Avis n° 2018-0101 de l'Autorité de régulation des communications électroniques et des postes en date du 30 janvier 2018 sur des dispositions relatives à la sécurité et à la défense des systèmes d'information dans le cadre projet de loi relatif à la programmation militaire pour les années 2019-2025

L'Autorité de régulation des communications électroniques et des postes, (ci-après « 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 « le règlement sur l'internet ouvert ») ;

Vu la directive 2002/21/CE du Parlement européen et du Conseil du 7 mars 2002 relative à un cadre règlementaire commun pour les réseaux et services de communications électroniques ;

Vu les lignes directrices de l'Organe des régulateurs européens des communications électroniques (ORECE) du 30 août 2016 pour la mise en œuvre par les régulateurs nationaux des règles européennes en matière de neutralité de l'internet ;

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. 34-1, L. 36-5, D. 98-5 et D. 99 ;

Vu la saisine pour avis du Secrétaire général de la défense et de la sécurité nationale en date du 18 janvier 2018, reçue le 22 janvier 2018,

Après en avoir délibéré le 30 janvier 2018, 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 CPCE prévoit que l'Autorité de régulation des communications électroniques et des postes 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 un courrier en date du 18 janvier 2018, 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 et à la défense des systèmes d'information dans le cadre d'une saisine rectificative au projet de loi relatif à la programmation militaire pour les années 2019-2025 et portant diverses dispositions intéressant la défense, et qui modifieraient le code des postes et des communications électroniques ainsi que le code de la défense.

L'Arcep note que l'objectif principal du projet de dispositions qui lui est soumis pour avis est de compléter le cadre juridique actuel en matière de sécurité et de défense des systèmes d'information

introduit par la loi n° 2013-1168 du 18 décembre 2013 relative à la programmation militaire pour les années 2014 à 2019 et portant diverses dispositions concernant la défense et la sécurité nationale.

Le dispositif juridique de cybersécurité actuellement en vigueur concerne les activités d'importance vitale pour le fonctionnement normal de la Nation, et impose aux opérateurs d'importance vitale (ci-après « OIV ») de mettre en œuvre les règles de sécurité nécessaires à la protection de leurs systèmes d'information et de déclarer les incidents affectant le fonctionnement de leurs systèmes[1].

L'Arcep relève que le présent projet vise à améliorer la protection des systèmes d'information contre les cybermenaces ainsi que renforcer les capacités nationales de détection, de caractérisation et de prévention des attaques informatiques, en impliquant l'ensemble des opérateurs de communications électroniques (ci-après « opérateurs ») et des fournisseurs de services de communication au public en ligne[2] (ci-après « FSCPL »), par les réseaux desquels peuvent transiter ces attaques.

Il consiste en deux mesures concernant des systèmes de détection des événements susceptibles d'affecter la sécurité des systèmes d'information. La première consistant principalement en la possibilité de mise en œuvre par les opérateurs de systèmes de détection sur leurs réseaux visant à l'identification de tels évènements ; la seconde, en la mise en œuvre et l'exploitation par l'autorité nationale de sécurité des systèmes d'information (ci-après « ANSSI ») de ses propres systèmes de détection sur le réseau des opérateurs ou sur le système d'information des FSCPL sous contrôle de l'Arcep.

S'agissant de la première mesure, l'article 19 *bis* du présent projet crée un article L. 34-1-1 dans le CPCE qui prévoit, pour les besoins de la sécurité et de la défense des systèmes d'information, la possibilité pour les opérateurs de mettre en œuvre sur leurs réseaux des systèmes de détection des événements susceptibles d'affecter la sécurité des systèmes d'information de leurs abonnés via la recherche de marqueurs techniques spécifiques caractérisant ces événements.

En outre, lorsque l'ANSSI a connaissance d'une menace susceptibles de concerner les systèmes d'information d'autorités publiques ou d'OIV, elle pourra demander aux opérateurs d'exploiter les marqueurs techniques qu'elle leur fournira aux fins de prévenir ladite menace. Dans ce cadre, lorsque des événements susceptibles d'affecter la sécurité de ces systèmes d'information seront détectés, les opérateurs devront en informer sans délai l'ANSSI.

Il prévoit également que, à la demande de l'ANSSI les opérateurs informent leurs abonnés de la vulnérabilité ou de l'atteinte de leurs systèmes d'information.

L'article 19 *ter* complète l'article L. 2321-3 du code de la défense en prévoyant que les agents habilités et assermentés de l'ANSSI peuvent obtenir les données techniques strictement nécessaires à l'analyse de cet événement, aux seules fins de caractériser la menace affectant la sécurité de ces systèmes et à l'exclusion de toute autre exploitation.

---

[1] L'article 22 de la loi n° 2013-1168 du 18 décembre 2013 a introduit des dispositions spécifiques relatives à la sécurité des systèmes d'information dans le code de la défense. L'article L. 1332-6-1 du code de la défense prévoit notamment que le Premier ministre fixe les règles de sécurité nécessaires à la protection des systèmes d'information des OIV et des opérateurs publics ou privés qui participent à ces systèmes, « *pour lesquels l'atteinte à la sécurité ou au fonctionnement risquerait de diminuer d'une façon importante le potentiel de guerre ou économique, la sécurité ou la capacité de survie de la Nation. Ces opérateurs sont tenus d'appliquer ces règles à leurs frais.*

[Ces règles] *peuvent notamment prescrire que les opérateurs mettent en œuvre des systèmes qualifiés de détection des événements susceptibles d'affecter la sécurité de leurs systèmes d'information*.[…] ».

[2] Les personnes mentionnées au 1° et au 2° de l'article 6 de la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique

S'agissant de la seconde mesure, l'article 19 *quater* du présent projet insère au code de la défense un article L. 2321-2-1 après l'article L. 2321-2 qui prévoit que lorsqu'elle a connaissance d'une menace susceptible de porter atteinte à la sécurité des systèmes d'information des autorités publiques ou des OIV, l'ANSSI peut mettre en œuvre sur le réseau d'un opérateur de communications électroniques « *un système de détection des seuls marqueurs techniques caractérisant des événements susceptibles d'affecter la sécurité des systèmes d'information* ». Il précise que « *ce système est mis en œuvre pour la durée et dans la mesure strictement nécessaires à la caractérisation de la menace* ».

Dans ce cadre, les agents de l'ANSSI seront autorisés, aux seules fins de caractériser la menace affectant les systèmes d'information des autorités ou des OIV à procéder au recueil et à l'analyse des données techniques pertinentes.

Enfin, l'article 19 quinquies intègre un nouvel alinéa à la suite du 9° de l'article L. 36-7 du CPCE et confie à l'Arcep la compétence de veiller au respect des conditions d'application de l'article L. 2321-2-1. En effet, cet article prévoit que l'Arcep « *est informée, par l'autorité nationale de sécurité des systèmes d'information, du champ et de la nature des mesures mises en œuvre sur le fondement de l'article L. 2321-2-1 du code de la défense. Dans le respect du secret de la défense nationale, elle dispose, à sa demande, d'un accès aux informations ou documents nécessaires pour s'assurer du respect des conditions d'application de cet article.* »

2 Observations de l'Arcep

À titre liminaire, l'Arcep tient à souligner que les mesures envisagées dans ce projet sont de nature à engendrer des impacts significatifs sur l'exploitation des réseaux des opérateurs de communications électroniques et considère qu'il conviendrait de se concerter préalablement avec les opérateurs concernés, en particulier sur l'ampleur des demandes de l'ANSSI et les modallités de leur mise en œuvre.

Par ailleurs, l'Arcep se concentrera, dans le présent avis – et conformément aux missions qui lui sont dévolues[3] – sur les aspects liés au projet de loi qui pourraient avoir un impact sur le bon fonctionnement des réseaux et des services de communications électroniques, le respect de la neutralité du net, le respect du secret des correspondances, et la sécurité juridique dont doivent bénéficier les opérateurs dans la mise en œuvre de leurs obligations légales.

Enfin, l'Arcep souhaite rappeler que les modalités de compensation des surcoûts spécifiques des prestations assurées par les opérateurs, à la demande de l'Etat, au titre de la cyber sécurité devront, le cas échéant, être prévues.

2.1 Sur le projet d'article 19 *bis*

La création de l'article L.34-1-1 du CPCE vise à permettre aux opérateurs de mettre en œuvre sur leurs propres réseaux des systèmes de détection « *des seuls marqueurs techniques caractérisant des événements susceptibles d'affecter la sécurité des systèmes d'information de leurs abonnés* ».

[3] Conformément à la loi, l'ARCEP doit veiller notamment au respect par les opérateurs de leurs obligations en matière de neutralité de l'internet, de qualité, de disponibilité, de sécurité et d'intégrité des réseaux et services de communications électroniques (voir notamment les articles L. 32-1 et L. 33-1 du CPCE). Elle doit également contrôler, en lien le cas échéant avec les autres services de l'Etat compétents, le respect par ces mêmes opérateurs de leurs obligations en ce qui concerne notamment la conservation des données de connexion (article L. 34-1 du CPCE), le secret des correspondances (article L. 32-3 du CPCE) et la mise en place des moyens nécessaires aux interceptions de correspondances (6° du II de l'article L. 32-1, e) du I de l'article L. 33-1 et article D. 98-7 du CPCE).

L'Arcep comprend que les systèmes de détection qui seraient installés sur les réseaux analysent *a minima* les données techniques de connexion et potentiellement le contenu des communications (correspondance privée et consultation de sites internet) pour y rechercher des marqueurs techniques spécifiques. Elle s'interroge donc sur le périmètre des informations auxquelles les opérateurs donneraient accès, le cas échéant, à ces systèmes de détection. L'Arcep s'interroge également sur le libre choix, laissé aux opérateurs, des marqueurs techniques à rechercher par ces systèmes de détection et estime qu'il conviendrait de s'assurer que ceux utilisés par les opérateurs visent à détecter, effectivement et exclusivement, des événements susceptibles d'affecter la sécurité. Par exemple, ces marqueurs techniques pourraient être répertoriés par les instances compétentes en la matière. Ces points mériteraient d'être précisés afin notamment de s'assurer de la proportionnalité de la mesure au regard de l'atteinte au respect de la vie privée et à la protection des données. En effet, la conservation des données qu'est susceptible d'impliquer le dispositif prévu par le projet de texte pose la question des garanties propres à assurer une conciliation équilibrée entre, d'une part, le droit au respect de la vie privée et, d'autre part, la prévention des atteintes à l'ordre public et la recherche des auteurs d'infractions[4].

L'Arcep souligne l'impact que pourrait également avoir une telle mesure sur le respect par les opérateurs du secret des correspondances prévu par l'article L. 32-3 du CPCE. Il conviendra de s'assurer que les opérateurs n'y dérogent que dans les cas limitativement définis par les textes[5].

Sur la conformité avec le règlement sur l'internet ouvert, l'Arcep comprend que, pour produire tous ses effets, le dispositif envisagé pourrait mener à terme à la mise en place de mesures de gestion de trafic pour bloquer des flux malveillants. Or, si les lignes directices de l'ORECE (ou BEREC selon son acronyme anglais) prévoient que la surveillance du trafic visant à détecter des menaces pour la sécurité, telle qu'elle est prévue par le présent projet, peut être mise en œuvre de manière continue, elles précisent également qu'une « *mesure réelle de gestion du trafic visant à préserver l'intégrité et la sécurité n'est activée que lorsque des menaces concrètes pour la sécurité sont activées* ». Il conviendra donc que l'Arcep soit en mesure de s'assurer du respect de ces dispositions[6].

Par ailleurs, l'Arcep estime qu'il serait utile de clarifier le champ d'application des dispositions prévues aux alinéas 2 et 3 du projet d'article L. 34-1-1.

Il conviendrait notamment de clarifier si l'alinéa 2 qui prévoit la possibilité pour l'ANSSI, lorsqu'elle a connaissance d'une menace susceptible de porter atteinte à la sécurité des systèmes d'information des autorités publiques et des OIV, de demander aux opérateurs d'exploiter les marqueurs techniques qu'elle leur fournit, s'applique uniquement aux opérateurs ayant choisi de mettre en œuvre les systèmes de détection mentionnés au 1er alinéa ou à l'ensemble des opérateurs de communications électroniques. Si cette mesure devait s'appliquer à l'ensemble des opérateurs, l'Autorité note que cela reviendrait *de facto* à imposer à tous les opérateurs sollicités par l'ANSSI de mettre en place un système de détection.

---

[4] Voir notamment : Conseil constitutionnel, décision n° 2015-713 DC du 23 juillet 2015, Loi relative au renseignement, décision n° 2015-715 DC du 5 août 2015, Loi pour la croissance, l'activité et l'égalité des chances économiques, décision n° 2017-646/647 QPC du 21 juillet 2017

La question de l'accès et de la conservation des données par les opérateurs fait par ailleurs l'objet d'une jurisprudence de la CJUE dite « Tele2 » du 21 décembre 2016 ; affaires jointes C-203/15 Tele2 Sverige AB et C-698/15 Secretary of State for the Home Department

[5] Le III de l'article L. 32-3 du CPCE prévoit que les dispositions sur le respect du secret des correspondances « ne font pas obstacle au traitement automatisé d'analyse, à des fins d'affichage, de tri ou d'acheminement des correspondances, ou de détection de contenus non sollicités ou de programmes informatiques malveillants, du contenu de la correspondance en ligne, de l'identité des correspondants ainsi que, le cas échéant, de l'intitulé ou des documents joints (…) »

[6] Article 3.3. b du règlement sur l'internet ouvert et § 85 et 87 des lignes directrices de l'ORECE pour la mise en œuvre par les régulateurs nationaux des règles européennes en matière de neutralité de l'internet

Il conviendrait de la même manière de préciser si l'obligation d'information des abonnés, sur demande de l'ANSSI, de la vulnérabilité ou de l'atteinte de leurs systèmes d'information prévue à l'alinéa 3 ne s'applique qu'aux alertes signalées par le système de détection, mis en œuvre en application du 1er alinéa du projet d'article L. 34-1-1 ou si elle s'impose à tous les opérateurs et concerne toutes les vulnérabilités et atteintes aux systèmes d'information dont l'ANSSI aurait connaissance et ce, quelle que soit la manière dont l'ANSSI en a eu connaissance.

Il conviendrait également de prévoir une obligation d'information de l'Arcep par les opérateurs de la mise en œuvre des systèmes de détection prévus au présent projet d'article.

Par ailleurs, l'exploitation des marqueurs techniques fournis par l'ANSSI et l'obligation d'information des abonnés sur demande de l'ANSSI pourraient, dans tous les cas, justifier la juste rémunération des opérateurs.

2.2 Sur le projet d'article 19 *ter*

Ce complément apporté à l'article L. 2321-1 du code de la défense accorde à l'ANSSI un droit d'accès aux données techniques des opérateurs dès lors qu'elles sont strictement nécessaires à l'analyse des événements affectant la sécurité des systèmes d'information d'une autorité publique ou d'un OIV.

L'Arcep rappelle que les opérateurs ne peuvent, à ce jour et conformément au VI de l'article L. 34-1 du CPCE, conserver et traiter que des données *« [portant] exclusivement sur l'identification des personnes utilisatrices des services fournis par les opérateurs, sur les caractéristiques techniques des communications assurées par ces derniers et sur la localisation des équipements terminaux. Elles ne peuvent en aucun cas porter sur le contenu des correspondances échangées ou des informations consultées, sous quelque forme que ce soit, dans le cadre de ces communications. »* Ces données sont limitativement énumérées par les textes. Si la conservation d'autres données devaient être demandée aux opérateurs, il conviendrait donc que le type de données et les modalités de leur conservation soient précisées par décret en Conseil d'État, notamment pour les raisons développées au point 2.1. De plus, les surcoûts identifiables et spécifiques des prestations assurées à ce titre par les opérateurs devraient faire l'objet d'une compensation.

2.3 Sur le projet d'article 19 *quater*

La création de l'article L. 2321-2-1 du code de la défense permet à l'ANSSI de mettre en œuvre son propre système de détection sur le réseau d'un opérateur de communications électroniques ou sur le système d'information d'un FSCPL dès lors qu'elle « a connaissance d'une menace susceptible de porter atteinte à la sécurité des systèmes d'information des autorités publiques ou des opérateurs mentionnés aux articles L. 1332-1 et L. 1332-2 du code de la défense ».

L'Arcep comprend que cette mesure préventive est destinée à détecter localement et temporairement les attaques à l'encontre d'autorités publiques ou d'OIV.

L'Arcep estime que la mise en œuvre de ces dispositifs de détection par l'ANSSI au cœur des réseaux des opérateurs n'est pas sans conséquences pour ces derniers ; elle est susceptible d'avoir un impact important en fonction notamment de la configuration de ces systèmes (nombre d'équipements à installer, spécifications techniques et interfaces, bonne interopérabilité des sondes avec les contraintes de fonctionnement des réseaux, les mesures de protection des équipements des opérateurs ainsi que de maintenance de ces dispositifs de détection). Si de telles mesures étaient mises en œuvre, il conviendrait de préciser les modalités d'intervention de l'ANSSI, en particulier sur les aspects procéduraux et de responsabilité.

De plus, l'Arcep rappelle que les modalités de juste rémunération des prestations assurées par les opérateurs à cet effet devraient également être prévues.

2.4 Sur le projet d'article 19 *quinquies*

Le projet prévoit l'insertion d'un nouvel alinéa à l'article L.36-7 du CPCE confiant à l'Arcep la compétence de veiller au respect des conditions d'application de l'article L. 2331-2-1 susmentionné.

Comme indiqué précédemment, il est nécessaire que l'Arcep puisse s'assurer de la compatibilité avec le règlement sur l'internet ouvert des éventuelles mesures de gestion du trafic que les opérateurs pourraient être amenés à prendre sur leurs réseaux – y compris suite à la mise en œuvre par l'ANSSI de son propre système de détection en application du projet d'article L. 2321-2-1 du code de la défense –, et notamment de la proportionnalité de la demande au regard de l'exception au traitement égal et non discriminatoire de tout le trafic pour préserver l'intégrité et la sûreté du réseau. A cet égard, il conviendrait que l'ANSSI informe l'Arcep sans délai de la mise en œuvre de telles mesures.

Par ailleurs, l'Arcep tient à souligner qu'en l'état actuel des textes il ne lui revient pas de contrôler les actions de l'ANSSI mises en œuvre sur les résaux des opérateurs. Si une telle mission devait lui être confiée par le législateur, il conviendrait de préciser les modalités de mise en oeuvre de ce contrôle, tant en précisant le champs de ce contrôle qu'en définissant une gouvernance adaptée.

En tout état de cause, l'Arcep attire très fortement l'attention du gouvernement sur la nécessité de prévoir les ressources et l'expertise adéquates, sur ces sujets extrêmement pointus, pour accomplir cette mission.

Enfin, la rédaction proposée ne définit pas l'objectif et les modalités du contrôle qui devra être mis en place, ni les conséquences en cas d'une constatation du non-respect des conditions d'application de l'article.

3 Conclusion

L'Arcep tient à souligner que les mesures envisagées impliquent la mise en œuvre de dispositifs d'analyse sur les réseaux des opérateurs de communications électroniques qui soulèvent notamment des questions concernant le respect du principe de neutralité de l'internet et leur impact technique et économique pour ces derniers. A cet égard, une concertation avec les opérateurs sur le dispositif envisagé apparaît indispensable.

En outre, l'Arcep rappelle qu'il est nécessaire qu'elle puisse s'assurer de la compatibilité avec le règlement sur l'internet ouvert des éventuelles mesures de gestion du trafic que les opérateurs pourraient être amenés à prendre sur leurs réseaux pour bloquer des flux malveillants.

Des précisions mériteraient par ailleurs d'être apportées, en particulier sur le type de données concernées par les mesures de détection mises en place par les opérateurs, les modalités d'intervention de l'ANSSI pour la mise en oeuvre de ses systèmes de détection, ainsi que, en tant que de besoin, sur les conditions de juste rémunération des opérateurs.

Enfin, s'agissant du projet de confier à l'Arcep un contrôle des mesures de détection mises en oeuvre à l'initiative de l'ANSSI, l'Arcep attire l'attention du gouvernement sur deux points : la nécessité, d'une part, de préciser les modalités de mise en oeuvre du contrôle de l'ANSSI par l'Arcep et, d'autre part, de prévoir les ressources et l'expertise adéquates pour accomplir cette mission.

Le présent avis sera transmis au Secrétaire général de la défense et de la sécurité nationale.

Fait à Paris, le 30 janvier 2018.

Le Président

Sébastien SORIANO