ce stade pas prévue, et invite le Gouvernement à engager une réflexion sur ce sujet, qu'ont

---

(1) Pour des raisons légistiques, ces interlocuteurs sont visés dans le texte de loi par la mention « personne mentionnée au 1 ou au 2 du I de l'article 6 de la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique ».

soulevé plusieurs auditionnés directement concernés par ces dispositions au cours de leur audition.

C. DES GARANTIES DE NÉCESSITÉ ET DE PROPORTIONNALITÉ DES MESURES INSCRITES À L'ARTICLE (ALINÉAS 10 À 14)

Outre la proportionnalité de la disposition inhérente à **la distinction entre le propriétaire du nom de domaine de bonne foi et le propriétaire malveillant**, l'article L. 2321-2-3 du code de la défense apporte plusieurs garanties :

– d'une part, les mesures que peut ordonner l'ANSSI sont prises dans **un délai ne pouvant être inférieur à quarante-huit heures** ;

– ces mesures doivent être « *mises en œuvre* ***pour la durée et dans la mesure strictement nécessaires et proportionnées dans leurs effets*** », aux seuls fins de prévenir, caractériser et neutraliser la menace ;

– s'agissant plus particulièrement de la **redirection du nom de domaine vers un serveur sécurisé de l'ANSSI**, l'article prévoit qu'une telle mesure ne peut **excéder une durée de deux mois, reconductible une seule fois** en cas de persistance de la menace, et après avis de l'ARCEP. Cette mesure doit, en revanche, cesser sans délai lorsque la menace est maîtrisée ;

– les autres mesures sont également **soumises au contrôle de l'ARCEP** et l'ensemble des mesures susceptibles d'être ordonnées par l'ANSSI seront susceptibles de **recours devant le juge administratif**, dans les conditions du droit commun ;

– les données collectées dans le cadre des mesures prises à l'encontre des propriétaires de noms de domaine malveillants sont **conservées sur une durée maximale de dix ans**. Les autres données sont détruites sans délai lorsqu'elles ne sont pas utiles à la caractérisation de la menace, à l'exception des données permettant d'identifier les utilisateurs ou les détenteurs des systèmes d'information menacés.

Dans son avis sur le projet de loi, le Conseil d'État observe que « *le dispositif envisagé est justifié par la sauvegarde des intérêts fondamentaux de la Nation et par la prévention des atteintes à l'ordre public [de sorte que] l'atteinte portée aux droits et libertés* (…) *est adaptée, nécessaire et proportionnée au motif d'intérêt général qui la justifie.* » [(1)]

D. LA PRISE D'UN DÉCRET EN CONSEIL D'ÉTAT (ALINÉA 15)

Enfin, l'article 32 prévoit qu'un décret en Conseil d'État, pris après avis de l'ARCEP, précisera les **modalités d'application** de cet article.

---

(1) Point 36.

Ce même décret précisera les **modalités de compensation des surcoûts** à la charge des FAI, des hébergeurs et de l'office d'enregistrement et des bureaux d'enregistrement des noms de domaine. L'étude d'impact indique que le montant de compensation des surcoûts « *pourrait être déterminé après consultation des entités concernées au regard de leurs pratiques existantes (coût d'un blocage, prix d'un transfert de nom de domaine qui va de 2 à 100 euros par an et par nom de domaine pour une dizaine de demandes par an,* etc.) »

*

* *

Article 33

(Art. L. 2321-3-1 *[nouveau]* du code de la défense)

Transmission à l'ANSSI de données techniques non identifiantes aux fins de détection et de caractérisation des attaques informatiques

➢ **Résumé du dispositif et effets principaux**

Aux fins de détection et de caractérisation des attaques informatiques, l'article 33 permet aux agents de l'ANSSI d'être destinataires des données techniques non identifiantes enregistrées temporairement sur les serveurs des opérateurs de communications électroniques et des fournisseurs de système de résolution de noms de domaine.

1. Le droit existant

Le système DNS (1) a pour objet de faire correspondre une adresse IP et un nom de domaine : cette opération s'appelle la « **résolution de nom de domaine** » et est proposée par des **fournisseurs de système de résolution de noms de domaine**.

Afin de limiter le temps nécessaire à la réalisation de cette opération, ces prestataires **conservent, de manière temporaire, certaines données dites « données de cache » dans leurs serveurs**. Le but de ce stockage est ainsi de diminuer le temps d'accès ultérieur à ces données. Ces données sont généralement conservées moins d'une journée, et parfois seulement sur des délais très courts dans le cas d'attaques malveillantes.

À cette fin, les fournisseurs de système de résolution de noms de domaine conservent donc **l'adresse IP du périphérique utilisé pour faire la recherche** (par exemple, l'ordinateur de l'utilisateur), ainsi que **le nom de domaine demandé, la date de cette demande et les adresses IP des différentes machines interrogées**.

(1) dont le fonctionnement est détaillé supra sous le commentaire de l'article 32.

2. Le dispositif proposé

L'article 33 crée un nouvel article L. 2321-3-1 au sein du code de la défense. Celui-ci permet à l'ANSSI, « *pour les seuls besoins de la sécurité des systèmes d'information et aux seules fins de détecter et de caractériser des attaques informatiques* », de solliciter auprès des opérateurs de communication électronique et des fournisseurs de système de résolution de noms de domaine les d**onnées de cache non identifiantes** enregistrées de manière temporaire dans leurs serveurs. L'ANSSI vise ainsi **l'ensemble des situations où l'utilisation de noms de domaine est motivée par des intentions malveillantes**.

La notion d'opérateur de communications électroniques

La notion d'opérateur de communications électroniques est définie au 15° de l'article L. 32 du code des postes et des communications électroniques : *« On entend par opérateur toute personne physique ou morale exploitant un réseau de communications électroniques ouvert au public ou fournissant au public un service de communications électroniques.* » Deux critères alternatifs le définissent : il s'agit de « toute personne physique ou morale exploitant un réseau de communications électroniques ouvert au public » ou « fournissant au public un service de communications électroniques ».

Aux termes du 6° du même article : « *On entend par services de communications électroniques, les services fournis via des réseaux de communications électroniques qui comprennent au moins l'un des types de services suivants : / - un service d'accès à Internet ; / - un service de communications interpersonnelles ; / - un service consistant entièrement ou principalement en la transmission de signaux tels que les services de transmission utilisés pour la fourniture de services de machine à machine et pour la radiodiffusion. / Ne sont pas visés les services consistant à fournir des contenus transmis à l'aide de réseaux et de services de communications électroniques ou à exercer une responsabilité éditoriale sur ces contenus.* »

Les fournisseurs de système de résolution de noms de domaine n'étant définis dans aucun texte de loi, le troisième alinéa en apporte une première définition, insérée directement au sein de ce nouvel article L. 2321-3-1. Il s'agit de « *toute personne mettant à disposition un service permettant la traduction d'un nom de domaine en un numéro unique identifiant un appareil connecté à internet.* »

Le quatrième alinéa apporte deux garanties dans l'exercice de cette prérogative :

– d'une part, les données recueillies **ne doivent pas être directement ou indirectement identifiantes**. L'étude d'impact précise que les données non identifiantes collectées concerneront uniquement **le nom du serveur de réponse, son adresse IP ainsi que la date de la réponse**. Un décret pris en Conseil d'État, après avis de l'ARCEP, fixera les modalités de l'article, et en particulier les données techniques collectées par les agents de l'ANSSI.

Ces données **ne peuvent pas être considérées comme des données à caractère personnel**, définies à l'article 4 du règlement dit RGPD [(1)], comme « *toute information se rapportant à une personne physique identifiée ou identifiable* », et précisant qu'« *est réputée être une "personne physique identifiable" une personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale* ».

Dans son avis (point 37) le Conseil d'État rappelle d'ailleurs que, « *si les adresses IP peuvent de manière générale, constituer des données personnelles, cette caractérisation résulte de la circonstance que ces données "permettent l'identification précise [des] utilisateurs" (CJUE, 24 novembre 2011, Scarlet Extended, n° C-70/10). Or, en l'espèce, les adresses IP collectées sont des données non identifiantes qui ne concernent que des noms de domaine et non des utilisateurs. Par conséquent, elles n'ont pas, en l'espèce, le caractère de données personnelles* ».

Votre rapporteure observe d'ailleurs que **la formulation employée dans l'article affirme clairement cette garantie** : les « *données techniques non identifiantes enregistrées de manière temporaire par* [les] *serveurs gérant le système d'adressage par domaines* » concernent en effet un périmètre plus circonscrit de données que les « données de cache », qui incluent notamment les adresses IP source, lesquelles sont identifiantes (et dont le présent article ne prévoit ainsi pas la collecte).

– d'autre part, la collecte de données doit uniquement permettre de **servir « *les seuls besoins de la sécurité des systèmes d'information* *et aux seules fins de détecter et de caractériser des attaques informatiques* ».

Il est précisé dans l'étude d'impact que **l'ARCEP aura un accès permanent à la base stockant ces données** et pourra ainsi exercer un plein contrôle sur le respect de ces garanties. Cette prérogative ne figure pas à l'article 33, mais est visée, pour des considérations légistiques, aux alinéas 17, 25 et suivantes de l'article 35.

L'étude d'impact justifie l'intérêt de cette disposition. Ainsi, « *le dispositif envisagé permettrait à l'ANSSI de connaître les requêtes DNS qui ont été effectuées par les clients, légitimes et malveillants, de manière anonymisée, pour identifier l'infrastructure de l'attaquant et suivre son activité. On pourrait, par exemple, considérer une situation opérationnelle dans laquelle les attaquants mettraient en place des serveurs d'attaque spécifiques pour leurs victimes en France. Une entrée du résolveur (ou journaux) pourrait être collectée pendant les recherches. Par ce*

(1) Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016, relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données).

biais, l'ANSSI pourrait alors accéder aux données relatives à la requête DNS, son horodatage et au résolveur ayant résolu la requête. Les résolveurs étant spécialisés par périmètre (téléphonie mobile, secteur d'activité, etc.*) chez les opérateurs de communications électroniques et les fournisseurs de système de résolution de noms de domaine, les données obtenues par l'ANSSI permettraient de caractériser plus finement l'attaque et la stratégie de l'attaquant.* »

*

* *

Article 34

(Art. L. 2321-4 *[nouveau]* du code de la défense)

Obligation d'information de l'ANSSI et des utilisateurs par les éditeurs de logiciel en cas de vulnérabilité significative ou d'incident informatique

➢ **Résumé du dispositif et effets principaux**

L'article 34 renforce les exigences de transparence qui s'appliquent aux éditeurs de logiciel en contraignant ces derniers à informer l'ANSSI et leurs utilisateurs en cas de vulnérabilité significative ou d'incident informatique susceptible d'affecter un de leurs produits.

1. Le droit existant

a. L'existence d'obligations d'information pour certains acteurs du numérique

Certains acteurs du numérique sont déjà contraints par des obligations d'information. C'est notamment le cas :

– des **responsables de traitement de données personnelles** : les articles 58 et 83 de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés obligent ces responsables à notifier à la Cnil, ainsi qu'à chaque personne concernée, toute violation de données à caractère personnel, définie comme « *toute violation de la sécurité entraînant accidentellement ou de manière illicite la destruction, la perte, l'altération, la divulgation ou l'accès non autorisé à des données à caractère personnel faisant l'objet d'un traitement dans le cadre de la fourniture au public de services de communications électroniques* » ;

– des **opérateurs d'importance vitale** (OIV) : l'article L. 1332-6-2 du code de la défense dispose ainsi qu'ils informent sans délai le Premier ministre des incidents affectant le fonctionnement ou la sécurité d'un de leurs systèmes d'information. Introduits dans le code de la défense par la loi de programmation militaire de 2013 et identifiés par l'État comme des opérateurs réalisant des activités indispensables à la survie de la nation, ces acteurs sont ainsi soumis à des obligations particulières en matière de sécurisation des systèmes d'information et sont accompagnés spécialement par l'ANSSI dans ce processus ;

– des **opérateurs de services essentiels** (OSE) et des **fournisseurs de services numériques** (FSN) : les articles 7 et 13 de la loi n° 2018-133 du 26 février 2018 portant diverses dispositions d'adaptation au droit de l'Union européenne dans le domaine de la sécurité dispose que ceux-ci doivent déclarer à l'ANSSI les incidents affectant les réseaux et systèmes d'information nécessaires à la fourniture de services essentiels, lorsque ces incidents ont ou sont susceptibles d'avoir un impact significatif sur la continuité de ces services. L'ANSSI peut prendre des mesures d'information du public lorsqu'une telle information est nécessaire pour prévenir ou traiter un incident ;

Les opérateurs d'importance vitale (OIV) et de services essentiels (OSE)

La notion d'**opérateurs d'importance vitale** (OIV), introduite dans le code de la défense par la loi de programmation militaire de 2013, désigne « *les opérateurs publics ou privés exploitant des établissements ou utilisant des installations et ouvrages, dont l'indisponibilité risquerait de diminuer d'une façon importante le potentiel de guerre ou économique, la sécurité ou la capacité de survie de la nation* ». Elle concerne plus d'une centaine d'opérateurs identifiés par l'État exerçant des activités ayant trait à la production et la distribution de biens ou de services indispensables, dès lors que ces activités sont difficilement substituables ou remplaçables, ou qui peuvent présenter un danger grave pour la population (1).

Le texte de l'article L. 1332-1 du code de la défense impose à ces opérateurs de coopérer à leurs frais, sur la base d'un plan individuel élaboré en concertation avec l'État, à la protection de leurs établissements contre toute menace, notamment à caractère terroriste. Ces acteurs sont entre autres soumis à des obligations particulières en matière de sécurisation des systèmes d'information.

Ainsi, le Premier ministre peut imposer des règles en matière de sécurité informatique, notamment l'installation de dispositifs de détection, qui devront être appliqués par les OIV à leurs frais (2). Ces opérateurs doivent par ailleurs informer le Premier ministre des attaques informatiques dont ils sont victimes (3), leurs systèmes d'information peuvent, à sa demande, faire l'objet d'un contrôle de l'ANSSI (4) et des mesures particulières peuvent être décidées à son initiative en cas de crise majeure menaçant ou affectant la sécurité des systèmes d'information (5).

La directive sur la sécurité des réseaux et des systèmes d'information du 6 juillet 2016, dite directive NIS (6), transposée par la loi n° 2018-133 du 26 février 2018 portant diverses dispositions d'adaptation au droit de l'Union européenne dans le domaine de la sécurité, a par la suite créé la catégorie des **opérateurs de services essentiels** (OSE).

Les OSE sont définis à l'article 5 de la directive comme « *les opérateurs, publics ou privés, offrant des services essentiels au fonctionnement de la société ou de l'économie*

(1) Article R. 1332-2 du code de la défense.

(2) Article L. 1332-6-1 du même code.

(3) Article L1332-6-2 du même code.

(4) Article L. 1332-6-3 du même code.

(5) Article L. 1332-6-4 du même code.

(6) Directive (UE) 2016/1148 du Parlement européen et du Conseil du 6 juillet 2016 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union.

et dont la continuité pourrait être gravement affectée par des incidents touchant les réseaux et systèmes d'information nécessaires à la fourniture desdits services ».

Un service essentiel correspond à 3 critères : ce service est essentiel au maintien d'activités sociétales ou économiques critiques ; la fourniture de ce service est tributaire des réseaux et des systèmes d'information ; un incident sur ces réseaux et systèmes aurait un effet disruptif important sur la fourniture dudit service.

Le décret du 23 mai 2018 (1) précise les critères d'identification des OSE, renvoyant à une liste d'activités, de sous-secteurs et d'entités figurant en annexe de ce décret. Tenant compte de ces éléments, l'ANSSI apprécie l'appartenance d'un opérateur ou non à cette catégorie en fonction de plusieurs critères (2), et soumet une liste au Premier ministre, auquel il revient la décision de désignation (3).

Un opérateur identifié comme OSE est notamment soumis à des obligations en matière d'application de règles de sécurité aux réseaux et systèmes d'informations essentiels (SIE) identifiés par l'OSE, et de notification à l'ANSSI en cas d'incident de sécurité (4).

– des **opérateurs de communications électroniques**, pour lesquels l'article L. 33-1 du code des postes et des communications électroniques prévoit « *des obligations de notification à l'autorité compétente des incidents de sécurité ayant eu un impact significatif sur leur fonctionnement* ».

En revanche, **il n'existe pas d'obligation légale contraignant les éditeurs de logiciels** à déclarer à l'ANSSI d'éventuelles vulnérabilités et à en informer leurs utilisateurs, qui ne sont dès lors notifiés que dans la mesure où ces vulnérabilités emportent des conséquences sur les données à caractère personnel. L'ANSSI n'est en effet compétente que pour traiter des vulnérabilités concernant l'État, les autorités publiques ainsi que certains opérateurs publics et privés. Son périmètre d'action ne couvre donc pas les éditeurs de logiciels.

Pourtant, l'étude d'impact relève que « *les éditeurs peuvent sous-estimer les conséquences, pour leurs utilisateurs et pour l'écosystème numérique, de l'existence de vulnérabilités. Surdéterminant les réactions potentielles des marchés financiers ou des investisseurs, ils peuvent ainsi s'avérer réticents à transmettre à leurs utilisateurs d'éventuelles faiblesses dans leurs produits. De surcroît, l'éditeur seul ne dispose pas toujours des capacités techniques suffisantes pour identifier les utilisateurs* (…) *et les alerter de manière efficace.* »

---

(1) Décret n° 2018-384 du 23 mai 2018 relatif à la sécurité des réseaux et systèmes d'information des opérateurs de services essentiels et des fournisseurs de service numérique.

(2) Ces critères sont précisés à l'article 2 du décret précité. 1° le nombre d'utilisateurs dépendant du service ; 2° la dépendance des autres secteurs d'activités figurant à l'annexe au présent décret à l'égard du service ; 3° les conséquences qu'un incident pourrait avoir, en termes de gravité et de durée, sur le fonctionnement de l'économie ou de la société ou sur la sécurité publique ; 4° la part de marché de l'opérateur ; 5° la portée géographique eu égard à la zone susceptible d'être touchée par un incident ; 6° l'importance que revêt l'opérateur pour assurer un niveau de service suffisant, compte tenu de la disponibilité de moyens alternatifs pour la fourniture du service ; 7° le cas échéant, des facteurs sectoriels.

(3) Article 5 de la loi n° 2018-133 du 26 février 2018 portant diverses dispositions d'adaptation au droit de l'Union européenne dans le domaine de la sécurité.

(4) Articles 7 et 8 de la loi précitée.

b. La publicité des menaces sur le site du CERT-FR

Lorsqu'un logiciel est fragilisé par une vulnérabilité, une alerte peut être publiée sur le site du **Centre gouvernemental de veille, d'alerte et de réponse aux attaques informatiques** (CERT-FR), qui assure notamment une mission de détection de la vulnérabilité des systèmes, sous l'autorité de l'ANSSI.

Des **campagnes de signalement** peuvent par ailleurs être mises en œuvre lorsque ces vulnérabilités concernent les logiciels les plus utilisés ou ceux particulièrement répandus parmi les administrations publiques ou les entreprises. Ces campagnes ont lieu, lorsque l'ANSSI a connaissance d'une vulnérabilité critique pouvant affecter ses bénéficiaires, sous la forme de courriels contenant des recommandations et les mesures à appliquer et sont parfois accompagnées du déploiement par l'ANSSI de moyens de détection.

2. Le dispositif proposé

L'article 34 créé un nouvel article L. 2321-4-1 au sein du code de la défense. Cet article impose à certains éditeurs une double obligation :

– **la notification à l'ANSSI de « *toute vulnérabilité significative* *affectant un de leurs produits* » ou « *tout incident informatique* *compromettant la sécurité de leurs systèmes d'information susceptible d'affecter un de leurs produits* »** [(1)], ainsi qu'une analyse de leurs causes et conséquences (alinéa 2).

Les notions de « vulnérabilité significative » et d' « incident informatique »

Les acteurs du numérique auditionnés par votre rapporteur ont souligné que les dispositions du texte pouvaient paraître insuffisamment claires, en particulier s'agissant des termes « *vulnérabilité significative* » et « *incident informatique* ».

L'emploi du terme « significatif » existe déjà en droit français, en particulier à l'article D. 98-5 du code des postes et des communications électroniques, dont le III dispose : « *le caractère significatif de l'impact de l'incident de sécurité est déterminé en particulier au regard des paramètres suivants : a) Le nombre d'utilisateurs touchés par l'incident de sécurité ; b) La durée de l'incident de sécurité ; c) L'étendue géographique de la zone touchée par l'incident de sécurité ; d) La mesure dans laquelle le fonctionnement du réseau ou du service est affecté ; e) L'ampleur de l'impact sur les activités économiques et sociétales.* »

Le SGDSN a précisé à votre rapporteure que **l'appréciation d'une « vulnérabilité significative »**, qui sera détaillée par décret, reposera notamment sur **trois critères** : le score CVSS [(2)] associé à la nature du produit (par exemple, s'il exerce un rôle clé dans

(1) Cette dernière précision reprend ainsi une recommandation du Conseil d'État (point 37) qui estimait « nécessaire, pour assurer la proportionnalité de cette obligation, d'en préciser la teneur en limitant le champ des incidents informatiques devant être déclarés par les éditeurs de logiciel à ceux qui sont susceptibles d'affecter l'un de leurs produits. *»*

(2) Le score CVSS (pour « Common Vulnerability Scoring System *») est un système d'évaluation standardisé du caractère critique des vulnérabilités.*

une infrastructure, est largement utilisé, *etc.*), le contexte de son exploitation ainsi que l'évolution de la situation, qui peut amener l'ANSSI a réévaluer le niveau de criticité.

La notion d' « incident » existe dans notre droit, sans être précisément définie (1). La directive NIS 2 propose néanmoins une définition de l'incident, qui représente « *un événement compromettant la disponibilité, l'authenticité, l'intégrité ou la confidentialité des données stockées, transmises ou faisant l'objet d'un traitement, ou des services que les réseaux et systèmes d'information offrent ou rendent accessibles* ». (2)

Le SGDSN a précisé à votre rapporteure qu'il s'agit de cibler, avec cet article, un type précis d'incident informatique – ceux compromettant la sécurité des systèmes d'information de l'éditeur, rappelant qu'il s'agit d'une cible privilégiée des attaquants.

– **l'information des utilisateurs du produit « *dans les meilleurs délais* »**. À défaut, l'ANSSI peut **enjoindre l'éditeur concerné de procéder à cette information**, voire informer les utilisateurs ou rendre publics la vulnérabilité ou l'incident concerné, ainsi que l'injonction qu'elle a adressée à l'éditeur si celui-ci n'y a pas donné suite (alinéa 6) (3).

L'article précise les éditeurs concernés par cette obligation : il s'agit de ceux fournissant le produit sur le territoire français, ou à des sociétés ayant leur siège social ou France, ainsi que les sociétés contrôlées par ces dernières (alinéas 3 à 5).

Enfin, l'article 34 prévoit que ses modalités d'application seront fixées par un décret en Conseil d'État (alinéa 7).

Si l'on fait exception de la procédure d'injonction prévue par l'article, la nouvelle obligation qu'il instaure n'est **assortie d'aucune sanction**. L'étude d'impact justifie ce choix par la menace que pourrait d'ores et déjà représenter, pour la réputation de l'éditeur, la possibilité offerte à l'ANSSI d'informer les utilisateurs du logiciel vulnérable, voire de rendre public le manquement de l'éditeur. Elle précise par ailleurs que cela peut « *constituer une première étape permettant d'habituer les acteurs du marché, sans exclure qu'à l'avenir, une sanction autre que seulement réputationnelle soit introduite par le législateur.* »

Votre rapporteure observe que **cet article s'inscrit, plus largement, dans une dynamique de notification des incidents qui existe déjà dans le droit de l'Union européenne**, s'agissant tant d'incidents portant sur les réseaux ou systèmes

(1) Voir notamment les articles L. 33-1 et D. 98 du code des postes et des communications électroniques, l'article L. 1332-6-2 du code de la défense et l'article 7 de la loi n° 2018-133 du 26 février 2018 portant diverses dispositions d'adaptation au droit de l'Union européenne dans le domaine de la sécurité.

(2) Point 6 de l'article 6 de la 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 (directive SRI 2).

(3) L'information des utilisateurs par l'ANSSI est une recommandation du Conseil d'État (point 37).

d'information que d'incidents relatifs à une violation des données à caractère personnel [(1)].

*

* *

Article 35

(Art. L. 2321-2-1, L. 2321-3 et L. 2321-5 du code de la défense, art. L. 33-14, L. 36-7 et L. 36-14 du code des postes et des communications électroniques)

Renforcement des capacités de détection des cyberattaques et d'information des victimes

➢ **Résumé du dispositif et effets principaux**

D'une part, l'article 35 permet à l'ANSSI, en cas de menace grave sur les systèmes d'information des autorités publiques et des opérateurs stratégiques, et aux seules fins de détection et de caractérisation de la menace, de mettre en œuvre des dispositifs de recueil de données sur le réseau d'un opérateur de communications électroniques ou sur le système d'information d'un fournisseur d'accès, d'un hébergeur ou d'un centre de données.

D'autre part, ce même article rend obligatoire, pour les opérateurs de communications électroniques qualifiés d'« opérateurs d'importance vitale », la mise en œuvre de systèmes de détection des attaques informatiques.

Enfin, il élargit aux hébergeurs de données l'obligation de communiquer à l'ANSSI certaines informations concernant des utilisateurs ou systèmes d'information vulnérables, menacés ou attaqués, afin de les alerter sur la vulnérabilité ou l'atteinte de leur système d'information, et supprime l'assermentation des agents de l'ANSSI habilités à obtenir ces informations. Il complète également une disposition permettant déjà à ces mêmes agents d'obtenir, de la part des opérateurs stratégiques et des autorités publiques victimes d'un évènement affectant la sécurité de leur système d'information, les données techniques nécessaires à l'analyse de cet évènement, en étendant cette prérogative aux sous-traitants de ces entités.

➢ **Dernières modifications législatives intervenues**

Depuis l'entrée en vigueur de la loi n° 2018-607 du 13 juillet 2018 relative à la programmation militaire pour les années 2019 à 2025, l'article L. 2321-2-1 du code de la défense habilite l'ANSSI, sous certaines conditions, à mettre en œuvre sur certains réseaux et systèmes d'information des dispositifs de détection des événements susceptibles d'affecter la sécurité des systèmes d'information des autorités publiques, des OIV ou des OSE.

---

(1) 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 (directive SRI 2).

La loi précitée a également créé l'article L. 33-14 du code des postes et des communications électroniques, qui permet aux opérateurs de communications électroniques de mettre en œuvre, sur leurs réseaux, des systèmes de détection des attaques informatiques visant leurs abonnés, exploitables par l'ANSSI en cas de menace.

Enfin, la loi de programmation militaire 2014-2019 (1) a créé un article L. 2321-3 au sein du code de la défense qui permet à l'ANSSI, en cas d'attaque informatique concernant des autorités publiques, OIV ou OSE, d'obtenir l'adresse IP, l'adresse postale et l'adresse électronique des utilisateurs de systèmes fragilisés afin de les informer de cette attaque. La loi du 13 juillet 2018 a introduit deux nouveaux alinéas à cet article permettant notamment à l'ANSSI, en cas d'événement visant les autorités publiques, OIV et OSE, d'obtenir les données techniques nécessaires à l'analyse de cet évènement auprès des OCE.

I. LE RENFORCEMENT DES CAPACITÉS DE DÉTECTION D'ÉVÈNEMENTS POUVANT ATTEINDRE LES SYSTÈMES D'INFORMATION DES AUTORITÉS PUBLIQUES ET DES OPÉRATEURS STRATÉGIQUES

Ainsi qu'en dispose l'article L. 2321-2-1 du code de la défense depuis la précédente loi de programmation militaire, l'ANSSI peut d'ores et déjà mettre en place des marqueurs techniques afin d'identifier une menace circulant sur les réseaux. L'article 35 complète cette disposition et vise à lui permettre, sous certaines conditions, de procéder à des recueils de données sur un réseau ou un système d'information.

A. DES CAPACITÉS DE DÉTECTION DÉJÀ EXISTANTES MAIS AUJOURD'HUI INSUFFISANTES

1. Le recours aux marqueurs techniques pour prévenir les menaces à l'encontre des systèmes d'information les plus sensibles

L'article 34 de la loi n° 2018-607 du 13 juillet 2018 relative à la programmation militaire pour les années 2019 à 2025 a inséré l'article L. 2321-2-1 au sein du code de la défense.

Celui-ci permet à l'ANSSI, lorsqu'elle a connaissance d'une menace susceptible de porter atteinte à la sécurité des systèmes d'information des autorités publiques, des OIV et des OSE, de mettre en œuvre, sur le réseau d'un opérateur de communications électroniques (OCE) ou sur le système d'information d'un fournisseur de services de communication au public en ligne ou d'un hébergeur, des **dispositifs de détection des événements susceptibles d'affecter la sécurité de ces systèmes d'information**.

---

(1) Loi n° 2013-1168 du 18 décembre 2013 relative à la programmation militaire pour les années 2014 à 2019 et portant diverses dispositions concernant la défense et la sécurité nationale.

Ces dispositifs de détection, qualifiés de « **marqueurs techniques** », sont définis par l'article R. 2321-1-3 du code de la défense comme des « *éléments techniques caractéristiques d'un mode opératoire d'attaque informatique, permettant de détecter une activité malveillante et d'identifier une menace susceptible d'affecter la sécurité des systèmes d'information. Ils visent à détecter les communications et programmes informatiques malveillants et à recueillir et analyser les seules données techniques nécessaires à la prévention et à la caractérisation de la menace.* »

Les marqueurs techniques

Les marqueurs techniques sont des données techniques qui peuvent être collectées via une sonde intégrée dans un système d'information. Elles permettent la détection de menaces et sont principalement de deux types : les signatures dites « simples » correspondent à un élément technique caractéristique de l'activité d'un attaquant, qui peut être un élément réseau (un nom de domaine qu'il utilise) ou système (le nom d'un fichier qu'il dépose sur la machine de sa victime) ; les signatures « complexes », plus sophistiquées, permettent de reconnaître des ensembles d'éléments techniques (« motifs » ou *patterns*) particuliers dans le trafic réseau, les fichiers, ou l'activité sur le système.

Ces sondes sont connectées à des systèmes de détection d'intrusion par signature, qui reposent sur des bibliothèques de description des attaques (appelées signatures). Au cours de l'analyse du flux réseau, le système de détection d'intrusion analysera chaque événement et une alerte sera émise dès lors qu'une signature sera détectée. Cette signature peut référencer un seul paquet, ou un ensemble (dans le cadre d'une attaque par « déni de service » par exemple), c'est-à-dire une attaque informatique ayant pour but de rendre indisponible un service.

Le déploiement des dispositifs de détection n'est possible que dans le cadre d'une unique finalité : la détection d'événements susceptibles d'affecter la sécurité des systèmes d'information des autorités publiques, des OIV et des OSE.

Par ailleurs, le texte prévoit un encadrement strict quant à la mise en œuvre du dispositif de détection, qui devra répondre à un principe de proportionnalité. Ainsi, il ne pourra être mis en œuvre que « *pour la durée et dans la mesure strictement nécessaires à la caractérisation de la menace* ». L'article R. 2321-1-2 du code de la défense précise à ce titre que ce dispositif est mis en œuvre pour **une période maximale de trois mois**, prorogeable en cas de persistance de la menace et dans cette limite. Toute prorogation fait l'objet d'une décision de l'ANSSI, communiquée à l'ARCEP.

Les données techniques pertinentes sont recueillies et analysées par **des agents de l'ANSSI individuellement désignés et spécialement habilités**, et ne peuvent être conservées plus de dix ans. Par ailleurs, les données recueillies autres que celles directement utiles à la prévention et à la caractérisation des menaces sont immédiatement détruites.

2. Une prérogative contrôlée par l'Arcep

Cette prérogative de l'ANSSI est contrôlée par l'ARCEP. L'article L. 2321-5 du code de la défense dispose ainsi : « *l'Autorité de régulation des communications électroniques et des postes est chargée de veiller au respect par l'autorité nationale de sécurité des systèmes d'information des conditions d'application de l'article L. 2321-2-1* (…) »

L'article L. 36-14 du code des postes et des communications électroniques précise les modalités de ce contrôle, opéré par **la formation de règlement des différends, de poursuite et d'instruction de l'ARCEP**.

Cet article dispose notamment que cette formation est informée sans délai des mesures de détection d'évènements mises en œuvre par l'ANSSI, qui doit lui fournir tous les éléments nécessaires à l'accomplissement de sa mission. Par ailleurs, la formation dispose d'un accès complet et permanent aux données recueillies ou obtenues en application de l'article L. 2321-2-1 du code de la défense.

La formation peut formuler toute recommandation à l'ANSSI, et, en cas de non-respect de cette dernière, l'enjoindre d'interrompre les opérations et de détruire les données collectées. Enfin, lorsque l'ANSSI ne se conforme pas à une injonction, la présidence de l'ARCEP peut saisir le Conseil d'État d'un recours.

3. Une disposition encore incomplète pour faire face à la menace

L'étude d'impact annexée au projet de loi souligne que ces dispositions permettent à l'ANSSI « *d'obtenir, pendant une durée limitée, des informations sur le trafic réseau* [de la machine faisant l'objet d'un marqueur technique]. *Toutefois, en pratique, **les données accessibles demeurent très limitées, permettant seulement de savoir avec quelles autres machines l'attaquant communique**, ainsi que la méthode de communication utilisée* (…). »

Or, selon l'étude d'impact « *la mise en œuvre de marqueurs spécifiques pour détecter des évènements **suppose une connaissance préalable de l'attaquant qui ne peut être obtenue que par l'analyse de l'ensemble de données** figurant sur une machine compromise.* »

La rédaction actuelle contraint pourtant l'ANSSI à **recueillir uniquement les données techniques, dites métadonnées**, la privant de données de contenu et d'informations qu'elle juge nécessaires pour mieux qualifier la menace. Or, les données techniques des flux réseaux auxquelles a accès l'ANSSI sont déclenchées par des actions lancées en amont par des acteurs malveillants à partir de codes et logiciels malveillants, auxquels l'ANSSI n'a pas accès. De surcroît, la mise en place de marqueurs techniques, si elle « *permet de prévenir certaines attaques, implique que l'ANSSI connaisse déjà en amont les modes opératoires utilisés par les attaquants et en ait tiré des marqueurs spécifiques pour pouvoir les détecter.* [Elle] *ne lui permet donc pas de détecter un acteur inconnu ou non caractérisé et ne permet que des actions en réaction.* »

Le recours, par les autorités publiques, les OIV et les OSE, à des sous-traitants, présente par ailleurs une difficulté particulière que le dispositif légal actuel ne prend pas en compte. Ceux-ci se voient en effet accorder des accès aux systèmes d'information « *alors que les mesures de sécurité qu'une entité sensible s'impose sont souvent bien moindres, voire inexistants chez les sous-traitants, lesquels ne disposent en outre pas des mêmes moyens financiers et humains que les entités sensibles et ne sont pas soumises aux mêmes obligations légales. Il en résulte que les attaquants, pour atteindre* in fine *des entités sensibles, utilisent fréquemment leurs sous-traitants comme porte d'entrée.* »

Enfin, l'étude d'impact précise que, lorsqu'un évènement pouvant porter atteinte aux intérêts fondamentaux de la Nation est détecté par l'ANSSI, le recours à des serveurs informatiques compromis est quasi systématique. Or, **la rédaction actuelle de l'article L. 2321-2-1 du code de la défense ne permet pas de cibler les opérateurs de centres de données** qui proposent le recours à ces serveurs, et ne sont juridiquement pas assimilables aux hébergeurs ou aux FAI [(1)].

B. LE DISPOSITIF PROPOSÉ : UNE EXTENSION MATÉRIELLE ET ORGANIQUE DES CAPACITÉS DE DÉTECTION DE L'ANSSI

Les alinéas 2 à 9 du présent article réécrivent les dispositions de l'article L. 2321-2-1 du code de la défense.

Tout en **maintenant la possibilité, pour l'ANSSI, de recourir à des marqueurs techniques** –et **en l'étendant aux opérateurs de centre de données** – l'article 35 lui permet également de **recueillir des données** sur le réseau d'un opérateur de communications électroniques ou sur le système d'information d'un hébergeur, d'un FAI ou d'un opérateur de centre de données. Concrètement, cela permettrait à l'ANSSI d'**accéder au contenu de la machine infectée**, par le biais d'une copie de son disque dur, afin de récupérer les configurations et le détail des codes malveillants utilisés par l'attaquant, ainsi que les données qu'il a dérobées, ses journaux de connexion et les éléments secrets permettant de déchiffrer le trafic malveillant.

Le recours à cette prérogative nécessite **une condition**, déjà présente dans la rédaction actuelle de l'article L. 2321-2-1 : l'ANSSI doit avoir eu connaissance d'une **menace susceptible de porter atteinte à la sécurité de systèmes d'information des autorités publiques, des OIV et des OSE**. En pratique, cela nécessite de remplir deux critères :

---

(1) L'article L. 32 du code des postes et des communications électroniques définit les centres de données comme des « installations accueillant des équipements de stockage de données numériques *» et les opérateurs de centre de données, comme «* toute personne assurant la mise à la disposition des tiers d'infrastructures et d'équipements hébergés dans des centres de données *». Concrètement, il s'agira d'une entreprise mettant à disposition des locaux sécurisés fournissant électricité, refroidissement et armoires pour les serveurs informatiques.*

– d'un point de vue opérationnel, la justification d'une menace auprès de l'OCE, l'hébergeur ou l'opérateur de centre de données par l'ANSSI, dont la portée réelle est appréciée par l'ARCEP, ainsi qu'en dispose l'alinéa 34 du présent article(1) ;

– par la nature des systèmes d'information visés, à savoir le fait qu'ils concernent ceux d'une autorité publique, d'un OIV ou d'un OSE.

Plusieurs garanties assurent la proportionnalité de ce dispositif (2). D'une part, un tel recueil de données ne peut être réalisé qu'après avis conforme de l'ARCEP et n'est permis qu'aux **agents de l'ANSSI individuellement désignés et spécialement habilités**, aux seules fins de prévention et de caractérisation de la menace et à l'exclusion de toute autre exploitation. Cela implique, en amont, d'avoir ciblé la machine compromise faisant l'objet de la copie. D'autre part, **les données directement utiles sont conservées pour une durée maximale de deux ans** – la durée de conservation a ainsi été réduite puisqu'elle est, dans la rédaction actuelle de l'article, de dix ans – et celles n'étant pas utiles à la menace sont supprimées sans délai. Un décret en Conseil d'État définira les modalités d'application de l'article.

Les possibilités ouvertes par le présent article seront ainsi circonscrites aux menaces les plus graves. Selon les informations transmises par le SGDSN à votre rapporteure, l'ANSSI devrait exploiter une vingtaine de marqueurs techniques, réaliser une vingtaine de recueils de données sur les flux réseaux et une cinquantaine de recueils de données sur les systèmes d'information chaque année.

II. LE RENFORCEMENT DES CAPACITÉS DE DÉTECTION SUR LES RÉSEAUX DES OPÉRATEURS DE COMMUNICATIONS ÉLECTRONIQUES

Le présent article modifie l'article L. 33-14 du code des postes et communications électroniques relatif aux capacités de détection des menaces pouvant être mis en place sur les réseaux des opérateurs de communication électroniques, mis en place par la précédente loi de programmation militaire. De simple faculté proposée aux OCE, elle deviendrait désormais obligatoire pour les

---

(1) Le SGDSN a précisé à votre rapporteure que l'ANSSI soumettra ainsi à l'ARCEP chaque projet de collecte de données malveillantes, qui accepterait, refuserait ou réviserait la demande. Le recueil se fera par le biais d'une sonde de détection des attaques, placée entre les réseaux ou le système d'information de l'opérateur affecté par la menace et les flux intérieurs à ces réseaux ou à ce système d'information. Seuls les éléments utiles à la prévention ou susceptibles de constituer des marqueurs d'attaque seront conservés.

(2) Ce que constate le Conseil d'État dans son avis (point 38). Celui-ci relève en effet que, si « le recueil de telles données porte atteinte au droit au respect de la vie privée, au droit à la protection des données personnelles, au secret des correspondances et à la liberté d'expression *(…) [celui-ci]* est motivé par la sauvegarde des intérêts fondamentaux de la Nation *(…)* les seules données analysées, dont la conservation est limitée à deux ans, sont celles qui sont directement utiles à la prévention et à la caractérisation de la menace, les autres données devant être détruites sans délai. Seuls les agents de l'ANSSI individuellement désignés et spécialement habilités peuvent procéder à leur analyse, dans la seule finalité précédemment évoquée. Enfin, cette possibilité de recueil ne peut être mise en œuvre que sur avis conforme de l'ARCEP. En conséquence, le Conseil d'État estime que les atteintes portées par ce nouveau dispositif aux droits et libertés précédemment évoqués sont adaptées, nécessaires et proportionnées à l'objectif poursuivi. »

opérateurs qualifiés d'OIV (ce qui concerne quatre OCE en France sur environ 3 500 opérateurs, selon les chiffres transmis à votre rapporteure par le SGDSN).

A. LA LOI DU 13 JUILLET 2018 A PERMIS LA MISE EN ŒUVRE FACULTATIVE DE CAPACITÉS DE DÉTECTION SUR LES RÉSEAUX DES OCE

1. Un dispositif facultatif proposé aux OCE…

L'article L. 33-14 du code des postes et des communications électroniques, créé par la loi n° 2018-607 du 13 juillet 2018 relative à la programmation militaire pour les années 2019 à 2025, permet aux OCE de **recourir, sur les réseaux qu'ils exploitent, à des marqueurs techniques**. Cette possibilité est néanmoins conditionnée à une information préalable de l'ANSSI et ne peut se faire que pour les besoins de la sécurité et de la défense des systèmes d'information (alinéa 1).

L'étude d'impact précise à ce titre que les systèmes de détection visés par cet alinéa sont des « ***dispositifs techniques qui comparent en temps réel l'activité d'un réseau à des marqueurs d'attaque*** *(ces marqueurs sont des éléments techniques propres à certains attaquants, tels que l'adresse IP d'un serveur malveillant ou le nom d'un site internet piégé). Ceux-ci analysent automatiquement le trafic sans s'intéresser au contenu, en se limitant à le comparer aux marqueurs d'attaque. Le trafic n'est pas stocké.* »

Les données techniques strictement nécessaires à la caractérisation d'un évènement peuvent être **conservées pendant six mois**, les autres devant être détruites immédiatement (alinéa 3). L'article R. 10-15 du code des postes et des communications électroniques précise les données pouvant être conservées par les opérateurs dans ce cadre.

Code des postes et des communications électroniques

Article R. 10-15. – En application de l'article L. 33-14, les opérateurs de communications électroniques sont autorisés à conserver, lorsqu'elles sont associées à une alerte mentionnée au II de l'article R. 9-12-1 et à l'exclusion du contenu des correspondances échangées :

1° Les données techniques permettant d'identifier l'origine de la communication et l'utilisateur ou le détenteur du système d'information affecté par l'événement détecté ;

2° Les données techniques relatives à l'acheminement de la communication par un réseau de communications électroniques, notamment le routage et le protocole utilisé ;

3° Les données techniques relatives aux équipements terminaux de communication concernés ;

4° Les caractéristiques techniques ainsi que la date, l'horaire, le volume et la durée de chaque communication ;

5° Les données techniques relatives à l'accès des équipements terminaux aux réseaux ou aux services de communication au public en ligne ;

6° Les caractéristiques techniques ainsi que la date et l'horaire de l'alerte dont l'utilisation des marqueurs techniques est à l'origine.

La conservation de ces données est limitée au temps strictement nécessaire à la prévention et à la caractérisation des événements susceptibles d'affecter la sécurité des systèmes d'information des abonnés sans excéder six mois.

L'ANSSI peut, lorsqu'elle a connaissance d'une menace susceptible de porter atteinte à la sécurité des systèmes d'information, **demander aux OCE d'exploiter ces systèmes de détection** (alinéa 2). Elle fournit à cette fin des marqueurs d'attaque : lorsqu'une attaque informatique est menée en lien avec ces marqueurs, les systèmes de détection des OCE produisent une alerte de sécurité. Quand un tel évènement est détecté sur leurs réseaux, les OCE doivent informer sans délai l'ANSSI, qui peut exiger d'eux d'informer leurs abonnés sur la vulnérabilité de leurs systèmes d'information ou sur des atteintes qu'ils ont subies (alinéas 4 et 5).

Si la menace concerne une autorité publique, un OIV ou un OSE, l'article L. 2321-3 du code de la défense, complété de deux nouveaux alinéas par la loi du 13 juillet 2018, permet aux agents de l'ANSSI habilités par le Premier ministre et assermentés, de **demander aux OCE les données techniques strictement nécessaires à l'analyse de cet événement** (par exemple, la volumétrie et le type de trafic), aux seules fins de caractérisation de la menace, voire d'information de la victime potentielle.

2. … qui paraît aujourd'hui insuffisant pour répondre à la menace cyber

L'étude d'impact annexée au projet de loi estime que le dispositif prévu par l'article L. 33-14 du code des postes et des communications électroniques n'a pas permis de répondre pleinement à l'objectif du législateur, du fait de son caractère

facultatif, alors même qu'il nécessite, lorsqu'il est respecté, d'importants investissements incombant aux OCE.

Cette disposition pourrait pourtant s'avérer très utile pour l'ANSSI : les cyberattaques transitent en effet par le réseau des opérateurs. L'étude d'impact estime à ce titre que « *le développement de la capacité des opérateurs à détecter efficacement les traces des cyberattaques serait une avancée majeure dans la lutte contre les cyberattaques touchant les entreprises et les administrations françaises.* »

B. LE DISPOSITIF PROPOSÉ : LA MISE EN ŒUVRE OBLIGATOIRE DE SYSTÈMES DE DÉTECTION DES ATTAQUES INFORMATIQUES POUR LES OCE DÉSIGNÉS OPÉRATEURS D'INTÉRÊT VITAL

Le présent article modifie les articles L. 33-14 du code des postes et des communications électroniques et L. 2321-3 du code de la défense afin de faire évoluer les modalités légales de mise en œuvre de systèmes de détection.

Les alinéas 20 à 22 réécrivent les deux premiers alinéas de l'article L. 33-14 du CPCE, qui détermine les modalités selon lesquelles les OCE peuvent recourir à des dispositifs mettant en œuvre des marqueurs techniques sur leurs réseaux.

La réécriture conduit à supprimer cette faculté, pour **la rendre obligatoire pour les seuls opérateurs de communications électroniques désignés opérateurs d'intérêt vital**. La réécriture complète la rédaction actuelle de l'article en indiquant que « *ces dispositifs sont mis en œuvre pour répondre aux demandes de l'ANSSI* ».

Lors de leur audition, les représentants du SGDSN et de l'ANSSI ont défendu cette position médiane qui consiste à tirer les leçons des difficultés liées à la rédaction actuelle du dispositif, qui le fait reposer sur la bonne volonté des acteurs, et sur la volonté de ne pas entraver l'activité des OCE par une obligation trop lourde. L'étude d'impact justifie ce choix, relevant que « *plus l'opérateur est important, plus les flux qui transitent par son réseau sont conséquents, ce qui permet de maximiser l'efficacité des marqueurs fournis par l'ANSSI.* »

L'article prévoit d'indemniser les OCE pour les surcoûts liés à la mise en œuvre de cette mesure (alinéa 24). L'ANSSI évalue son coût à un million d'euros par an.

III. UNE MEILLEURE INFORMATION DES VICTIMES DE CYBERATTAQUES ET LA SUPPRESSION DE L'ASSERMENTATION DES AGENTS DE L'ANSSI

L'article 35 préconise d'élargir le périmètre de l'article L. 2321-3 du code de la défense – dont l'une des finalités est de mieux informer les victimes de cyber-assaillants – en intégrant d'autres acteurs concernés par les cyberattaques. À des fins d'allégement procédural, il propose également de supprimer l'assermentation des agents de l'ANSSI ciblés à ce même article.

A. L'ÉTAT DU DROIT : DES DISPOSITIONS PARTICULIÈRES S'AGISSANT DES CYBER ATTAQUES VISANT DES OPÉRATEURS STRATÉGIQUES

L'article L. 2321-3 du code de la défense a deux finalités. D'une part, il permet à des agents habilités par le Premier ministre et assermentés de l'ANSSI, pour les besoins de la sécurité des systèmes d'information des autorités publiques, OIV et OSE, d'**obtenir auprès des OCE l'identité, l'adresse postale et l'adresse électronique d'utilisateurs ou de détenteurs de systèmes d'information vulnérables, menacés ou attaqués, afin de les alerter sur la vulnérabilité ou l'atteinte de leur système**. Il s'agit d'une disposition permettant à l'ANSSI d'informer facilement la victime en cas d'attaque.

L'habilitation et l'assermentation des agents de l'ANSSI – extraits de la partie réglementaire du code de la défense

Art. R. 2321-2. – Les habilitations prévues aux articles L. 2321-2-1 et L. 2321-3 sont accordées, de manière individuelle, par décision du Premier ministre à des agents de l'ANSSI.

Nul ne peut être habilité s'il n'a fait l'objet d'une enquête administrative conformément à l'article L. 114-1 du code de la sécurité intérieure. Si besoin, l'enquête administrative peut être reconduite pendant la période d'habilitation de l'agent (…)

L'habilitation peut être retirée à tout moment par décision du Premier ministre. Elle prend fin lorsque son titulaire n'exerce plus les fonctions à raison desquelles il a été habilité.

Art. R. 2321-3. – Pour accomplir leur mission prévue à l'article L. 2321-3, les agents habilités de l'ANSSI présentent une commission d'emploi aux opérateurs de communications électroniques. La commission d'emploi mentionne la décision d'habilitation de l'agent.

Tout agent qui n'est plus habilité remet sans délai sa commission d'emploi à l'ANSSI.

Art. R. 2321-4. – Les agents habilités de l'ANSSI prêtent devant le tribunal judiciaire dans le ressort duquel ils exercent leurs fonctions le serment suivant : « *Je jure de bien et fidèlement remplir la mission pour laquelle je suis habilité et de ne rien révéler ou utiliser de ce qui sera porté à ma connaissance à l'occasion de son exercice.* » (…)

Art. R. 2321-5. – Les agents habilités de l'Agence nationale de la sécurité des systèmes d'information veillent à la protection des informations à caractère secret qui sont recueillies dans le cadre de leur mission prévue à l'article L. 2321-3 et dont la révélation est réprimée par les dispositions de l'article 226-13 du code pénal.

La transmission des informations mentionnées à l'article L. 2321-3 par les opérateurs de communications électroniques aux agents habilités de l'Agence nationale de la sécurité des systèmes d'information est effectuée selon des modalités assurant la sécurité, l'intégrité et le suivi de ces informations.

D'autre part, et comme précisé *supra*, le deuxième alinéa de cet article permet à ces mêmes agents de l'ANSSI, dans le cadre de l'exercice de ses prérogatives mentionnées à l'article L. 33-14 du CPCE, d'**obtenir des opérateurs de communications électroniques les données techniques** strictement nécessaires à l'analyse d'un évènement concernant une autorité publique, un OIV ou un OSE.

L'étude d'impact avance **trois raisons nécessitant une modernisation des dispositions de cet article** :

– les dispositions du deuxième alinéa de l'article L. 2321-3 ne sont applicables qu'aux autorités publiques, OIV et OSE, et non aux **opérateurs publics et privés qui peuvent participer à leurs systèmes d'information**. Or, selon l'étude d'impact, ces opérateurs « *représentent une porte d'entrée de prédilection pour les cyber-attaquants qui visent, par rebonds, les systèmes d'informations des entités plus critiques* » ;

– alors que les pratiques numériques évoluent, les **hébergeurs de données** sont de plus en plus victimes d'opérations malveillantes, sans pour autant être concernés par le périmètre du premier alinéa de l'article L. 2321-3 ;

– **l'assermentation des agents** est une garantie exigée pour les agents chargés de rechercher ou poursuivre des infractions pénales, ce qui n'est pas le cas des agents de l'ANSSI ciblés à cet article et complexifie inutilement leur mission.

Selon l'étude d'impact, cette dernière disposition s'applique en effet à la quasi-totalité des agents de la sous-direction des opérations de l'ANSSI, soit près de 200 agents sur un total de 280. Elle induit **des procédures lourdes d'assermentation pour les agents** et expose ces derniers lorsque les données exploitées ne permettent pas d'identifier une victime et nécessitent des recherches complémentaires à mener avec d'autres analystes n'étant pas soumis à cette obligation d'assermentation.

Votre rapporteure observe d'ailleurs que le caractère principalement judiciaire de l'assermentation a été rappelé par le Conseil d'État dans son rapport d'avril 2021 sur les pouvoirs d'enquête de l'administration. Il y est ainsi précisé que, « *à l'exception des agents de la DGCCRF, la loi prévoit que les agents habilités, commissionnés ou agréés doivent être assermentés pour pouvoir rechercher et constater des infractions pénales. La prestation de serment constitue l'engagement solennel de l'agent, généralement pris devant le président du tribunal judiciaire du ressort de son affectation, ce qui est une manifestation du caractère judiciaire des fonctions qu'il exerce, de bien remplir ses fonctions et de respecter les règles déontologiques inhérentes à leur exercice.* » (page 86).

B. LA SOLUTION PROPOSÉE : UN ÉLARGISSEMENT DES ACTEURS DU NUMÉRIQUE VISÉS PAR LE DISPOSITIF ET LA SUPPRESSION DE L'ASSERMENTATION DES AGENTS DE L'ANSSI

L'article L. 2321-3 du code de la défense est modifié à plusieurs titres par le présent article :

– le premier alinéa est modifié afin d'étendre le dispositif aux hébergeurs et de supprimer l'assermentation des agents de l'ANSSI (alinéa 11) ;

– le deuxième alinéa est complété afin d'élargir ses dispositions aux sous-traitants des autorités publiques, OIV et OSE (alinéa 13).

1. Un élargissement des dispositions de l'article aux hébergeurs et aux opérateurs publics et privés des autorités publiques, OIV et OSE

● Inclure les hébergeurs dans le périmètre de l'article

Le premier alinéa de l'article L. 2321-3 du code de la défense est modifié afin d'en **élargir le périmètre aux hébergeurs de données** (alinéa 11). Ceux-ci devront ainsi, pour les besoins de la sécurité des systèmes d'information des autorités publiques, OIV et OSE, transmettre à l'ANSSI l'identité, l'adresse postale et l'adresse électronique d'utilisateurs ou de détenteurs de systèmes d'information vulnérables, menacés ou attaqués, afin de les alerter sur la vulnérabilité ou l'atteinte de leur système.

Le décret n° 2021-1362 du 20 octobre 2021 relatif à la conservation des données permettant d'identifier toute personne ayant contribué à la création d'un contenu mis en ligne oblige déjà les hébergeurs à collecter ces données. L'étude d'impact précise que les données de connexion qui pourront être transmises à ce titre sont visées à l'article 2 de ce même décret [(1)].

En conséquence, les alinéas 14 à 16 réécrivent le dernier alinéa de l'article L. 2321-3 relatif aux modalités de compensation des surcoûts afin de prévoir que les prestations assurées par les hébergeurs sont compensées selon des modalités prévues en Conseil d'État.

● Étendre les dispositions de l'article aux opérateurs

Le deuxième alinéa de l'article L. 2321-3 est modifié afin d'**intégrer les sous-traitants des autorités publiques, OIV et OSE** (qualifiés dans le texte d'opérateurs publics ou privés participant aux systèmes d'information de ces entités) [(2)] dans le périmètre de cet alinéa. Il prévoit également que la durée de conservation maximale des données exploitées par l'ANSSI est de dix ans.

Cet élargissement du périmètre de l'article aux opérateurs s'inscrit en cohérence avec d'autres dispositions imposant déjà des règles de sécurité particulières aux sous-traitants dans le domaine de la défense des systèmes d'informations des OIV et OSE [(3)].

---

(1) 1° Les nom et prénom, la date et le lieu de naissance ou la raison sociale, ainsi que les nom et prénom, date et lieu de naissance de la personne agissant en son nom lorsque le compte est ouvert au nom d'une personne morale ; 2° La ou les adresses postales associées ; 3° La ou les adresses de courrier électronique de l'utilisateur et du ou des comptes associés le cas échéant ; 4° Le ou les numéros de téléphone.

(2) Cette terminologie reprend celle de l'article L. 1332-6-1 du code de la défense.

(3) Articles L. 1332-6-1 et R. 1332-41-2 du code de la défense s'agissant des OIV et articles 7 et 17 du décret n° 2018-384 relatif à la sécurité des réseaux et systèmes d'information des opérateurs de services essentiels et des fournisseurs de service numérique, s'agissant des OSE.

2. La suppression de la procédure d’assermentation des agents de l’ANSSI

L’alinéa 11 supprime la condition d’assermentation des agents de l’ANSSI prévue par l’article L. 2321-3. Les agents de l’ANSSI demeureront spécialement habilités, dans les conditions déjà précisées aux articles R. 2321-2 à R. 2321-3 et R. 2321-5.

L’étude d’impact précise que l’ANSSI fournira à l’ARCEP la liste des agents spécialement habilités, afin de lui permettre de s’assurer que seuls ces agents disposent effectivement d’un accès aux données qui leur sont communiquées au titre de cet article.

PERSONNES ENTENDUES

(par ordre chronologique)

- **Secrétariat général de la défense et de la sécurité nationale (SGDSN)**
  - — M. Benjamin Delannoy, conseiller juridique du secrétaire général
  - — Mme Julie Holveck, conseillère judiciaire du secrétaire général
  - — M. Gwénaël Jézéquel, conseiller « institutions » du secrétaire général
- **Agence nationale de la sécurité des systèmes d'information (ANSSI)**
  - — Général de brigade aérienne Emmanuel Naegelen, directeur général adjoint
  - — M. Mathieu Feuillet, sous-directeur « opérations »
- **Fédération Syntec, représentée par Numeum (*)**
  - — Mme Nolwenn Le Ster, présidente de la commission Cybersécurité de Numeum
  - — M. Paul Pastor, délégué aux affaires juridiques et à la Cybersécurité
  - — M. Clément Emine, délégué aux affaires publiques
- **Club de la sécurité de l'information français (Clusif)**
  - — M. Benoît Fuzeau, président
  - — M. Jean-Marc Grémy, vice-président
- **Club des experts de la sécurité de l'information et du numérique (CESIN)**
  - — Mme Mylène Jarossay, présidente
- **Conseil national des barreaux (*)**
  - — M. Philippe Baron, président de la commission Numérique
  - — M. Charles Renard, chargé de mission
- **Conférence des Bâtonniers (*)**
  - — M. Bruno Carriou, secrétaire général
- **Association française pour le nommage Internet en coopération (Afnic) (*)**
  - — M. Pierre Bonis, directeur général
  - — M. Lucien Castex, représentant pour les affaires publiques
- **Bouygues Telecom (*)**
  - — Mme Muriel Lévêque, directrice des obligations légales

— M. Corentin Durand, responsable du pôle affaires publiques

- **Free (*)**

  — Mme Ombeline Bartin, directrice des affaires publiques

  — M. Lucas Buthion, responsable des affaires publiques

- **SFR (*)**

  — Mme Marie Lhermelin, secrétaire générale adjointe et directrice des affaires publiques

- **Orange (*)**

  — Mme Carole Gay, responsable des relations institutionnelles

  — M. Stéphane Tibéri, directeur des Obligations légales

- **Fédération Française des Télécoms (*)**

  — M. Alexandre Galdin, directeur délégué aux études économiques, à l'environnement et à la sécurité

- **Autorité de régulation des communications électroniques, des postes et de la distribution de la presse (ARCEP)**

  — Mme Laure de la Raudière, présidente

- **Commission nationale de l'informatique et des libertés (CNIL)**

  — M. Bertrand Pailhès, directeur des technologies et de l'innovation

  — M. Thibaud Antignac, ingénieur expert

  — Mme Marion de Gasquet, adjointe à la cheffe du service des affaires régaliennes et des collectivités territoriales

- **Ligue des droits de l'Homme (*)**

  — Mme Maryse Artiguelong, membre du bureau national

- **Quadrature du Net (*)**

  — Mme Noémie Levain, juriste

  — M. Tom Barthe, sympathisant

- **Mme Brunessen Bertrand, professeure à l'université de Rennes**

- **Hexatrust**

  — M. Jean-Noël De Galzain, président

  — M. Jacques de La Rivière, vice-président

  — Mme Dorothée Decrop, déléguée générale

  — M. David Chassan, secrétaire général

  — M. Alain Garnier, membre du bureau

— M. Guillaume Faucher, consultant affaires publiques

- **OVHcloud (*)**

  — M. Julien Levrard, responsable de la sécurité des systèmes d'information

  — Mme Blandine Eggrickx, responsable des affaires publiques

- **Outscale (*)**

  — M. Édouard Camoin, vice-président résilience

(*) Ces représentants d'intérêts ont procédé à leur inscription sur le répertoire de la Haute Autorité pour la transparence de la vie publique, s'engageant ainsi dans une démarche de transparence et de respect du code de conduite établi par le Bureau de l'Assemblée nationale.