RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

FAQ

Mesures de la loi de programmation militaire 2024-2030 relatives à la sécurité informatique

Version du 29 avril 2024

En application du V de l'article L. 32-1 du code des postes et des communications électroniques, l'ANSSI a lancé le 29 janvier 2024 une consultation publique sur le projet de décret en Conseil d'Etat pris en application de la Loi n°2023-703 du 1er août 2023 relative à la programmation militaire (LPM) pour les années 2024 à 2030 et portant diverses dispositions intéressant la défense concernant les mesures relatives à la sécurité informatique.

Cette consultation publique s'adressait en premier lieu aux hébergeurs, aux fournisseurs d'accès à Internet (FAI), aux bureaux d'enregistrement de noms de domaine, aux éditeurs de logiciels et aux opérateurs de centres de données, qui sont les premiers concernés par ces nouveaux dispositifs.

Les entités suivantes ont répondu à la consultation publique :

- la société de conseil Cyberens ;
- l'entreprise Alcatel-Lucent ;
- l'organisation professionnelle de l'écosystème numérique en France, Numeum ;
- l'opérateur de centre de données Equinix ;
- la Fédération Française des Télécoms ;
- l'entreprise Huawei ;
- l'hébergeur et opérateur de communications électroniques OVHCloud ;
- l'entreprise Microsoft.

L'ANSSI a également reçu des contributions de particuliers.

Ce document vise à apporter des réponses à l'ensemble des questions adressées à l'ANSSI sur le projet de décret.

Table des matières

1 Article 67 LPM – Article L.2321-2-1 du code de la défense

1.1 Article 1er - Sous-section 1 : Mise en œuvre des dispositifs exploitant des marqueurs techniques ou permettant le recueil de données

1.1.1 Art. R.2321-1-1. Cahier des charges et phase de test des dispositifs.

Questions ou remarques reçues par l'ANSSI :

- *Une concertation pour l'élaboration du cahier des charges avec les personnes destinataires de la décision de mettre en œuvre les dispositifs exploitant des marqueurs techniques ou permettant le recueil de données semble indispensable et non facultative, ne serait-ce que dans un souci d'efficacité et d'adaptation à l'architecture du réseau ou système d'information concerné. De même une phase de test semble être impérative et non facultative.*

Comme elle l'avait fait lors de la mise en œuvre de dispositifs exploitant des marqueurs techniques dans le cadre de la LPM 2019-2023, l'ANSSI organisera une concertation pour l'élaboration d'un cahier des charges avec les personnes destinataires de la décision de mettre en œuvre les dispositifs exploitant des marqueurs techniques ou permettant le recueil de données. Ainsi, une étude amont sera bien réalisée avec les acteurs pour lesquels elle est nécessaire. En revanche, l'ANSSI considère que l'imposer serait contre-productif dans certaines situations, notamment pour les dispositifs déjà existants issus de la LPM 2019-2023.

1.1.2 Art. R. 2321-1-2.-I. Extension des dispositifs aux opérateurs de centres de données.

Questions ou remarques reçues par l'ANSSI :

- *Est-il possible de clarifier l'intention du législateur au regard des opérateurs de centre de données, sur ce point précis : « Art. R. 2321-1-2.-I. – La décision de mettre en œuvre les dispositifs mentionnés au 1° de l'article L. 2321-2-1 est notifiée par l'Agence nationale de la sécurité des systèmes d'information à l'opérateur de communications électroniques, à la personne mentionnée au 1 ou 2 du I de l'article 6 de la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique ou à l'opérateur de centre de données, et communiquée sans délai à l'Autorité de*

régulation des communications électroniques, des postes et de la distribution de la presse. »

L'ANSSI observe régulièrement l'utilisation par des acteurs malveillants de serveurs hébergés par des opérateurs de centres de données - au sens de l'article L. 32 du code des postes et des communications électroniques (CPCE) - situés sur le territoire national. Ces équipements, parfois loués par des entités étrangères fournissant des services d'hébergement, n'étaient pas soumis au cadre légal de la LPM 2019-2023. L'application de l'article L. 2321-2-1 aux centres de données permettra à l'ANSSI d'améliorer sa capacité à prémunir les autorités publiques et opérateurs régulés des menaces utilisant ce type d'infrastructure.

1.1.3 Art. R. 2321-1-2.-I. Commentaires relatifs aux interruptions de service ou instabilités générées par les dispositifs.

Questions ou remarques reçues par l'ANSSI :

- *Un fournisseur se doit contractuellement d'assurer la continuité d'activité de tous les services à ses clients, sous risque de pénalités financières. Cette même exigence de continuité d'activité est aussi réglementaire.*
- *L'introduction de dispositifs dont les caractéristiques techniques sont inconnues, même en prévoyant une phase de test préliminaire, crée des risques d'instabilité de service et pourrait invalider les mesures existantes d'atténuation des risques*

L'application de l'article L. 2321-2-1 du code de la défense, notamment pour le recueil de données sur un équipement, peut engendrer dans certains cas des interruptions de service mineures. Toutefois, préalablement à l'usage du dispositif, les risques d'interruption de service seront systématiquement appréciés en concertation avec l'entité concernée. En outre, la mise en œuvre sera, dans la mesure du possible, réalisée par cette dernière de sorte à limiter les risques d'interruption ou d'instabilité.

1.1.4 Art. R.2321-1-4. Définition des marqueurs techniques.

Questions ou remarques reçues par l'ANSSI :

- *Le projet de décret décrit à l'article R. 2321-1-4 du code de la défense les « marqueurs techniques » comme des éléments techniques caractéristiques d'un mode opératoire d'attaque informatique permettant de « détecter une activité malveillante ou d'identifier une menace susceptible d'affecter*

la sécurité des systèmes d'information ». Cette mention apparait trop large et trop sujette à interprétation pour permettre d'identifier de manière objective quels sont les éléments visés par l'article 67 de la LPM. Le périmètre de ces marqueurs mériterait par conséquent d'être précisé : à cette fin, il pourrait être indiqué dans le décret que les activités malveillantes et menaces visées sont celles qui sont susceptibles de porter atteinte à la sécurité des systèmes d'information des autorités publiques.

- *Le passage « une menace susceptible d'affecter la sécurité des systèmes d'information » de l'article R. 2321-1-4 semble large et susceptible d'être interprété. Afin de le préciser, et en cohérence avec les missions de l'ANSSI, il est suggéré d'ajouter « une menace susceptible d'affecter la sécurité des systèmes d'information opérés par l'État français et ses administrations ».*

La définition des marqueurs techniques proposée dans l'article R.2321-1-4 est une définition générale, qui permet de clarifier la nature de cet élément technique. En revanche, l'article L.2321-2-1 du code de la défense fixe le cadre d'emploi de ce type d'élément technique, qui ne peut être mis en œuvre que pour des finalités très précises. En particulier, l'ANSSI ne peut y avoir recours que si elle démontre à l'ARCEP l'existence d'une menace susceptible de toucher des autorités publiques, des opérateurs d'importance vitale et des opérateurs de services essentiels ou de porter atteinte à la sécurité nationale. L'ARCEP, qui contrôle cette justification, peut demander la suspension des mesures à l'ANSSI, voire saisir le Conseil d'Etat si l'ANSSI ne se conforme pas à ses injonctions.

1.1.5 Art. R. 2321-1-5. Catégories de données recueillies, proportionnalité du dispositif et mise en œuvre par les acteurs concernés.

Questions ou remarques reçues par l'ANSSI :

- *Parmi les informations et catégories de données listées par le projet d'article R. 2321-1-5 comme pouvant faire l'objet d'un recueil au titre de l'article 67 de la LPM, figurent les « communications électroniques ». L'article L. 32 du code des postes et des communications électroniques définit ces dernières comme les « émissions, transmissions de ou réceptions de signes, de signaux, d'écrits, d'images ou de sons, par voie électromagnétique ». Le choix de cette qualification interroge, car semble très large et peu adapté pour désigner les données visées par l'article 67 de la LPM. Il est suggéré qu'une précision des données concernées soit*

apportée pour garantir la proportionnalité du dispositif et garantir sa bonne mise en œuvre auprès des acteurs concernés.

- *Les mesures prévues par l'article 67 de la LPM pourraient requérir de donner accès aux agents de l'ANSSI aux clés de chiffrement des données afin de pouvoir prendre connaissance des données collectées. Cet élément, à l'impact potentiellement important sur la confiance des utilisateurs, devrait être mieux pris en compte par le projet de décret.*
- *Les informations et les catégories de données utiles à la prévention et à la caractérisation des menaces concernent :*
    1. *Les communications électroniques liées aux activités de l'attaquant ;*
    2. *Les traces d'activité système liées à l'attaquant.*

  Un hébergeur ou un centre de données, selon son contexte d'exploitation, ne dispose pas nécessairement d'un compte d'accès système sur les machines. La mise en œuvre du 2° si celui-ci correspond à la récupération des journaux hébergés sur le système pourrait ne pas être réalisable.
- *La proportionnalité de cette mesure au regard de l'objectif poursuivi soulève une inquiétude. La disposition pourrait être précisée afin d'éviter les différences d'interprétation. En l'état, le placement de dispositifs utilisant des marqueurs techniques ou permettant la collecte de données sur le réseau ou les systèmes d'information est préoccupant pour plusieurs raisons :*
    - *la demande ne cible pas de comptes ou d'identifiants spécifiques, mais recueille potentiellement des données sur des personnes et des organisations au-delà des clients que la loi a l'intention d'aider ;*
    - *les fournisseurs n'ont pas la capacité de filtrer les données fournies (plus précisément, de ne fournir que les données spécifiques associées à la cible de la demande gouvernementale) ;*
    - *tel que rédigé, le projet de décret présente des contradictions potentielles avec les pratiques existantes en matière de données au sein de certains hébergeurs, notamment sur les questions de transparence : la possibilité pour les gouvernements d'obtenir des données directement auprès des clients lorsque cela est possible, et la possibilité d'exposer des clés de chiffrement ou des informations d'identification.*

Si les dispositifs prévus par l'article L. 2321-2-1 du code de la défense sont effectivement étendus en matière d'acteurs concernés et de types de données, ils sont néanmoins réservés à des équipements utilisés à des fins malveillantes par un attaquant, ce qui en encadre strictement la portée.

Les recueils de données sont systématiquement ciblés au plus près de la menace afin de limiter au maximum la présence de données issues de tiers, en excluant toute collecte large de données. Dans tous les cas, au plus tard à l'issue de la phase de qualification de trois mois prévue par le décret et sous le contrôle de l'ARCEP, seules les données dont il est établi qu'elles sont directement utiles à la prévention et à la caractérisation des menaces peuvent être conservées, comme l'indique l'article R. 2321-1-5 *(Il est à noter que conformément à l'avis de la CNIL, le projet de décret a été ajusté pour faire référence aux données directement utiles à la prévention et à la caractérisation des menaces, comme défini dans la loi.)*

En réponse à plusieurs contributions relatives à l'article R.2321-1-5-2°, une reformulation a été prise en compte dans le projet de décret : *« Les traces d'activité système liées à l'attaquant »* est remplacé par *« les données système, liées à l'attaquant »*. Cette modification vise à clarifier les données visées par le recueil, qui inclut notamment les données liées à l'attaquant présentes en mémoire.

Si le déchiffrement d'une partie du trafic réseau est techniquement possible au moyen des dispositifs prévus par l'article L. 2321-2-1 lorsque des secrets de chiffrement sont présents sur l'équipement, ces possibilités sont extrêmement limitées. Par exemple, pour la navigation web, du fait de l'usage de mécanismes cryptographiques de type *Perfect Forward Secrecy,* une telle opération nécessiterait de collecter la mémoire vive de l'équipement à des fréquences très élevées, ce qui ne correspond pas à l'usage prévu. En particulier, dans les débats au Parlement, le Gouvernement a évoqué une cinquantaine de collectes de mémoire par an.

Enfin, la proportionnalité du dispositif a fait l'objet d'un avis du Conseil d'Etat (n° 406858 sur le projet de loi relatif à la programmation militaire pour les années 2024 à 2030 et portant diverses dispositions intéressant la défense) et repose notamment sur les garanties accrues que l'ANSSI apporte dans la mise en œuvre du dispositif et le contrôle de l'ARCEP, à savoir :

- le ciblage préalable de la machine compromise faisant l'objet du recueil de données ;
- le contrôle de l'application de ces nouvelles mesures par l'ARCEP, dont la justification de la menace, notamment au moyen d'un avis conforme pour les dispositifs permettant le recueil des données ;

- la destruction sous un jour ouvré des données, dès lors qu'il est établi qu'elles ne sont pas directement utiles à la prévention et à la caractérisation des menaces ;
- la durée de conservation des données directement utiles à la prévention et à la caractérisation des menaces a été réduite à 2 ans.

1.1.6 Art. R. 2321-1-5 2. Destruction des données non directement utiles à la prévention et à la caractérisation des menaces.

Questions ou remarques reçues par l'ANSSI :

- *Concernant les données non conservées et détruites au bout d'une journée, il n'est pas fait mention de PV de 'destruction' (ou de constat ou certificat) ni de contrôle de la destruction effective.*

Dans le cadre de l'article L. 2321-2-1 du code de la défense, la destruction des données qui ne sont pas directement utiles à la prévention et à la caractérisation des menaces est effectuée sous le contrôle de l'ARCEP. La CNIL dispose également d'un pouvoir de contrôle sur les traitements de données utilisés par l'ANSSI dans ce cadre.

L'article R. 2321-1-15 dans sa dernière version précise que la traçabilité des accès et modifications (incluant la suppression) des données doit être assurée et auditable. En effet, certaines de ces actions devant se faire au fil des avancées des investigations (par exemple la destruction des données qui ne sont pas directement utiles à la prévention et à la caractérisation des menaces), le formalisme associé doit être pragmatique.

2 Article 67 LPM – Article L.33-14 al.2 du CPCE

2.1 Article 2 – Modifications du CPCE

2.1.1 Art. R.9-12-2. Catégories de marqueurs et modalités de mise en œuvre.

Questions ou remarques reçues par l'ANSSI :

- *L'article 2, alinéa II.2 de ce projet de décret stipule dans le nouveau deuxième alinéa de l'article R.9-12.2 du Code des Postes et Communications Electroniques l'utilisation d'un marqueur technique à la demande exclusive de l'ANSSI. L'agence peut-elle préciser quel marqueur précis est envisagé ?*

Les marqueurs techniques qui peuvent être mis en œuvre dans le cadre de l'article L. 33-14 al.2 du code des postes et des communications électroniques (CPCE) dépendent du type de menace, et de la capacité des dispositifs de détection de l'opérateur de communications électroniques.

Un marqueur technique est une signature qui permet de détecter la présence de l'attaquant, notamment dans le trafic réseau. Il peut s'agir d'une simple adresse IP ou d'un nom de domaine contrôlés par l'attaquant, ou encore d'un motif dans le trafic réseau qui est caractéristique d'un code malveillant de l'attaquant. La notion de marqueur technique est une extension de celle d'indicateur de compromission, qui permet d'inclure des signatures plus complexes (notamment sur le trafic réseau issu de codes malveillants).

Le travail d'étude amont permettra de déterminer les types de marqueurs adaptés aux dispositifs mis en œuvre par les OCE. Ces marqueurs seront transmis dans un format structuré aux OCE préalablement identifiés comme pertinents pour leur exploitation, accompagnés d'une date limite d'exploitation.

3 Article 64 LPM – Article L.2321-2-3 Code de la défense

3.1 Article 1er - Sous-section 2 : Blocage, enregistrement, suspension, transfert et redirection de nom de domaine

3.1.1 Art. R. 2321-1-8. Délai de mise en œuvre des mesures.

Questions ou remarques reçues par l'ANSSI :

- *Qu'est-il entendu par « mise en œuvre » ? La mesure doit-elle être mise en place ou effective ? Certaines mesures peuvent demander du temps afin d'être effectives en raison de la propagation DNS, raison pour laquelle une précision pourrait être nécessaire dans le décret.*
- *Le projet de décret prévoit que les demandes émises par l'ANSSI comprennent « le délai imparti pour [la] mise en œuvre [de la mesure] ». Cette rédaction ne présente pas de difficulté particulière. Toutefois, même en lançant les mesures requises dans les délais impartis, ces dernières peuvent parfois nécessiter un temps supplémentaire pour être pleinement effectives (parfois vingt-quatre heures). L'ANSSI devra par conséquent tenir compte de ce temps de propagation lorsqu'elle déterminera dans ses demandes le délai donné au fournisseur de services.*

Pour l'application des mesures prévues par l'article L. 2321-2-3 du code de la défense, la demande est implicitement considérée comme effective lorsqu'elle a été mise en place sur les résolveurs DNS du fournisseur ou sur le serveur DNS autoritaire dans le cas des bureaux ou de l'office d'enregistrement. Le délai de mise en œuvre fixé par l'ANSSI, qui ne peut être inférieur à deux jours ouvrés, n'inclut pas par défaut le temps de propagation de la modification.

3.1.2 Art. R. 2321-1-8. Cas de l'expiration des noms de domaine.

Questions ou remarques reçues par l'ANSSI :

- *Dans le cas où un fournisseur de service reçoit une demande de redirection et qu'au cours de celle-ci le nom de domaine expire, quels procédés pourraient être mis en œuvre pour assurer le renouvellement ? Est-ce-que la mesure prend fin automatiquement ?*
- *Pour toute demande de redirection de nom de domaine, une procédure spécifique devrait être prévue pour les cas où le nom de domaine aurait dû être renouvelé par le client auprès de son fournisseur.*

Lorsqu'une demande est effectuée auprès d'un bureau d'enregistrement pour un nom de domaine expiré qui n'a pas été renouvelé par son propriétaire, l'ANSSI demandera l'enregistrement du nom de domaine en application de l'article L. 2321-2-3 du code de la défense.

3.1.3 Art. R. 2321-1-8. Modalités de mise en œuvre : moyens de communication, format des données, informations techniques et obligation de confidentialité

Questions ou remarques reçues par l'ANSSI :

- *Le recours à un courrier pour les demandes de l'ANSSI est à éviter dans un souci de sécurité, de confidentialité et de rapidité du traitement de la demande.*
- *Il est souhaitable que l'ANSSI gère directement la durée du dispositif et ne demande pas aux personnes mentionnées de prendre la responsabilité d'arrêter le dispositif. Il est souhaité que l'ANSSI communique à échéance régulière une liste des noms de domaine à bloquer.*
- *Il n'est pas nécessaire de préciser le délai de mise en œuvre, car la loi prévoit déjà une mise en œuvre sous 2 jours.*
- *« Les personnes mentionnées au 1 mettent en œuvre par tout moyen tenant compte de la menace et de l'urgence, les mesures demandées et en tiennent informée sans délai l'Agence précitée en lui communiquant les informations techniques relatives à leur mise en œuvre. Elles préservent la confidentialité de toutes les données qui leur sont confiées dans ce cadre. » : ici, quelles informations techniques sont visées ?*
- *Le projet d'article R. 2321-1-8 prévoit que les entités destinataires des demandes de l'ANSSI tiennent cette dernière informée de la mise en œuvre des mesures par la communication d'informations techniques et qu'elles « préservent la confidentialité de toutes les données qui leur sont confiées dans ce cadre ». Cette mention semble faire peser une obligation de confidentialité sur le titulaire d'un nom de domaine, sans que la portée et le champ d'application de cette obligation ne soient clarifiés.*
- *Les moyens de mise en œuvre des mesures devraient être fixés par les fournisseurs de résolveurs DNS.*

Les modalités de mise en œuvre de cette mesure seront déterminées en concertation avec les fournisseurs de résolveurs DNS, notamment afin de s'adapter aux éventuelles capacités déjà existantes. À ce titre, l'ANSSI est disposée à demander explicitement le retrait d'une mesure de blocage ou de redirection plutôt que d'indiquer la durée de cette dernière lors de la demande initiale. Le délai de mise en œuvre, qui ne peut être inférieur à deux jours ouvrés d'après la loi, pourra également faire l'objet d'une concertation préalable avec le fournisseur.

Les demandes formulées par l'ANSSI auprès des fournisseurs de résolveurs DNS, bureaux ou office d'enregistrement seront effectuées par des moyens de communication sécurisés, préalablement convenus avec ces derniers. La demande de confidentialité prévue à l'article R. 2321-1-8 vise les données communiquées par l'ANSSI.

Enfin, les informations techniques attendues par l'ANSSI en réponse à une demande formulée au titre de l'article L. 2321-2-3 peuvent varier selon chaque demande. Il s'agit principalement d'informations relatives :

- pour les fournisseurs de résolveurs DNS, au périmètre d'application et à la mesure technique mise en œuvre ;
- pour les bureaux d'enregistrement et l'office d'enregistrement, la liste des enregistrements DNS ayant fait l'objet d'une modification et les métadonnées d'enregistrement du nom de domaine.

3.1.4 Art. R. 2321-1-8 : Périmètre d'application de la mesure et sur les critères d'appréciation relatifs à la menace.

Questions ou remarques reçues par l'ANSSI :

- *Des précisions pourraient être formulées sur l'article 64 de la LPM, tant sur son champ d'application (application aux registrars étrangers, à la messagerie, etc.), que sur les critères d'appréciation de l'ANSSI en matière de menace portée à la sécurité nationale.*

La mesure s'applique aux fournisseurs de système de résolution de noms de domaine au sens de l'article L. 2321-3-1 du code de la défense, à savoir les personnes mettant à disposition un service permettant la traduction d'un nom de domaine en un numéro unique identifiant un appareil connecté à Internet, à l'office d'enregistrement défini par l'article L. 45 du CPCE (l'Association française pour le nommage Internet en coopération) ou à un bureau

d’enregistrement établi sur le sol français au sens de l’article L. 45-4 du CPCE. Enfin, l’article L. 2321-2-3 du code de la défense s’applique uniquement aux menaces susceptibles de porter atteinte à la défense et à la sécurité nationale comme indiqué dans la loi.

4 Article 65 LPM - Article L.2321-3-1 Code de la défense

4.1 Article 1er - Sous-section 4 : Communication de données

4.1.1 Art. R.2321-1-12 & R.2321-1-13. Mise en œuvre : délais et notifications de décision.

Questions ou remarques reçues par l'ANSSI :

- *Le projet de décret prévoit que la décision de l'ANSSI concernant la communication de données doit tenir compte des contraintes techniques du fournisseur de système de résolution de noms de domaine. Cette démarche est positive et essentielle pour adapter chaque demande aux impératifs auxquels font face ces fournisseurs, en fonction de l'ampleur du volume et de la typologie des données attendues. La communication des données ne prend-elle effet qu'à compter de la notification de la décision de l'ANSSI ? Il semble nécessaire de préciser explicitement dans le projet de décret que celle-ci n'a pas d'effet rétroactif.*
- *La communication des données ne prend-elle effet qu'à compter de la notification de la décision de l'ANSSI au fournisseur de services ? Il semble nécessaire de préciser explicitement dans le projet de décret que celle-ci n'a pas d'effet rétroactif. La décision devrait aussi préciser le temps de conservation des logs.*
- *Une concertation étroite avec les entités concernées par la mesure semble indispensable.*

La communication des données prévue par l'article L. 2321-3-1 n'a pas d'effet rétroactif, et ne prend effet qu'à compter de la notification de décision de l'ANSSI auprès du fournisseur. Par ailleurs, les données visées se limitent aux enregistrements DNS déjà présents dans les données de cache, à l'exclusion de toute journalisation complémentaire. En particulier, les données techniques permettant d'identifier la source de la connexion ou relatives aux équipements utilisés (par exemple l'adresse IP ayant émis la requête DNS) ne doivent pas être communiquées à l'ANSSI.

La mise en œuvre de cette mesure sera effectuée en concertation étroite avec les fournisseurs de résolveurs DNS, avec l'objectif de s'appuyer sur les moyens existants.

4.1.2 Art. R.2321-1-12 2°. Horodatage des enregistrements.

Questions ou remarques reçues par l'ANSSI :

- *Techniquement, un enregistrement DNS ne contenant pas de date, il est seulement possible de transmettre "l'horodatage de l'export des enregistrements DNS".*

Pour l'application de l'article L. 2321-3-1, l'horodatage s'applique à la copie, ou à « l'export » des enregistrements DNS. L'ANSSI devra également être informée de la fréquence de ces copies, ainsi que du schéma de données permettant le suivi des évolutions techniques du fournisseur de résolveur DNS.

5 Article 66 LPM - Article L.2321-4-1 Code de la défense

5.1 Article 1er - Sous-section 6 : Signalement de vulnérabilités et incidents par les éditeurs de logiciels

5.1.1 Art. R.2321-1-16 I. Notion de « vulnérabilité significative », seuils et normes applicables.

Questions ou remarques reçues par l'ANSSI :

- *L'absence de seuil rend plus difficile et probablement variable (d'un éditeur à l'autre) l'évaluation du caractère « significatif » des vulnérabilité. Des seuils devraient être donnés pour chaque critère (nombre d'utilisateurs concernés, nombre de produits intégrant le produit affecté, […] existence de code d'exploitation)*
- *Le niveau « Significatif » pour déclencher le processus de notification en temps contraint des vulnérabilités devrait être clarifié. Il semble plus pertinent d'associer un score de sévérité contextualisé, basé sur un calcul type reconnu par la communauté cyber.*
- *Quelle norme doit être utilisée pour apprécier précisément le caractère « significatif » pour les incidents et les vulnérabilités prévues à l'article R. 2321-1-16.I ? Sera-t-il défini selon les pratiques et standards internationaux communément admis en référence à l'état de l'art ? L'ANSSI fournira-t-elle des indications supplémentaires sur la détermination de l'incident significatif et de la vulnérabilité ?*

Le décret d'application de l'article L. 2321-4-1 prévoit une liste non exhaustive de critères à prendre en compte dans l'évaluation du caractère significatif d'une vulnérabilité. Une marge d'appréciation est volontairement ménagée à l'éditeur sur ce point, car ce dernier est le plus à même d'évaluer la vulnérabilité. Il dispose en effet de la meilleure connaissance des utilisateurs, de l'environnement et de l'utilisation du produit affecté.

La liste de critères permettant d'apprécier le caractère significatif d'une vulnérabilité s'appuie bien entendu sur les standards internationaux et l'état de l'art. En effet, la majeure partie des critères proposés est présente dans le score CVSS[1] *(Common Vulnerability Scoring System)*, qui est la référence

[1] voir https://www.first.org/cvss/v4.0/specification-document pour les détails sur ce standard établi par le réseau de coopération international FIRST

internationale pour la mesure de l'impact technique d'une vulnérabilité. Cette liste est complétée, notamment sur la prise en compte du type de produit, par des critères s'appuyant sur un travail de l'université de Carnegie Mellon[2].

Enfin, le signalement de vulnérabilité est parfois effectué par l'ANSSI aux éditeurs de logiciels, par exemple en application de l'article L. 2321-4 du code de la défense. Dans ce cas particulier, l'ANSSI peut disposer d'informations suggérant le caractère significatif de la vulnérabilité, et ainsi imposer à l'éditeur un délai maximal pour la qualification de cette dernière. À ce titre, la phrase suivante a été ajoutée à l'article R. 2321-1-16, II : « Lorsque la vulnérabilité ou l'incident a été notifié par l'autorité nationale de sécurité des systèmes d'information à l'éditeur de logiciel ce dernier dispose d'un délai fixé par cette autorité pour apprécier son caractère significatif. Ce délai ne pourra être inférieur à 48 heures. »

5.1.2 Art. R.2321-1-16 II. Délai de notification.

Questions ou remarques reçues par l'ANSSI :

- *Quel est la définition claire du moment où le décompte des 24h commence ? Est-ce au moment où l'entité concernée est informée (par exemple réception d'une alerte en provenance d'un CERT, détection d'une vulnérabilité lors de campagne de tests d'intrusion, information de son fournisseur ou sous-traitant dans le cas des produits qui ne sont pas développés par l'éditeur de logiciel, autre ?). Ces 24h s'entendent-elles 365 jours par an (incluant jours fériés, week-end…) ?*
- *Compte tenu du délai extrêmement court (24h) demandé pour analyser une vulnérabilité (processus non automatisable, car nécessitant une analyse très approfondie du contexte dans lequel une vulnérabilité peut, ou non, avoir un impact), il est proposé d'étendre ce délai à 72h. Permettre un délai plus important aurait comme impact immédiat une réduction très importante de potentiels faux positifs, rendant ainsi le processus de traitement des notifications par l'utilisateur final beaucoup plus efficace.*

L'éditeur doit notifier la vulnérabilité ou l'incident significatif à l'ANSSI lorsqu'il est en mesure d'établir son caractère significatif, c'est-à-dire lorsqu'il dispose des éléments et connaissances permettant d'établir ce caractère significatif au-

[2] https://insights.sei.cmu.edu/documents/606/2021_019_001_653461.pdf

delà du doute raisonnable. Ainsi, le travail de qualification de la vulnérabilité est effectué préalablement à la notification à l'ANSSI.

La formulation initiale du projet de décret (« dans un délai de vingt-quatre heures après en avoir eu connaissance ») étant ambiguë, elle a été supprimée. Il est ainsi entendu que l'éditeur doit notifier l'ANSSI dès qu'il a établi le caractère significatif de la vulnérabilité ou de l'incident.

Enfin, l'origine de la découverte de la vulnérabilité n'a pas d'incidence sur la notification. Toutefois, le délai maximal pour la qualification du caractère significatif de la vulnérabilité (qui ne peut être inférieur à 48 heures) est fixé par l'ANSSI lorsque l'Agence est à l'origine du signalement.

5.1.3 Art. R.2321-1-16 II. Source de signalement et veille sur les vulnérabilités.

Questions ou remarques reçues par l'ANSSI :

- *Pour ce qui concerne les sources acceptables pour les vulnérabilités, existera-t-il une liste officielle (mentionnant peut-être les différents CERT, les notifications de l'ANSSI, autre), ou est-ce laissé à la discrétion de l'entité concernée ? L'utilisation d'un CERT unique est-elle suffisante, ou doit-on la compléter par des abonnements à d'autres sources (par exemple des communautés de développeurs dédiées : Debian, OpenSSL, Rocky Linux, NodeJS, npm…)*

L'article L. 2321-4-1 s'applique indifféremment de la manière dont l'éditeur a eu connaissance de la vulnérabilité (à l'exclusion du délai de qualification, qui est fixé par l'ANSSI lorsque l'Agence est à l'origine du signalement). Pour les éditeurs de produits intégrant des composants tiers, l'ANSSI recommande d'appliquer les bonnes pratiques de gestion des vulnérabilités et d'effectuer une veille technique sur les vulnérabilités affectant chacun de ces composants.

5.1.4 Art. R.2321-1-16 II et III. Modalités de déclaration à l'ANSSI.

Questions ou remarques reçues par l'ANSSI :

- *Si les informations demandées pour la déclaration ne peuvent pas être fournies au moment de la déclaration, peuvent-elles être fournies de manière différée ou échelonnée ? Dans l'affirmative, quel serait le délai requis ? L'ANSSI doit préciser les informations spécifiques à fournir pour la déclaration. Seront-elles à préciser directement dans le*

formulaire de déclaration ? Est-ce que les critères listés au R. 2123-1-16.I peuvent suffire pour se conformer à l'obligation de signalement ?

- *Dans le projet de décret, la nature des informations à déclarer par les éditeurs de logiciels n'a pas été clarifiée. Par exemple, le formulaire de déclaration n'est pas disponible et il n'est pas clair quels renseignements le gouvernement peut demander après un premier signalement ;*
- *Sur quelle plateforme les déclarations et notifications auprès de l'ANSSI doivent-elles se faire ?*
- *Le décret devrait préciser que le formulaire soit envoyé par un moyen sécurisé.*

Pour l'application de l'article L. 2321-4-1 du code de la défense, un formulaire de déclaration de vulnérabilité et d'incident sera mis en ligne par l'ANSSI à destination des éditeurs. Ce formulaire indiquera clairement les informations à fournir à l'ANSSI, et pourra être modifié par l'ANSSI en fonction de l'évolution des pratiques et des standards. Un moyen de communication sécurisé sera fourni aux éditeurs pour la transmission du signalement.

Conformément aux bonnes pratiques de divulgation responsable de vulnérabilités (CVD), les échanges entre l'éditeur et l'ANSSI peuvent permettre de compléter des éventuels éléments manquants à la déclaration.

5.1.5 Art. R.2321-1-16 II. Vulnérabilités affectant les logiciels « *Software-as-a-Service* » *(SaaS)*

Questions ou remarques reçues par l'ANSSI :

- *L'obligation de notification des vulnérabilités s'applique-t-elle uniquement aux vulnérabilités affectant les produits logiciels déployés « on-premise » ou également aux services SaaS ?*
- *L'obligation de notification des incidents s'applique-t-elle aux services SaaS et/ou aux systèmes d'information utilisés dans le cadre du développement des produits ?*

L'obligation de notification porte sur les vulnérabilités affectant des produits et ce quel que soit leur mode de distribution *(Software-as-a-Service (SaaS), on-premise…)*. Elle ne s'applique cependant pas aux services : lorsqu'une vulnérabilité significative affecte un produit distribué en SaaS, l'obligation de

signalement s'applique à l'éditeur du produit et non au gestionnaire du service SaaS.

Les environnements de développement sont concernés par l'obligation de déclaration d'un incident, dans la mesure où la compromission de l'environnement de développement peut affecter la sécurité du produit (par exemple, par une compromission avant sa distribution). L'obligation de déclaration de vulnérabilités ne s'applique qu'aux produits développés par l'éditeur, et n'est donc pas applicable aux produits utilisés pour les développer.

5.1.6 Art. R.2321-1-17 I. Délai minimal de communication aux clients.

Questions ou remarques reçues par l'ANSSI :

- *Quel est l'objectif du délai minimal de 10 jours pour prévenir les utilisateurs ?*
- *Le délai pour communiquer aux clients devrait être établi en accord avec l'éditeur.*

Pour l'application de l'article L. 2321-4-1 du code de la défense, l'imposition par l'ANSSI d'un délai à l'éditeur pour communiquer auprès des utilisateurs vise à établir une date limite à la communication.

Suivant les bonnes pratiques de CVD, un plan d'action sera en effet en priorité établi avec l'éditeur pour le traitement de la vulnérabilité. Cette bonne pratique permet, d'une part, de limiter la fenêtre d'exposition du produit et, d'autre part, de laisser le temps nécessaire à l'éditeur de développer un correctif ou d'élaborer des mesures de contournement ainsi que de préparer une communication adaptée.

Dans le cas où un éditeur n'aurait pas respecté le plan d'action convenu ni le délai établi, l'ANSSI sera alors en mesure d'enjoindre à l'éditeur de communiquer la vulnérabilité aux utilisateurs dans un délai déterminé. Le décret prévoit une limite minimale de dix jours ouvrables, qui permet d'assurer à l'éditeur un délai raisonnable pour avertir ses clients.

Le délai peut toutefois être inférieur à dix jours en cas de risque pour la défense et la sécurité nationale requérant une information des utilisateurs sans délai.

5.1.7 Art. R.2321-1-17 II. Définition des utilisateurs du produit.

Questions ou remarques reçues par l'ANSSI :

- *Comment doit être interprété le mot « utilisateur » dans la procédure de notification visée par l'article R.2321-1-17 ? Dans le cas d'un modèle de distribution indirect des produits, l'utilisateur final n'est pas connu, seulement le revendeur qui installe le produit chez l'utilisateur final.*
- *A quoi correspond le terme « utilisateur » mentionné à l'article R. 2321-1-17.I ? Faut-il comprendre l'utilisateur C (consommateur final) ou l'utilisateur B (par exemple un opérateur de communications électroniques) ?*

Les guides de bonnes pratiques de divulgation responsable de vulnérabilités (notamment les guides établis par l'organisme de coopération internationale FIRST[3] ou le CERT/CC[4]) recommandent aux éditeurs d'informer la chaîne de distribution avale (ou « *downstream* »), c'est-à-dire les intégrateurs, distributeurs et utilisateurs finaux.

L'ANSSI recommande d'appliquer les recommandations de ces guides et d'interpréter "utilisateur" comme couvrant l'ensemble de la chaîne de distribution d'un produit. Pour atteindre cet objectif, un plan de communication sera établi conjointement avec l'éditeur. Il pourra prévoir une communication publique par l'éditeur, ou une communication de l'éditeur à ses intégrateurs et revendeurs leur enjoignant d'informer leurs propres clients (dans la mesure du possible, cela devra être intégré par l'éditeur dans les contrats avec les intégrateurs et revendeurs).

5.1.8 Art. R.2321-1-17 II & R.2321-1-19 - Vulnérabilités pour lesquelles il n'existe pas de correctif disponible et produits non maintenus.

Questions ou remarques reçues par l'ANSSI :

- *Il est délicat pour des raisons de sécurité de communiquer largement sur une vulnérabilité qui n'a pas encore été remédiée. En effet, une telle communication à tous les utilisateurs risque d'exposer un peu plus le logiciel aux actions malveillantes. Si le dialogue entre l'ANSSI et les éditeurs de logiciels constitue un gage de fluidité et d'agilité dans le traitement des vulnérabilités, il serait pertinent de préciser dans le*

[3] Guidelines and Practices for Multi-Party Vulnerability Coordination and Disclosure, 2020, FIRST, https://www.first.org/global/sigs/vulnerability-coordination/multiparty/guidelines-v1.1
[4] The CERT Guide to Coordinated Vulnerability Disclosure, 2019, CERT/CC, https://vuls.cert.org/confluence/display/CVD

décret que la communication aux utilisateurs s'applique aux seules vulnérabilités pour lesquelles un correctif est disponible, et une fois que ledit correctif a été développé.

- *L'industrie s'est fermement opposée au signalement des vulnérabilités non atténuées dans le cadre du Cyber Resilience Act en raison d'inquiétudes qui se retrouvent également dans le projet de décret, notamment une plus grande communication sur les vulnérabilités non atténuées augmente les chances qu'un acteur malveillant obtienne les informations sur les vulnérabilités et les exploite.*
- *Rendre obligatoire le signalement des vulnérabilités et des incidents sans clarifier l'étendue des produits couverts crée une ambiguïté inutile. Par exemple, le projet de décret ne contient pas de limite de temps ni de portée du cycle de vie du produit. Pour plus de clarté, le décret ne devrait pas s'appliquer aux produits qui ne sont plus pris en charge par les éditeurs. Les révisions du décret devraient résoudre ce problème.*

L'ANSSI applique les bonnes pratiques de divulgation responsable de vulnérabilités. À ce titre, le plan d'action de l'éditeur, établi conjointement avec l'ANSSI, doit prévoir des délais de communication permettant de limiter la fenêtre d'exposition tout en laissant le temps nécessaire pour développer un correctif ou élaborer des mesures de contournement. L'article R. 2321-1-17 du projet de décret a ainsi été modifié pour inclure la mention « Après analyse conjointe de la vulnérabilité ou de l'incident [...] avec l'éditeur ».

La communication sur une vulnérabilité non corrigée n'est pas une pratique privilégiée, mais peut, dans de rares cas, être préférable à l'absence de communication. Cette situation peut se produire lorsque l'éditeur n'offre pas de garantie de prise en compte de la vulnérabilité et que l'ANSSI estime que les risques présentés par le refus de communiquer de l'éditeur sont plus importants que ceux présentés par une communication sans correctif (visant par exemple à recommander le remplacement du produit affecté).

L'ANSSI estime que des vulnérabilités peuvent être significatives sans être activement exploitées, permettant d'assurer un traitement préventif de ces dernières et d'anticiper les attaques. Le coût de remédiation post-exploitation de vulnérabilité est en effet bien plus élevé que celui de l'application d'un correctif.

Enfin, l'évaluation du caractère significatif de la vulnérabilité tient compte de l'environnement et du contexte du produit vulnérable, ce qui doit permettre

d'éviter le recours à l'article L. 2321-4-1 pour une vulnérabilité qui affecte un produit dont le cycle de vie est officiellement terminé.

5.1.9 Art. R.2321-1-17 II. Contenu et format de l'information aux utilisateurs

Questions ou remarques reçues par l'ANSSI :

- *Par quel moyen spécifique l'éditeur informe les utilisateurs, le décret mentionnant simplement un « message d'information » ? Quels sont les moyens de notification autorisés (publication sur un site à accès restreint ou public, notification individuelle, autre) ?*
- *En quoi doit consister le « message d'information » mentionné à l'article R. 2321-1-17 ? Un message d'information sur le site internet de l'éditeur (comme une CVE) est-il considéré comme satisfaisant à cette obligation ?*

La méthode de communication aux clients sera établie par l'éditeur, conjointement avec l'ANSSI, en tenant compte de la situation. Elle pourra effectivement prendre la forme d'un avis de sécurité publié sur le site de l'éditeur, de l'enregistrement d'une CVE, ou encore d'une communication privée vers les clients.

5.1.10 Cohérence avec les dispositifs européens.

Questions ou remarques reçues par l'ANSSI :

- *L'augmentation des législations qui obligent les équipes d'intervention en cas d'incident et de vulnérabilité de sécurité des produits à mettre en œuvre des seuils, des calendriers et des processus de signalement différents nuisent à l'élaboration de mesures d'atténuation efficaces. Idéalement, les réglementations devraient harmoniser les seuils, les délais et les rapports de signalement des vulnérabilités et des incidents. Il est recommandé que les exigences en matière de signalement des vulnérabilités soient alignées avec le Cyber Resilience Act, qui s'appliquera également à un large éventail de produits logiciels, comme le décret semble le faire. De même, les exigences en matière de signalement des incidents devraient être alignées sur la directive NIS 2 en raison de l'accent mis sur les opérateurs de services essentiels.*
- *Il est demandé à l'ANSSI d'assurer la cohérence du dispositif avec le cadre européen : CRA/NIS2/LPM.*
- *La directive NIS2, qui fera prochainement l'objet d'une transposition en droit français, prévoit également une procédure de notification en*

cas d'incident. Certains éditeurs de logiciels pourront être soumis à la fois à la directive et à l'article 65 de la LPM : il est dès lors essentiel d'assurer dès maintenant la cohérence entre ces deux dispositifs. Par conséquent, les critères listés à l'article 23.3) de la directive NIS2 pour qualifier un incident « d'important » devraient être mieux intégrés avec les critères prévus par le projet de décret pour qualifier un incident de « significatif ». Par ailleurs, les critères listés dans le projet de décret sont plus nombreux que ceux prévus par la directive NIS2 : doivent-ils dès lors être considérés comme cumulatifs ou alternatifs ?

- *Le Cyber Resilience Act, récemment adopté au niveau européen et applicable à partir de 2027, prévoit aussi une procédure de notification pour les vulnérabilités « activement exploitées » (actively exploited vulnerability) : sur ce point également, le texte français devrait assurer dès maintenant une bonne cohérence avec le futur cadre européen.*

La mise en œuvre de l'article L. 2321-4-1, notamment en matière de procédures et de traitement des signalements, sera effectuée dans un souci de cohérence avec le futur CRA.

L'article L. 2321-4-1 du code de la défense vise les incidents informatiques qui sont susceptibles d'affecter la sécurité du produit développé par un éditeur. Ce contexte particulier diffère de celui des incidents visés par la directive NIS2 dont le périmètre est beaucoup plus large.

6 Entrée en vigueur

6.1 Article 3 du projet de décret : Entrée en vigueur

6.1.1 Délai d'entrée en vigueur des mesures

Questions ou remarques reçues par l'ANSSI :

- *Les demandes de blocage pourraient être exécutées dès 2024, mais le relevé et communication des données DNS demande préalablement des études (qui n'ont pas démarré à date) avant tout développement de solutions techniques non encore choisies. Le développement ne pourra donc intervenir qu'en 2025 après les études menées en 2024. Une réalisation dès 2024 sans étude serait de surcroit très risquée pour la sécurité et le bon fonctionnement des systèmes pendant les Jeux Olympiques.*
- *La date d'entrée en vigueur prévue un mois seulement après la publication du texte semble insuffisante au regard des objectifs poursuivis.*
- *La date d'entrée en vigueur des dispositions du décret, prévue un mois après la publication du texte, apparait trop courte pour permettre aux acteurs de mettre en place les procédures internes et mesures d'information requises vis-à-vis des utilisateurs afin de se mettre en conformité. Un délai allongé apparait plus opportun pour s'assurer de la bonne mise en œuvre des mesures.*

Le niveau élevé de la menace informatique, dans le contexte des Jeux Olympiques et Paralympiques de Paris 2024, encourage à une mise en œuvre rapide d'au moins une partie des dispositifs, en s'appuyant sur des capacités existantes des entités visées. Par exemple, les mesures de filtrage DNS (article L. 2321-2-3 du code de la défense) peuvent permettre de prévenir ou d'endiguer des incidents de sécurité informatique. De même, le signalement d'une vulnérabilité significative par un éditeur (article L. 2321-4-1 du code de la défense) peut permettre d'anticiper l'exploitation de cette vulnérabilité.

La mise en place de certaines mesures nécessitant une étude amont conséquente, comme l'article L. 33-14 alinéa 2 du CPCE, est reportée à décembre 2024.