Avis n° 2024-1131
de l'Autorité de régulation des communications électroniques, des postes et de la distribution de la presse
en date du 23 mai 2024
sur le projet de loi relatif à la résilience des activités d'importance vitale, à la protection des infrastructures critiques, à la cybersécurité et à la résilience opérationnelle numérique du secteur financier

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

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

Vu la directive (UE) 2022/2555 du Parlement européen et du Conseil du 14 décembre 2022 concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union, modifiant le règlement (UE) n° 910/2014 et la directive (UE) 2018/1972, et abrogeant la directive (UE) 2016/1148 (directive SRI 2) ;

Vu la directive (UE) 2022/2556 du Parlement européen et du Conseil du 14 décembre 2022 modifiant les directives 2009/65/CE, 2009/138/CE, 2011/61/UE, 2013/36/UE, 2014/59/UE, 2014/65/UE, (UE) 2015/2366 et (UE) 2016/2341 en ce qui concerne la résilience opérationnelle numérique du secteur financier ;

Vu la directive (UE) 2022/2557 du Parlement européen et du Conseil du 14 décembre 2022 sur la résilience des entités critiques, et abrogeant la directive 2008/114/CE du Conseil ;

Vu le code des postes et des communications électroniques (ci-après « CPCE »), notamment ses articles L. 36-5, L. 39-1, L. 42-1, L. 97-2 ;

Vu le code de la défense ;

Vu le code de la recherche, notamment son article L. 331-2 ;

Vu la loi n° 2008-518 du 3 juin 2008 relative aux opérations spatiales ;

Vu la saisine pour avis du secrétaire général de la défense et de la sécurité nationale en date du 7 mai 2024 ;

Après en avoir délibéré le 23 mai 2024,

1 Contexte de la saisine

L'article L. 36-5 du code des postes et des communications électroniques (ci-après « CPCE ») 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 électronique en date du 7 mai 2024, le secrétaire général de la défense et de la sécurité nationale a sollicité l'avis de l'Arcep sur un projet de loi relatif à la résilience des activités d'importance vitale, à la protection des infrastructures critiques, à la cybersécurité et à la résilience opérationnelle numérique du secteur financier.

2 Rappel du cadre institué par la directive « NIS 2 » applicable aux acteurs régulés par l'Arcep

La directive (UE) 2022/2555 du Parlement européen et du Conseil du 14 décembre 2022, dite « NIS 2 », définit des mesures relatives à la cybersécurité dans l'ensemble de l'UE[1]. Succédant à la directive « NIS »[2], celle-ci élargit significativement le périmètre d'application (acteurs assujettis, systèmes concernés et obligations) des mesures de cybersécurité.

L'article 3 de cette directive a notamment pour objet d'introduire les concepts d'*entités essentielles* et d'*entités importantes* pour les aspects relatifs à la cybersécurité. Sont notamment qualifiées :

- d'entités essentielles, toutes les entités (entreprises, administrations, etc.) relevant des 11 secteurs d'activité *« hautement critiques »*[3] listés dans la directive qui sont au moins des entreprises de taille intermédiaire ou grande[4] au sens de la recommandation 2003/361/CE de la Commission européenne[5], ainsi que les opérateurs de communications électroniques qui sont au moins des entreprises de taille moyenne[6] au sens de cette même recommandation ;
- d'entités importantes, les entités relevant des 11 secteurs hautement critiques ou des 8 autres secteurs critiques[7] listés dans la directive, qui ne sont pas des entités essentielles et qui sont au moins des entreprises de taille moyenne, ainsi que les opérateurs de communications électroniques qui ne sont pas des entités essentielles.

Son article 7 impose en outre aux États membres d'adopter une stratégie nationale en matière de cybersécurité, qui *« détermine les objectifs stratégiques, les ressources nécessaires pour atteindre ces objectifs ainsi que les mesures politiques et réglementaires appropriées, ainsi que les mesures politiques et réglementaires appropriées en vue de parvenir à un niveau élevé de cybersécurité et de le maintenir ».* À cet égard, cet article prévoit un certain nombre d'éléments que doit comprendre cette stratégie nationale.

Son article 21 demande aux États membres de veiller à ce que, dans le cadre de cette stratégie nationale, les entités essentielles et importantes prennent des *« mesures techniques, opérationnelles et organisationnelles appropriées et proportionnées pour gérer les risques, qui menacent la sécurité des réseaux et des systèmes d'information que ces entités utilisent dans le cadre de leurs activités ou de la fourniture de leurs services, ainsi que pour éliminer ou réduire les conséquences que les incidents ont sur les destinataires de leurs services et sur d'autres services »*.

Pour ce qui concerne les secteurs régulés par l'Arcep, il est à noter :

- que les fournisseurs de réseaux de communications électroniques publics ou de services de communications électroniques accessibles au public font l'objet d'une règle spécifique. En effet, l'ensemble de ces opérateurs y compris les petites et microentreprises (qui sont qualifiées d'entités importantes) sont assujetis aux mesures de NIS 2 et, contrairement aux

[1] Directive (UE) 2022/2555 du Parlement européen et du Conseil du 14 décembre 2022 concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union, modifiant le règlement (UE) nº 910/2014 et la directive (UE) 2018/1972, et abrogeant la directive (UE) 2016/1148 (directive SRI 2).

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

[3] 11 secteurs hautement critiques : l'énergie, les transports, le secteur bancaire, les infrastructures des marchés financiers, la santé, l'eau potable, les eaux usées, les infrastructures numériques, la gestion des services informatiques, l'administration publique et l'espace.

[4] Au moins 250 employés, ou bien au moins 50 M€ de chiffre d'affaires annuels ou 43 M€ de bilan annuel.

[5] Recommandation 2003/361/CE de la Commission du 6 mai 2003 concernant la définition des micro, petites et moyennes entreprises.

[6] Au moins 50 employés, ou bien au moins 10 M€ de chiffre d'affaires annuels ou de bilan annuel.

[7] 8 secteurs critiques : les services postaux et de courrier, la gestion des déchets, la fabrication, production et distribution de produits chimiques, la production, transformation et distribution de denrées alimentaires, la fabrication, les fournisseurs numériques et les organisations de recherche.

entités essentielles et importantes des autres secteurs, auxquels le principe du « pays d'origine » s'applique, la directive prévoit que les opérateurs de communications électroniques sont *« considérés comme relevant de la compétence de l'État membre dans lequel ils fournissent leurs services »* ;

- que les fournisseurs de services d'informatique en nuage font partie du secteur hautement critique des infrastructures numériques, et seront donc, à l'exception des petites ou microentreprises, assujettis aux mesures en tant qu'entité essentielle ou importante ;
- que les entités du secteur des services postaux et de courrier sont des entités importantes si elles sont au moins de taille moyenne.

3 Présentation du projet de loi

Le projet de loi soumis à l'avis de l'Arcep est structuré en trois titres, chacun consacré notamment à la transposition d'une directive :

- Le titre I[er] (articles 1[er] à 3) contient notamment les dispositions qui transposent celles de la directive « **REC** » relative à la résilience des activités critiques[8]. Cette directive actualise le cadre européen applicable aux systèmes d'information et aux opérateurs d'importance vitale.
- Le titre II (articles 4 à 33) s'attache principalement à transposer la directive « **NIS 2** ». Il contient par ailleurs des dispositions spécifiquement consacrées aux communications électroniques qui ne sont pas liées à la transposition de la directive NIS 2 (chapitre V du titre II), notamment liées à l'accès aux fréquences et aux sanctions contre les auteurs de brouillages préjudiciables.
- Le titre III (articles 34 à 52) a pour objet de transposer la directive « **DORA** »[9] consacrée à la résilience opérationnelle numérique du secteur financier et qui, en complément du règlement du même nom, regroupe une série de dispositions techniques, visant à clarifier les obligations et à actualiser les références en droit interne de directives.

L'Arcep concentrera ses remarques sur les mesures s'appliquant de manière spécifique aux secteurs qu'elle régule, à savoir la transposition de la directive NIS 2, l'accès aux fréquences par les terminaux satellitaires terrestres et les sanctions contre les auteurs de brouillages préjudiciables.

⁂

Les articles 4 à 30 du projet de loi soumis à l'avis de l'Arcep ont notamment pour objet :

- de désigner l'ANSSI comme chargée de la mise en œuvre de la législation et de la politique du Gouvernement en matière de sécurité des systèmes d'information ;
- d'introduire dans le cadre français les notions d'entité essentielle et importante, de renvoyer à un décret en Conseil d'État la liste des secteurs d'activité hautement critiques et critiques, et de renvoyer à un texte réglementaire la définition des seuils d'effectifs, de chiffre d'affaires annuel et de total de bilan annuel des entités ;
- de préciser que notamment les entités essentielles et importantes doivent prendre des mesures garantissant, pour leurs réseaux et leurs systèmes d'information, un niveau de sécurité adapté et proportionné au risque existant, et renvoyer à un décret en Conseil d'État

[8] Directive (UE) 2022/2557 du Parlement européen et du Conseil du 14 décembre 2022 sur la résilience des entités critiques, et abrogeant la directive 2008/114/CE du Conseil

[9] Directive (UE) 2022/2556 du Parlement européen et du Conseil du 14 décembre 2022 modifiant les directives 2009/65/CE, 2009/138/CE, 2011/61/UE, 2013/36/UE, 2014/59/UE, 2014/65/UE, (UE) 2015/2366 et (UE) 2016/2341 en ce qui concerne la résilience opérationnelle numérique du secteur financier.

la *« nature des mesures de gestion des risques auxquelles doivent se conformer »* les entités essentielles et importantes, afin de respecter ces objectifs ;

- d'habiliter notamment des agents de l'ANSSI *« spécialement désignés et assermentés »* à rechercher et constater les manquements et infractions aux obligations prévues notamment par l'ensemble de ce projet de loi.

⁂

Les articles 31 à 33 du projet de loi soumis à l'avis de l'Arcep comprennent des mesures qui modifient le code des postes et des communications électroniques (CPCE), le code de la recherche et la loi sur les opérations spatiales (LOS). Elles ont notamment pour objet :

- de renforcer les sanctions pénales à certaines infractions d'atteinte aux fréquences, et notamment celles liées aux brouillages ;
- de subordonner à un avis conforme du CNES, délivré dans les conditions prévues par la loi n° 2008-518 du 3 juin 2008 relative aux opérations spatiales, la délivrance de toute autorisation d'utilisation de fréquences ayant pour objet l'exploitation sur le territoire national d'un réseau ouvert au public du service fixe ou mobile par satellite à destination des équipements terminaux des utilisateurs finals. Cet avis conforme n'est toutefois pas requis pour les systèmes satellitaires ayant fait l'objet d'un arrêté du ministre en charge de l'espace autorisant l'opération spatiale en application de ladite loi ;
- de préciser les conditions de déclaration par la France des assignations de fréquence relatives à un système satellitaire auprès de l'Union Internationale des Télécommunications (UIT) ainsi que les conditions d'attribution des autorisations d'exploitation d'une assignation de fréquence à un système satellitaire et les sanctions applicables en cas non-respect de ces conditions.

4 Observations de l'Arcep

4.1 Sur les dispositions de transposition de la directive NIS 2

À titre liminaire, l'Autorité tient à souligner qu'elle partage pleinement l'objectif de renforcement des mesures visant à assurer un niveau élevé de cybersécurité.

Le projet de loi soumis à l'avis de l'Arcep a pour objet d'élargir le périmètre des secteurs couverts par la directive NIS 2 et de renforcer les exigences en matière de sécurisation des systèmes d'information applicables aux entités concernées, notamment aux opérateurs de communications électroniques et aux fournisseurs de services postaux et de courrier. Aucun d'entre eux n'était intégré au périmètre de la directive NIS.

NIS 2 introduit une nouveauté importante : c'est désormais, par défaut, l'ensemble des systèmes d'information des entités essentielles ou importantes qui est soumis à des exigences de sécurité des systèmes d'information, et non uniquement les systèmes d'information essentiels. En pratique, il n'est pas exclu que certains acteurs nouvellement désignés entités essentielles ou importantes doivent mettre en œuvre des mesures de protection qui sont totalement nouvelles pour eux. Il en est de même pour les acteurs déjà opérateurs de services essentiels au titre de la directive précédente, qui devront étendre les mesures de gestion des risques à l'ensemble de leurs systèmes d'information.

En conséquence, il paraît nécessaire de prévoir une date d'entrée en vigueur de ces obligations qui donne aux acteurs un délai suffisant pour se mettre en conformité.

Par ailleurs, il convient de rappeler que certains acteurs sont susceptibles d'intervenir dans plusieurs secteurs d'activité couverts ou non par la directive, ou ont des activités dans plusieurs pays de l'Union européenne, voire en dehors. En conséquence, dans un souci de lisibilité et de sécurité juridique dont doivent pouvoir bénéficier les acteurs, l'Arcep invite le Gouvernement à veiller à ce que les critères de

prise en compte de la taille des entreprises qui seront considérées comme entités essentielles ou importantes, au regard de leurs différentes activités et de leur emprise géographique, soient suffisamment précisés.

Enfin, il est à noter que le cadre juridique introduit par la transposition de la directive NIS 2 s'ajoute à celui qui s'applique aux opérateurs d'importance vitale. L'Arcep invite le Gouvernement à s'assurer de la bonne articulation entre les obligations prévues par les dispositions du code de la défense pour les opérateurs d'importance vitale et celles prévues par le dispositif général de cybersécurité.

4.2 Sur les dispositions relatives à l'accès aux fréquences et aux sanctions contre les auteurs de brouillages préjudiciables

L'article 32 du projet de loi vise à conditionner au respect de prescriptions techniques prévues par la loi n° 2008-518 du 3 juin 2008 relative aux opérations spatiales (LOS)[10], les demandes d'attribution d'autorisation d'utilisation des fréquences satellitaires pour exploiter un réseau ouvert au public du service fixe ou mobile par satellite à destination des équipements terminaux des utilisateurs finals. À cet effet, lorsque la demande émane d'acteurs non soumis à cette loi, les autorisation de fréquences seront soumises à un avis conforme du CNES.

L'Arcep souscrit à cette démarche qui tend, dans un contexte de déploiement d'un nombre croissant de satellites – lequel peut engendrer des problématiques de pollution spatiale – à la prise en compte de l'objectif de protection de l'environnement. En effet, cette mesure permettra *in fine* de contribuer à prendre en compte les préoccupations environnementales liées aux systèmes satellitaires en soumettant les opérateurs satellitaires qui souhaitent fournir un réseau ouvert au public à destination des utilisateurs finals sur le marché français à des exigences techniques en matière d'utilisation durable de l'espace (par exemple, en matière de gestion des débris spatiaux).

L'Arcep rappelle que l'avis conforme du CNES devra être délivré en tenant compte des délais réglementaires d'instruction par l'Arcep des demandes d'autorisation d'utilisation de fréquences.

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 23 mai 2024,

La Présidente

Laure de LA RAUDIÈRE

[10] Pour rappel, cette loi subordonne à autorisation du ministre chargé de l'espace les opérations spatiales qu'entendent mettre en œuvre tout opérateur français ou tout opérateur non établi en France mais lançant un objet spatial depuis le sol français. Cette autorisation est conditionnée au respect d'un ensemble de contraintes techniques destinées à garantir la sécurité des personnes et des biens ainsi que la protection de la santé publique et de l'environnement. Le contrôle de la conformité technique des systèmes satellitaires que ces opérateurs souhaitent déployer est assuré par le Centre national d'études spatiales (CNES) qui remet un avis motivé au ministre chargé de l'espace conformément à l'article 3 du décret n°2009-643 du 9 juin 2009 relatif aux autorisations délivrées en application de la LOS.