Avis n° 2024-0369
de l'Autorité de régulation des communications électroniques, des postes et de la distribution de la presse
en date du 28 février 2024
sur le projet de décret pris en application des dispositions relatives à la sécurité des systèmes d'information de la loi de programmation militaire pour les années 2024 – 2030

L'Autorité de régulation des communications électroniques, des postes et de la distribution de la presse (ci-après « l'Autorité » ou « l'Arcep »),

Vu le 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 (ci-après « règlement internet ouvert ») ;

Vu la directive (UE) 2018/1972 du Parlement européen et du Conseil du 11 décembre 2018 établissant le code des communications électroniques européen ;

Vu le code de la défense, notamment ses articles L. 2321-1 et suivants ;

Vu le code des postes et des communications électroniques (ci-après « CPCE »), notamment ses articles L. 32-1, L. 33 à L. 33-2, L. 33-14, L. 34-1, L. 36-5, L. 36-7, L. 36-14, D. 98-5 et D. 99 ;

Vu la loi n° 2004-575 du 21 juin 2004 modifiée pour la confiance dans l'économie numérique (ci-après « LCEN »), notamment son article 6 ;

Vu la saisine pour avis du Secrétaire général de la défense et de la sécurité nationale en date du 23 janvier 2024 ;

Après en avoir délibéré le 28 février 2024,

1 Contexte de la saisine

L'article L. 36-5 du code des postes et des communications électroniques prévoit que l'Arcep est consultée sur les projets de loi, de décret ou de règlement relatifs au secteur des communications électroniques, et participe à leur mise en œuvre.

Par courrier en date du 22 janvier 2024, le secrétaire général de la défense et de la sécurité nationale a sollicité l'avis de l'Arcep sur un projet de décret pris en application des dispositions relatives à la sécurité des systèmes d'information de la loi de programmation militaire pour les années 2024-2030 et portant diverses dispositions intéressant la défense, dans le domaine cyber, et qui modifieraient notamment le CPCE ainsi que le code de la défense.

2 Cadre juridique

La loi de programmation militaire pour la période 2024 à 2030, promulguée le 1er août 2023, comporte plusieurs dispositions permettant à l'ANSSI de renforcer ses capacités de détection, de caractérisation et de prévention des attaques informatiques en impliquant les opérateurs de communications électroniques (ci-après « OCE »), les fournisseurs d'accès à internet (ci-après « FAI »), les hébergeurs

de données, les opérateurs de centres de données, les fournisseurs de système de résolution de noms de domaine ainsi que les offices et bureaux d'enregistrement de noms de domaine.

Les dispositions de la loi permettent notamment à l'ANSSI de :

- prescrire des mesures graduelles de filtrage des noms de domaine[1], en cas d'attaque, aux fournisseurs de systèmes de résolution de nom de domaine, et aux offices et bureaux d'enregistrement de noms de domaine afin de neutraliser l'utilisation dévoyée d'un nom de domaine et prévenir les potentielles victimes de la vulnérabilité ou de l'atteinte de leurs systèmes d'information. L'ANSSI peut ainsi demander à ces acteurs de bloquer, enregistrer, renouveler, suspendre, transférer et rediriger un nom de domaine concerné par une menace susceptible de porter atteinte à la sécurité nationale ;
- obliger les fournisseurs de système de résolution de noms de domaine à transmettre à l'ANSSI les données de résolution des noms de domaine (« *cache DNS* »)[2]. L'ANSSI peut ainsi obtenir les données techniques non identifiantes enregistrées de manière temporaire par leurs serveurs gérant le système d'adressage par domaines, elles permettent de conserver la traduction des noms de domaine en des numéros uniques identifiants l'adresse des équipements connectés à internet ;
- obliger les éditeurs de logiciel à notifier à l'ANSSI et leurs clients lorsqu'ils sont victimes d'un incident informatique ou qu'ils ont une vulnérabilité critique sur un de leurs produits[3] ;
- imposer aux OCE également désignés comme opérateur d'importance vitale (OIV) de se doter de leur propre système de détection pour mettre en œuvre les marqueurs techniques de l'ANSSI sur leurs réseaux[4] aux seules fins de détecter des événements susceptibles d'affecter la sécurité des systèmes d'information de certains de leurs abonnés : autorité publique (AP), opérateur d'importance vitale (OIV), opérateur de service essentiel (OSE) ou un de leurs sous-traitants ;
- mettre en œuvre des sondes de circonstance[5] sur le réseau d'un opérateur, sur le système d'information d'un hébergeur ou sur celui d'un opérateur de centre de données afin de recueillir les données de trafic ou les données stockées sur les équipements concernés par une menace susceptible d'affecter la sécurité des systèmes d'information des AP, des OIV ou des OSE[6] ainsi que de leurs sous-traitants.

En conséquence, la loi fait évoluer les modalités du contrôle exercé par l'Arcep :

- d'une part, elle étend les modalités de contrôle *a posteriori*, qui sont actuellement en vigueur pour la mise en œuvre de sondes de circonstance chez les hébergeurs ou les opérateurs, à la transmission de marqueurs techniques aux opérateurs, ainsi qu'aux nouveaux dispositifs de caractérisation de menace (filtrage ou redirection de noms de domaine, collecte des données de cache DNS) ;
- d'autre part, elle instaure un contrôle *a priori* au travers d'avis préalables de l'Arcep auxquels l'ANSSI doit se conformer pour le renouvellement d'une redirection de noms de domaine, ainsi que la mise en œuvre de la collecte élargie de données réseaux et de copie de serveurs dans le cadre des sondes de circonstance.

[1] Article L. 2321-2-3 du code de la défense.

[2] Article L. 2321-3-1 du code de la défense.

[3] Article L. 2321-4-1 du code de la défense.

[4] Article L. 2321-3 du code de la défense.

[5] Article L. 2321-2-1 du code de la défense.

[6] Article L. 2321-2-1 du code de la défense.

3 Présentation du projet de décret qui fait l'objet d'une saisine de l'Arcep

Le projet de décret vise à définir les modalités d'application des articles législatifs relatifs aux modes d'actions de l'ANSSI (L. 2321-2-1 à L. 2321-4-1 du code de la défense) et aux modalités de leur contrôle par l'Arcep (L. 33-14, L. 36-7 et L. 36-14 du CPCE).

3.1 S'agissant des modifications du code de la défense

L'article 1er du projet de décret prévoit de créer les sous-sections 1 à 5 du chapitre Ier du titre II du livre III de la deuxième partie réglementaire du code de la défense. L'objet de chaque sous-section est présentée ci-après.

La sous-section 1 précise les modalités de mise en œuvre par l'ANSSI des copies physiques de serveur et des captures des communications électroniques émises et reçues par un serveur sur le réseau des opérateurs de communications électroniques ou le système d'information d'un FAI, d'un hébergeur ou d'un centre de données. Elles prévoient à cet effet que :

- s'agissant de la capture des communications électroniques :
    - la décision de mise en œuvre des captures des communications électroniques sur les réseaux des personnes susmentionnées est accompagnée d'un cahier des charges précisant notamment « *les conditions techniques d'organisation et de fonctionnement nécessaires* », dont l'élaboration est précédée, le cas échéant, d'une phase de test préalable sur les réseaux des opérateurs de communications électroniques ou systèmes d'information des fournisseurs d'accès, des hébergeurs ou des centres de données[7] ;
    - cette décision est subordonnée à l'obtention d'un avis conforme de l'Arcep[8]. La durée de mise en œuvre initiale d'une capture ne saurait excéder trois mois. Elle pourra néanmoins être prorogée, après avis conforme de l'Arcep, par décision de l'ANSSI notifiée aux personnes concernées[9] ;
- s'agissant de la copie de serveur sur un équipement appartenant à une des personnes susmentionnées, la décision de mise en œuvre de ce dispositif est subordonnée à l'obtention d'un avis conforme de l'Arcep[10] ;
- les données recueillies doivent être analysées dans un délai de trois mois par les agents habilités de l'ANSSI. Les données relatives aux communications électroniques liées aux activités de l'attaquant ou aux traces d'activité système liées à l'attaquant et jugées utiles à la prévention et à la caractérisation des menaces ne peuvent être conservées plus de deux ans. Les autres données analysées sont détruites par l'ANSSI dans un délai d'un jour ouvré une fois leur analyse effectuée[11] ;
- les modalités de juste rémunération des prestations assurées par les opérateurs de communications électroniques, les fournisseurs d'accès, les hébergeurs ou les centres de données au titre de l'article L. 2321-2-1 sont fixées par arrêté conjoint du Premier ministre et du ministre chargé des communications électroniques[12].

⁂

[7] Article R. 2321-1-2 du code de la défense.

[8] Article R. 2321-1-2 du code de la défense.

[9] Article R. 2321-1-3 du code de la défense.

[10] Article R. 2321-1-3 du code de la défense.

[11] Article R. 2321-1-5 du code de la défense.

[12] Article R. 2321-1-6 du code de la défense.

La sous-section 2 précise les modalités de mise en œuvre, par les fournisseurs de système de résolution de noms de domaine[13] et les offices et bureaux d'enregistrement de noms de domaine établi sur le territoire français, des mesures de blocage, suspension, redirection, enregistrement, renouvellement ou transfert de noms de domaine demandées par l'ANSSI. Elles prévoient à cet effet que :

- s'agissant des demandes notifiées par l'ANSSI aux titulaires de nom de domaine[14] :
    - la demande de neutralisation de la menace précise « *les mesures techniques correctives ainsi que le délai dans lequel ces mesures doivent être mises en œuvre* » ;
    - le titulaire doit rendre compte à l'ANSSI en fournissant notamment « *la liste des mesures qu'il a mises en œuvre pour permettre d'établir que la menace est neutralisée* » ;
    - l'ANSSI peut demander des informations complémentaires pour lui permettre d'établir que la menace est neutralisée.
- s'agissant des demandes de filtrage adressées aux fournisseurs de système de résolution de noms de domaine ou aux offices et bureaux d'enregistrement[15] notifiées par l'ANSSI par tout moyen tenant compte de la menace et de l'urgence ;
    - ces demandes, qui sont communiquées à l'Arcep, précisent notamment « *la nature et la durée de la mesure demandée* » ;
    - les personnes destinataires des demandes tiennent informée sans délai à l'ANSSI de la mise en œuvre des mesures demandées.
- s'agissant des données ainsi recueillies dans le cadre de ces deux dispositifs[16] :
    - l'analyse de l'utilité des données à la prévention et à la caractérisation doit être faite dans un délai de trois mois ;
    - les données relatives aux communications électroniques liées aux activités de l'attaquant à destination du nom de domaine concerné et jugées utiles ne peuvent être conservées plus de 5 ans et celles qui ne le sont pas doivent être détruites dans un délai d'un jour ouvré une fois leur analyse effectuée.

Par ailleurs, les dispositions précisent que les modalités de juste rémunération des prestations assurées par fournisseurs de système de résolution de noms de domaine et les offices et bureaux d'enregistrement au titre de l'article L. 2321-2-3 sont fixées par arrêté conjoint du Premier ministre et du ministre chargé des communications électroniques[17].

⁂

La sous-section 3 précise les modalités de collecte par l'ANSSI des enregistrements des serveurs de résolution de noms de domaine auprès des fournisseurs de système de résolution de noms de domaine. Elles prévoient à cet effet que :

- les conditions de transmission par les fournisseurs de système de résolution de noms de domaine des données sur les serveurs de résolution de noms de domaine à l'ANSSI, sont déterminées par le présent décret et précisées par une décision de l'ANSSI notifiée aux fournisseurs et communiquée à l'Arcep. Cette décision « *tient compte des contraintes techniques* » du fournisseur et précise notamment la fréquence du relevé des données de cache DNS et la fréquence de transmission des données[18] ;

[13] Cela peut comprendre les FAI et hébergeurs. Toutefois ces acteurs n'offrent pas tous un système de résolution de noms de domaine.

[14] Articles R. 2321-1-7 et R. 2321-1-9 du code de la défense.

[15] Article R. 2321-1-8 du code de la défense.

[16] Article R. 2321-1-10 du code de la défense.

[17] Article R. 2321-1-11 du code de la défense.

[18] Article R. 2321-1-13 du code de la défense.

- les catégories de données techniques transmises à l'ANSSI comprennent notamment « *les enregistrements DNS issus des serveurs gérant le système d'adressage par domaine* » (type, durée de vie, valeur et horodatage)[19].

⁂

La sous-section 4 précise que les dispositifs de traçabilité des données collectées doivent garantir notamment l'identification des agents de l'ANSSI ayant accès à celles-ci et permettre l'enregistrement des opérations effectuées sur celles-ci, et en particulier la suppression des données collectées à l'issue des délais légaux (2 ans dans le cadre des sondes de circonstance et 5 ans dans le cadre du dispositif d'envoi de marqueurs, des mesures de filtrage de noms de domaine et de la collecte des caches DNS)[20].

⁂

La sous-section 5 précise les modalités de notification des vulnérabilités affectant un produit et des incidents informatiques par les éditeurs logiciels, ainsi que les critères d'appréciation du caractère significatif de ces vulnérabilités ou incidents exigeant des éditeurs de logiciels qu'ils avertissent l'ANSSI et informent leurs utilisateurs. Elles prévoient à cet effet que :

- le caractère significatif de la vulnérabilité ou de l'incident est apprécié par l'éditeur logiciel selon notamment « *le nombre d'utilisateurs concernés par la vulnérabilité* » et l'impact technique de la vulnérabilité ou de l'incident sur le fonctionnement attendu du produit[21] ;
- la notification d'une vulnérabilité ou d'un incident significatif à l'ANSSI doit être effectuée par l'éditeur logiciel sans délai et au plus tard dans un délai de vingt-quatre heures après en avoir eu connaissance en complétant le formulaire de déclaration disponible sur le site internet de l'ANSSI ; cette notification comprend notamment les informations qui ont permis à l'éditeur logiciel d'établir la vulnérabilité ou l'incident[22] ; l'ANSSI peut lui demander des informations complémentaires et l'application de mesures utiles afin de sécuriser la vulnérabilité ou l'incident déclaré[23] ;
- l'injonction faite par l'ANSSI à un éditeur de logiciel n'ayant pas informé les utilisateurs du produit affecté dans le délai imparti par l'ANSSI de procéder à cette information lui est notifiée par lettre recommandée avec avis de réception[24] ; si l'éditeur logiciel ne met pas en œuvre cette injonction, l'ANSSI informe cet éditeur qu'elle peut notamment rendre public la vulnérabilité ou l'incident[25].

3.2 S'agissant des modifications du CPCE

L'article 2 du projet de décret modifie en particulier les articles R. 9-12-1 et R. 9-12-6 du CPCE et crée un article R. 9-12-6-1.

Le projet d'article R. 9-12-1 précise le contenu de la juste rémunération permettant notamment de couvrir les coûts de conception, de déploiement et de maintenance des dispositifs de détection mis en œuvre par les OCE pour répondre aux demandes de l'ANSSI. La solution technique envisagée par l'opérateur doit être validée par le ministre chargé des communications électroniques après avis de l'ANSSI.

[19] Article R. 2321-1-14 du code de la défense.

[20] Article R. 2321-1-15 du code de la défense.

[21] Article R. 2321-1-16, I du code de la défense.

[22] Article R. 2321-1-16, II du code de la défense.

[23] Article R. 2321-1-16, III du code de la défense.

[24] Article R. 2321-1-18 du code de la défense.

[25] Article R. 2321-1-19 du code de la défense.

Le projet d'article R. 9-12-6 précise les modalités de contrôle *a posteriori* de l'ANSSI par la formation RDPI de l'Arcep. Il liste ainsi le minimum d'informations que l'ANSSI est tenue de communiquer sans délai à la formation RDPI au titre des dispositifs relatifs aux envois de marqueurs techniques, aux sondes de circonstances, aux mesures de filtrage de noms de domaine et à la collecte des données de cache DNS. Il s'agit notamment des éléments justifiant l'existence d'une menace, des réseaux et systèmes d'information concernés, des caractéristiques techniques des dispositifs, des catégories de données obtenues ainsi que des résultats de l'analyse technique.

Le projet d'article R. 9-12-6-1 précise les modalités de contrôle *a priori* de l'ANSSI par la formation RDPI. Il précise ainsi un délai maximum d'un mois pour rendre l'*« avis conforme »*[26] et liste les éléments à produire par l'ANSSI lors de la saisine dans les cas de la mise en œuvre des dispositifs de capture de flux et de copie d'équipements ou d'une demande de prorogation de redirection de noms de domaine. Il s'agit notamment des éléments justifiant l'existence d'une menace, des réseaux et systèmes d'information concernés, des caractéristiques techniques des dispositifs ainsi que des éléments de nature à justifier la persistance de la menace dans le cas des mesures de redirection de noms de domaine.

4 Observations de l'Arcep

À titre liminaire, l'Autorité tient à rappeler, comme elle l'a souligné dans son avis n° 2023-0542 du 9 mars 2023 sur le projet de loi relatif à la programmation militaire pour les années 2024-2030 (ci-après « LPM »), qu'elle partage le souci affiché par le Gouvernement de renforcer les capacités nationales de détection, de caractérisation et de prévention des attaques informatiques que ce projet de décret vise à améliorer. La lutte contre la cybercriminalité et les cybermenaces est en effet un enjeu majeur pour la sécurité nationale et l'économie française dans son ensemble.

À cet égard, l'Autorité accueille favorablement la possibilité pour l'ANSSI, prévue par la LPM et son projet de décret d'application, d'impliquer au-delà des opérateurs de communications électroniques, d'autres acteurs du numérique notamment les hébergeurs de données, les opérateurs de centres de données, les fournisseurs de systèmes de résolution de noms de domaine ou les offices et bureaux d'enregistrement de noms de domaine, de renforcer ses capacités de détection, de caractérisation et de prévention des attaques informatiques.

Par ailleurs, l'Arcep reste vigilante quant au respect par les opérateurs du règlement internet ouvert[27] et notamment des dérogations prévues pour les cas limitativement définis par ce règlement. En particulier, en cas de filtrage d'un ou plusieurs noms de domaine réalisé au titre des dispositions de la LPM, il conviendra de veiller à ce que les mesures de gestion du trafic mise en œuvre sur les réseaux pour bloquer des flux malveillants, n'excèdent pas les demandes de l'ANSSI.

4.1 S'agissant de l'impact sur les acteurs régulés

L'élargissement du périmètre de l'ANSSI en termes de collecte de données et de filtrage de noms de domaine en cas d'attaque est susceptible d'avoir un impact majeur sur le fonctionnement des réseaux ou systèmes d'information des personnes concernées, et ce, à plusieurs égards.

En premier lieu, il est à noter que ces mesures sont de nature à engendrer des effets significatifs sur l'exploitation des réseaux et des systèmes d'information des personnes concernées, ainsi que des services qu'elles offrent. C'est pourquoi il semble indispensable que l'ANSSI s'assure, notamment lors

[26] « *En l'application du II de l'article L. 36-14, la formation de règlement des différends, de poursuite et d'instruction de l'Autorité de régulation des communications électroniques, des postes et de la distribution de la presse rend un avis conforme dans un délai d'un mois.* »

[27] 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.

d'échanges préalables avec les acteurs obligés, en particulier les moins familiers avec les actions et demandes de l'ANSSI :

- de clarifier le type de demandes qu'effectuera l'ANSSI et les expliciter de manière suffisamment compréhensible ;
- de préciser la façon de mettre en œuvre efficacement les mesures dans les délais prévus en fonction notamment de l'architecture des réseaux ou des systèmes d'information concernés ;
- d'établir les points de contacts pertinents et le partage de responsabilité en cas de dysfonctionnement ;
- de définir, pour la collecte des informations de cache DNS, une fréquence adaptée au volume d'activité des fournisseurs de systèmes de résolution de noms de domaine ;
- de prévoir un message aisément compréhensible pour l'utilisateur lorsqu'un nom de domaine est redirigé vers un serveur neutre ou maîtrisé par l'ANSSI.

En deuxième lieu, l'Autorité accueille favorablement le fait qu'une compensation financière ait été prévue pour prendre en charge les surcoûts identifiables et spécifiques des prestations assurées au titre de la mise en œuvre et du fonctionnement des différents dispositifs par les opérateurs et fournisseurs de services.

En troisième lieu, l'ANSSI prévoit de s'appuyer sur une plateforme interministérielle opérée par le commissariat aux communications électroniques de défense (CCED) pour standardiser et sécuriser les échanges liés à la mise en œuvre des demandes d'exploitation de marqueurs techniques ou de sondes de circonstance. Par ailleurs, sur un plan plus technique, le projet de décret définit des procédures de filtrage des noms de domaine qui visent à sécuriser le système de noms de domaine en cas de menace susceptible de porter atteinte à la sécurité nationale, alors que plusieurs dispositions prévoient par ailleurs des obligations de blocage par DNS sur décision d'autres autorités administratives[28] ou judiciaires. Dans ce contexte, l'Arcep estime nécessaire que l'ANSSI veille à ce que les modalités de mise en œuvre de la technique de blocage DNS pour ses besoins soient harmonisées avec celles liées aux autres dispositifs de blocage DNS s'imposant aux fournisseurs de service.

En dernier lieu, afin de renforcer la lisibilité et la sécurité juridique pour les opérateurs concernés, il conviendrait de prévoir dans le décret les délais objectifs de mise en œuvre des mesures demandées par l'ANSSI, compatibles avec les nécessités opérationnelles de l'action publique en matière de protection contre les attaques informatiques. Le détail des modifications proposées est exposé en annexe.

4.2 S'agissant de l'impact sur les missions de contrôle confiées à l'Arcep

Comme évoqué dans son avis n° 2023-0542, l'Autorité rappelle que la mise en œuvre de ce contrôle *a priori* constitue un changement de la nature du contrôle effectué, et que son organisation et son mode de fonctionnement pourraient limiter sa réactivité opérationnelle.

Dans ces conditions, l'Autorité prend acte du délai maximum d'un mois qui lui est imparti pour rendre des avis préalables au renouvellement d'une redirection de noms de domaine, ainsi qu'à la mise en œuvre de la collecte élargie de données réseaux et de copie de serveurs dans le cadre des sondes de circonstance.

Toutefois, il conviendrait que les moyens opérationnels et organisationnels dont dispose l'Arcep pour mener cette mission évoluent en lien avec l'activité de l'ANSSI, notamment si celle-ci devait être amenée à transmettre plusieurs saisines en parallèle à l'Arcep.

Par ailleurs, l'Autorité accueille positivement la précision, comme elle l'avait demandé dans son précédent avis, du délai de suppression des données jugées non utiles par l'ANSSI pour la prévention et la caractérisation de la menace, fixé à un jour ouvré. Une telle précision permet de clarifier les

[28] Notamment dans les cas de contenus terroristes, contenus pédopornographiques, et selon divers dispositifs notamment liés à la loi n° 2004-575 du 21 juin 2004 modifiée pour la confiance dans l'économie numérique (LCEN).

conditions dans lesquelles la formation RDPI exercera son contrôle. L'Arcep sera vigilante quant aux moyens techniques mis à disposition par l'ANSSI pour, d'une part, lui assurer un accès complet et permanent aux informations de traçabilité et, d'autre part, accomplir sa mission de vérification.

Le présent avis sera transmis au Secrétaire général de la défense et de la sécurité nationale et sera publié au *Journal officiel de la République française*.

Fait à Paris, le 28 février 2024,

La Présidente

Laure de LA RAUDIÈRE

Annexe à l'avis n° 2024-0369 de l'Autorité de régulation des communications électroniques, des postes et de la distribution de la presse

Les ajouts proposés figurent en **gras.**

Les suppressions proposées sont ~~barrées.~~

Projet de décret et dispositifs concernés	Modification proposée	Commentaires
R. 2321-1-7 – Mesures de blocage, enregistrement, renouvellement, suspension, transfert et redirection de nom de domaine	« *Pour l'application du I de l'article L. 2321-2-3, lorsque l'Agence nationale de la sécurité des systèmes d'information demande au titulaire du nom de domaine de prendre les mesures adaptées pour neutraliser la menace, elle lui notifie**, sous un délai de XXX, par tout moyen tenant compte de la menace et de l'urgence,** les mesures techniques correctives à appliquer ainsi que le délai dans lequel ces mesures doivent être mises en œuvre.* »	Lorsque l'ANSSI notifie des mesures correctives, la loi dispose que l'ANSSI doit tenir compte de la nature du titulaire et de ses contraintes opérationnelles. Il conviendrait que ces dispositifs soient mis en œuvre en concertation avec le titulaire notamment pour déterminer le délai imparti et préciser la forme de la notification.
R. 2321-1-7 – Mesures de blocage, enregistrement, renouvellement, suspension, transfert et redirection de nom de domaine	« *Le titulaire de bonne foi rend compte à l'Agence précitée de la mise en œuvre des mesures **par tout moyen sous un délai de X**.* »	Préciser les valeurs des délais impartis aux personnes concernées afin d'assurer la sécurité juridique des acteurs et des dispositifs
R. 2321-1-16 II – Signalement de vulnérabilités et incidents par les éditeurs de logiciels	« *S'il constate que la vulnérabilité ou l'incident est significatif, l'éditeur de logiciel le notifie **à** l'Agence nationale de la sécurité des systèmes d'information ~~sans délai~~ **sous un délai de X** et au plus tard dans un délai de vingt-quatre heures après en avoir eu connaissance.* »	

Projet de décret et dispositifs concernés	Modification proposée	Commentaires
R. 2321-1-17 I – Signalement de vulnérabilités et incidents par les éditeurs de logiciels	« *Ce délai ne peut être inférieur à dix jours ouvrables, sauf en cas de risque pour la défense et la sécurité nationale requérant une information des utilisateurs ~~sans délai~~* ***sous un délai de X****.* »	
R. 2321-1-18 – Signalement de vulnérabilités et incidents par les éditeurs de logiciels	« *En application du cinquième alinéa de l'article L. 2321-4-1, l'injonction est motivée et mentionne le délai imparti****, au plus tard dans un délai de X,*** *ainsi que les mesures requises pour s'y conformer.* »	
R. 2321-1-2 II – Décision de mise en œuvre d'une capture de flux ou d'une copie de serveur	*« La décision de mettre en œuvre les dispositifs mentionnés au 2° du même article ne peut être notifiée****, aux personnes mentionnées au I de l'article R. 2321-1-2 et à l'Autorité de régulation des communications électroniques, des postes et de la distribution de la presse,*** *qu'après avoir obtenu l'avis conforme de* ***celle-ci*** *~~l'Autorité de régulation des communications électroniques, des postes et de la distribution de la presse~~. »*	Les destinataires des notifications ne sont pas précisées.
R. 2321-1-3 al. 3 – Décision de prorogation de capture de flux	« *Elle est notifiée aux personnes mentionnées au I de l'article R. 2321-1-2* ***et communiquée à l'Autorité de régulation des communications électroniques, des postes et de la distribution de la presse.*** »	
R. 2321-1-8 II – Mesures de blocage, enregistrement, renouvellement, suspension, transfert et redirection de nom de domaine	« *l'Agence précitée communique****, sans délai,*** *chaque demande mentionnée au I du présent article à l'Autorité de régulation des communications électroniques, des postes et de la distribution de la presse* »	Le délai de communication à l'Arcep des demandes n'est pas précisé.

Projet de décret et dispositifs concernés	Modification proposée	Commentaires
R. 2321-1-9 – Mesures de blocage, enregistrement, renouvellement, suspension, transfert et redirection de nom de domaine	« *L'Agence nationale de la sécurité des systèmes d'information demande, le cas échéant, des informations complémentaires permettant d'établir que la menace est neutralisée.* ***Lorsque le titulaire communique des informations complémentaires, l'agence précitée les communique sans délai à l'Arcep***. »	
R. 2321-1-15 al. 1er – Identification des agents spécialement habilités	*« Les dispositifs de traçabilité des données collectées mentionnés au 2° de l'article L. 36-14 du code des postes et des communications électroniques garantissent notamment l'identification des agents mentionnés au cinquième alinéa de l'article L. 2321-2-1**, au IV de l'article L. 2321-2-3,** au deuxième alinéa de l'article L. 2321-3 et au premier alinéa de l'article L. 2321-3-1. »*	Les agents qui travaillent sur les données du dispositif de filtrage DNS et qui ont notamment accès aux données utiles à la prévention devraient aussi être dûment identifiés.