Avis n° 2023-0542 de l'Autorité de régulation des communications électroniques, des postes et de la distribution de la presse en date du 9 mars 2023 sur des dispositions relatives à la sécurité des systèmes d'information dans le cadre du projet de loi relatif à la 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 sur 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 février 2023,

Après en avoir délibéré le 9 mars 2023, en présence des six membres du collège nommés à date, sur les sept membres devant le composer,

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 23 février 2023, enregistré à l'Autorité le 24 février, le secrétaire général de la défense et de la sécurité nationale a sollicité l'avis de l'Arcep sur des dispositions relatives à la sécurité des systèmes d'information dans le cadre d'une saisine du projet de loi relatif à la programmation militaire pour les années 2024 – 2030 et portant diverses dispositions intéressant la défense, dans le domaine cyber, et qui modifieraient notamment le code des postes et des communications électroniques ainsi que le code de la défense.

2 Présentation des dispositions qui font l'objet d'une saisine de l'Arcep

Les dispositions du projet de loi, soumis pour avis à l'Arcep, complète le cadre juridique actuel en matière de sécurité des systèmes d'information introduit par l'article 34 de la loi n° 2018-607 du

13 juillet 2018 relative à la programmation militaire pour les années 2019 à 2025. Il comporte plusieurs dispositions permettant à l'Agence nationale de sécurité des systèmes d'information (ci-après « ANSSI ») de renforcer ses capacités de détection, de caractérisation et de prévention des attaques informatiques en impliquant les opérateurs de communications électroniques (ci-après « opérateurs »), les fournisseurs d'accès à internet (ci-après « FAI ») et hébergeurs de données (ci-après « hébergeurs »), les opérateurs de centres de données, les offices et bureaux d'enregistrement de noms de domaine.

Ainsi, le projet d'article 32 introduit un article L. 2321-2-3 au code de la défense et prévoit d'étendre les capacités d'action de l'ANSSI dans le secteur des noms de domaine. Dans ce cadre, l'ANSSI peut prescrire des mesures de filtrage des noms de domaine aux FAI, aux hébergeurs, et aux offices et bureaux d'enregistrement de noms de domaine afin de neutraliser l'utilisation dévoyée d'un nom de domaine.

L'ANSSI peut ainsi notamment demander aux FAI et hébergeurs, *« lorsqu'il est constaté qu'une menace susceptible de porter atteinte à la sécurité nationale résulte de l'exploitation d'un nom de domaine enregistré à cette fin »* et *« en l'absence de neutralisation de cette menace »* par le titulaire du nom de domaine, *« de procéder, sans délai, au blocage ou à la redirection des noms de domaine concernés vers un serveur neutre ou vers un serveur sécurisé »* qu'elle maîtrise.

L'ANSSI peut également demander à *« l'office d'enregistrement du domaine de l'internet correspondant aux codes pays du territoire national ou à un bureau d'enregistrement établi sur le territoire français »* d'*« enregistrer, de renouveler, de suspendre ou de transférer, sans délai, les noms de domaine concernés »* par cette menace.

Dans ce cadre, il prévoit également que l'ANSSI peut informer *« les utilisateurs ou les détenteurs des systèmes d'information menacés »* de la vulnérabilité ou de l'atteinte de leurs systèmes d'information.

Le projet d'article 33 crée un article L. 2321-3-1 au code de la défense et prévoit d'imposer, pour les besoins de la sécurité des systèmes d'information et afin de détecter et de caractériser des attaques informatiques, une obligation pour les opérateurs ou les fournisseurs de système de résolution des noms de domaine de transmettre à l'ANSSI *« les données techniques non identifiantes enregistrées de manière temporaire par leurs serveurs gérant le système d'adressage par domaines »*.

Le projet d'article 35 complète, en premier lieu, l'article L. 2321-2-1 du code de la défense qui prévoit que, lorsque l'ANSSI a connaissance d'une menace susceptible de porter atteinte à la sécurité des systèmes d'information des autorités publiques (ci-après « AP »), des opérateurs d'infrastructures vitales (ci-après « OIV ») ou des opérateurs de services essentiels (ci-après « OSE »), elle peut mettre en œuvre sur le réseau d'un opérateur, sur le système d'information d'un hébergeur ou sur celui d'un opérateur de centre de données des sondes de circonstance afin de recueillir les données de trafic sur les réseaux et des données stockées sur les équipements concernés par la menace, en réalisant notamment une copie de serveur. Il précise que ces dispositifs sont mis en œuvre pour la durée et dans la mesure strictement nécessaires à la caractérisation de la menace et aux seules fins de détecter et de caractériser des événements susceptibles d'affecter la sécurité des systèmes d'information des AP, des OIV ou des OSE, ainsi que des opérateurs publics ou privés *« participant aux systèmes d'information de ces entités »*, notamment leurs sous-traitants.

Il prévoit par ailleurs que la mise en place des dispositifs de détection et la copie des données des machines auprès des entités ciblées peuvent être sous-traitées à un autre service de l'État.

En second lieu, le projet d'article 35 complète l'article L. 33-14 du CPCE et prévoit que les opérateurs désignés comme OIV doivent mettre en œuvre des marqueurs techniques sur leurs réseaux aux seules fins de détecter des événements susceptibles d'affecter la sécurité des systèmes d'information de leurs abonnés.

Il prévoit également de supprimer l'exigence d'assermentation des agents de l'ANSSI qui exploitent les données collectées auprès des opérateurs.

En troisième lieu, le projet d'article 35 modifie le premier alinéa de l'article L. 2321-3 du code de la défense et prévoit d'étendre aux hébergeurs l'obligation de transmettre à l'ANSSI, pour les besoins de la sécurité des systèmes d'information des autorités publiques, des OIV et des OSE, « *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* ».

En quatrième lieu, s'agissant des missions dévolues à l'Arcep, le projet d'article 35 modifie, d'une part, l'article L. 36-7 du CPCE en prévoyant de confier à l'Arcep la compétence de veiller au respect des dispositions introduites par les projets d'articles 32 et 33 et, d'autre part, prévoit de soumettre à un avis de l'Arcep le renouvellement des mesures de redirection d'un nom de domaine mentionnées au projet d'article 32 et la mise en œuvre des sondes de circonstance prévue au projet d'article 35. L'ANSSI doit se conformer à ces avis avant d'appliquer ces mesures.

3 Observations de l'Arcep

À titre liminaire, l'Autorité tient à souligner 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 loi vise à améliorer. La lutte contre la cybercriminalité et les cybermenaces est en effet un enjeu majeur pour notre pays, la sécurité nationale et l'économie française dans son ensemble. À titre d'illustration, l'OCDE estime, dans un rapport publié en 2021, que les risques liés à la sécurité numérique ont un coût annuel mondial supérieur à 100 milliards de dollars.

3.1 Sur l'élargissement du périmètre de l'ANSSI en termes de collecte de données et de filtrage de noms de domaine en cas d'attaque

Pour rappel, la loi relative à la programmation militaire pour les années 2019 à 2025 et portant diverses dispositions intéressant la défense[1] a introduit des dispositions permettant à l'ANSSI de :

- transmettre aux opérateurs des marqueurs caractéristiques d'une attaque informatique et, si ces marqueurs permettent à l'opérateur de détecter de potentielles victimes de cette attaque[2], obtenir des opérateurs les données techniques strictement nécessaires à l'analyse de celle-ci ;
- mettre en œuvre et exploiter ses propres systèmes de détection sur le réseau des opérateurs ou sur le système d'information des hébergeurs[3] sur la base de marqueurs techniques pour ne recueillir que les données techniques strictement nécessaires à la prévention et à la caractérisation des menaces ;
- demander aux opérateurs qui mettent en œuvre des marqueurs techniques d'informer leurs abonnés de la vulnérabilité de leurs systèmes d'information ou des atteintes qu'ils ont subies.

Elle a également confié à la formation de règlement des différends, de poursuite et d'instruction (formation RDPI), de l'Arcep la mission de veiller, par des contrôles *a posteriori*, au respect par l'ANSSI des conditions d'application des articles de loi[4]. La formation RDPI doit ainsi s'assurer que l'ANSSI n'accède qu'aux données strictement prévues par la loi.

[1] Article 34 de la loi n°2018-607 en date du 13 juillet 2018 relative à la programmation militaire pour les années 2019 à 2025 et portant diverses dispositions intéressant la défense.

[2] La loi n'autorise l'ANSSI à solliciter de tels éléments que si les victimes potentielles détectées sont des autorités publiques (AP) ou des opérateurs d'importance vitale (OIV) ou des opérateurs de service essentiel (OSE).

[3] Ou plus généralement les personnes mentionnées aux 1 et 2 du I de l'article 6 de la loi du 21 juin 2004 pour la confiance dans l'économie numérique.

[4] Articles L. 2321-2-1 et L. 2321-3 du code de la défense.

Depuis 2019, la formation RDPI a été informée par l'ANSSI – et a contrôlé – 11 mises en œuvre de sondes de circonstance et de 13 transmissions de marqueurs caractéristiques d'une attaque informatique[5].

⁂

L'Arcep comprend que les dispositions introduites dans ce projet de loi permettront à l'ANSSI de :

- mettre en œuvre des systèmes de détection à même de capturer l'intégralité d'un trafic réseau – et non plus uniquement les données techniques – ou de copier la totalité d'un serveur pour y rechercher des informations caractérisant une menace ;
- obtenir des données techniques supplémentaires de la part d'exploitant de serveurs DNS ;
- ordonner le blocage de noms de domaine.

Or, d'une part, ces dispositions, qui étendent le champ des données que l'ANSSI peut collecter à l'ensemble du trafic réseau et des copies de serveurs, et non plus aux seules données techniques, présentent un risque accru quant au respect des libertés publiques. Elles ne sont donc pas sans conséquence sur la confiance des utilisateurs finals vis-à-vis des acteurs qui font l'objet de telles demandes. En particulier, en fonction de la nature et du volume des données concernées par ces demandes, les utilisateurs pourraient questionner leur choix de fournisseur d'accès à internet ou de services numériques, ce qui, *in fine,* pourrait avoir des effets sur les modèles d'affaires de ces acteurs et conduire à des distorsions concurrentielles avec des acteurs, par exemple extraterritoriaux, qui ne sont pas eux-mêmes soumis à ces obligations.

D'autre part, les mesures envisagées dans ce projet sont de nature à engendrer des effets significatifs sur l'exploitation des réseaux des opérateurs de communications électroniques ainsi que des services qu'ils offrent.

Dans le même temps, il ne peut de plus être exclu que ces mécanismes se heurtent en pratique à certaines limites. En particulier, la généralisation des technologies de chiffrement sur les réseaux et sur les serveurs pourrait avoir des conséquences sur l'efficacité des dispositifs envisagés.

C'est pourquoi l'Arcep estime utile qu'une évaluation précise de ces dispositifs soit réalisée dans les meilleurs délais par le Gouvernement afin d'analyser les bénéfices obtenus, voire, pour ce qui concerne les dispositifs susceptibles de capter des volumes importants de données, qu'un cadre législatif expérimental soit privilégié à un cadre pérenne.

Par ailleurs, **dans ce contexte, l'Arcep estime dommageable la suppression de l'assermentation demandée aux personnels de l'ANSSI** qui interviennent dans le processus de transmission de marqueurs techniques aux opérateurs de communications électroniques et d'exploitation des données ainsi collectées. Une telle suppression semble en effet de nature à diminuer la confiance des citoyens vis-à-vis de ce type de mesures de lutte contre les cyberattaques.

Enfin, eu égard au volume de données potentiellement capturé, il semble complexe, voire impossible, pour l'ANSSI de supprimer *« immédiatement »* les données finalement jugées inutiles pour la prévention et la caractérisation de la menace. À ce titre, il pourrait être utile de préciser un délai raisonnable de suppression de ces données par l'ANSSI. Une telle précision, outre qu'elle paraît plus réaliste, permettrait de clarifier les conditions dans lesquelles la formation RDPI exercera son contrôle.

⁂

S'agissant de la mise en œuvre de ces dispositions et compte tenu de leurs effets, potentiellement significatifs, sur l'exploitation des réseaux des opérateurs de communications électroniques et des

[5] Voir paragraphe 5 de la partie 2 du tome 1 du rapport public d'activité de l'Arcep, édition 2022 (https://www.arcep.fr/uploads/tx_gspublication/Arcep-RA2022-Tome1-marches-regules_juil2022.pdf, page 50).

autres systèmes impliqués, une concertation préalable avec l'ensemble des acteurs concernés semble constituer une étape préalable utile au déploiement efficace de ces dispositifs.

Il s'agirait notamment, au regard de l'ampleur des demandes de l'ANSSI et des modalités techniques de mise en œuvre souhaitées, d'identifier et de caractériser les développements informatiques ou le déploiement de systèmes d'information qui pourraient, en pratique, se révéler nécessaires pour que les opérateurs, les hébergeurs, les exploitants de centre de données et les fournisseurs de systèmes de résolution de noms de domaine soient à même de répondre à l'ensemble des demandes. À ce titre, il conviendrait ainsi que les textes d'application de ces dispositions législatives prévoient des délais raisonnables de mise en œuvre.

Par ailleurs, afin d'éviter de faire peser une charge disproportionnée sur ces acteurs, les surcoûts identifiables et spécifiques des prestations assurées au titre du projet d'article 33 devraient faire l'objet d'une compensation, qui n'est pour l'heure pas prévue par le projet de texte.

Enfin, s'agissant de la possibilité décrite au projet d'article 35 que des services de l'État autres que l'ANSSI puissent, pour le compte de celle-ci, mettre en œuvre la collecte de données techniques des flux réseaux et des copies de serveurs, il conviendrait que des garanties, notamment procédurales, existent afin d'assurer que le sous-traitant de l'ANSSI ne fasse que collecter les données, sans en connaître le contenu, et que ce ou ces sous-traitant(s) soient soumis à une obligation d'assermentation telle qu'elle existe aujourd'hui pour les agents de l'ANSSI.

⁂

Sur un plan plus technique, le mécanisme introduit à l'article 32 du projet de loi vise, dans la pratique, à créer, afin de sécuriser le système de noms de domaine en cas de menace susceptible de porter atteinte à la sécurité nationale, une procédure de blocage par DNS sur décision administrative, procédure jusqu'à présent réservée à quelques cas (contenus terroristes, contenus pédopornographiques, etc.). Or, plusieurs dispositions prévoient déjà des obligations de blocage DNS par les fournisseurs d'accès à internet, selon divers dispositifs notamment liés à la loi n° 2004-575 du 21 juin 2004 modifiée pour la confiance dans l'économie numérique (LCEN). Il semble nécessaire de veiller à l'harmonisation des modalités de mise en œuvre de la technique de blocage DNS par les fournisseurs d'accès à internet pour procéder aux blocages de sites dans le cadre d'injonctions de l'autorité judiciaire ou administrative.

Il conviendra également que l'Arcep soit en mesure de s'assurer, pour ce qui concerne le règlement internet ouvert, que les opérateurs n'y dérogent que dans les cas limitativement définis par le règlement.

S'agissant en particulier du projet d'article 33, l'Arcep comprend que le périmètre et la nature des informations auxquelles les opérateurs et les fournisseurs de systèmes de résolution de noms de domaine sont tenus de donner accès seront précisés par décret. Toutefois, elle attire l'attention du Gouvernement sur le fait que, contrairement au cas des opérateurs de communications électroniques, aucun texte ne prévoit, à sa connaissance, l'obligation pour les fournisseurs de systèmes de résolution de noms de domaine de conserver certaines données techniques enregistrées temporairement par les serveurs de résolution DNS.

3.2 Sur les missions dévolues à l'Arcep

Les dispositions du projet de loi conduisent à augmenter significativement le périmètre et les activités de contrôle qu'exerce l'Arcep sur les opérations de l'ANSSI. Ce projet étend en effet 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 DNS, collecte des données de serveurs de résolution). Il demande par ailleurs à l'Arcep de produire des avis préalables au renouvellement d'un filtrage ou d'une redirection DNS, 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.

L'Autorité tient à souligner que la mise en œuvre de ce contrôle *a priori* constitue un changement complet de la nature du contrôle effectué, et que son organisation et son mode de fonctionnement ne lui permettent pas d'assurer une réactivité opérationnelle courte.

Elle souligne également qu'il n'appartient pas à l'Arcep d'évaluer la levée d'une menace, comme l'article 32 du projet de loi le prévoit, et qu'il conviendrait en conséquence que cette mission soit confiée à l'ANSSI.

En toute hypothèse, **l'Arcep attire très fortement l'attention du Gouvernement sur la nécessité,** du fait de l'extension du champ de ses missions de contrôle des actions de l'ANSSI et de la charge de travail, **de renforcer ses moyens, notamment humains, et de prévoir l'expertise adéquate**, sur ces sujets extrêmement spécialisés.

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 9 mars 2023,

La Présidente

Laure de LA RAUDIÈRE