

CONSEIL D'ETAT
Assemblée générale

Séance du 6 juin 2024

Section de l'administration
Section des finances

N° 408329

EXTRAIT DU REGISTRE
DES DÉLIBÉRATIONS

AVIS 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

1. Le Conseil d'Etat a été saisi le 7 mai 2024 d'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. Ce projet de loi a été modifié par une saisine rectificative reçue le 5 juin 2024. L'étude d'impact de ce projet de loi a été modifiée par une saisine rectificative reçue le 5 juin 2024.
2. Ce projet de loi, qui comprend cinq-deux articles, est organisé en trois titres respectivement intitulés « Résilience des activités d'importance vitale », « Cybersécurité » et « Résilience opérationnelle numérique du secteur financier ». Le titre I^{er}, divisé en trois chapitres est consacré à la transposition de la directive (UE) 2022/2557 du Parlement européen et du Conseil du 14 décembre 2022 sur la résilience des entités critiques (dite directive « REC »). Le titre II, divisé en cinq chapitres, a pour objet principal de transposer la directive (UE) 2022/2555 (dite directive « NIS2 ») 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. Le titre III, divisé en trois chapitres, a pour objet de transposer 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.
3. L'étude d'impact du projet de loi, dans sa dernière version reçue le 5 juin 2024, comporte, exposés dans l'ensemble avec clarté et précision, les éléments requis par l'article 8 de la loi organique n° 2009-403 du 15 avril 2009, pris pour l'application du troisième alinéa de l'article 39 de la Constitution.
4. Le Conseil d'Etat relève que le projet de loi a fait l'objet, ainsi qu'il le devait, de la consultation de l'Autorité de régulation des communications électroniques, des postes et de la distribution de la presse (ARCEP), du Comité consultatif de la législation et de la réglementation financières (CCLRF), de la Commission supérieure du numérique et des postes (CSNP) et du Conseil national d'évaluation des normes (CNEN).

5. S'agissant du congrès de la Nouvelle Calédonie et des assemblées territoriales de la Polynésie française, de Wallis-et-Futuna et de Saint-Pierre-et-Miquelon, dont l'avis a été sollicité par le Gouvernement, le Conseil d'Etat relève qu'à la date à laquelle il se prononce, le congrès de la Nouvelle-Calédonie n'a pas disposé du délai de quinze jours qui lui est imparti pour rendre son avis.

Toutefois, il observe que dans ces collectivités, le projet de loi se borne à rendre applicables, par des mentions expresses, certaines de ses dispositions relevant des domaines de compétence de l'Etat, sans prévoir de règles particulières touchant au fond du droit. Il prévoit, en outre, un mécanisme permettant d'étendre à ces quatre collectivités, qui constituent des pays et territoires d'outre-mer de l'Union européenne au sein desquels le droit européen n'est pas applicable de plein droit, certains règlements de l'Union. S'agissant en particulier du règlement 2022/2554/UE du Parlement européen et du Conseil du 14 décembre 2022 sur la résilience opérationnelle numérique du secteur financier, dit règlement « DORA », le projet de loi comporte une disposition donnant compétence au ministre chargé de l'économie pour fixer par arrêté ses conditions d'application dans ces collectivités, ainsi que celles de ses futurs actes modificatifs, actes d'exécution et actes délégués, tout en prévoyant que ces conditions devront être définies de telle sorte que les dispositions de ce règlement « y aient des effets identiques à ceux produits en France métropolitaine ».

Le Conseil d'Etat estime que cette disposition qui, tout en permettant en tant que de besoin l'introduction de « grilles de lecture » propres aux territoires concernés, n'autorise pas le ministre chargé de l'économie à adopter des règles matériellement différentes de celles applicables en métropole, ne peut être regardée, à la différence de dispositions dérogatoires au droit commun applicable en métropole (cf. Cons. const., 28 juil. 2016, n° 2016-733 DC, *Loi organique rénovant les modalités d'inscription sur les listes électorales des ressortissants d'un État membre de l'Union européenne autre que la France pour les élections municipales*, paragr. 7), comme une « disposition particulière » à ces collectivités au sens des règles régissant la consultation de leurs assemblées territoriales.

Il suit de là qu'en l'absence d'obligation de procéder à la consultation de ces assemblées, la circonstance que, à la date d'examen du texte par l'assemblée générale du Conseil d'Etat, le congrès de Nouvelle-Calédonie n'ait pas émis d'avis et que le délai de quinze jours qui lui est imparti pour se prononcer ne soit pas expiré ne fait pas obstacle, au regard des dispositions de l'article 90 de la loi organique n° 99-209 du 19 mars 1999 relative à la Nouvelle-Calédonie, à ce que le Conseil d'Etat se prononce sur ces dispositions.

6. Au-delà de ces remarques liminaires et outre de nombreuses améliorations de rédaction qu'il propose au Gouvernement de retenir, ce projet de loi appelle, de la part du Conseil d'Etat, les observations qui suivent.

Dispositions relatives à la résilience des activités d'importance vitale

7. La directive (UE) 2022/2557 du Parlement européen et du Conseil du 14 décembre 2022 sur la résilience des entités critiques, dite directive « REC », vise à renforcer, en fixant un standard européen minimum, la préparation et la réponse aux risques de toute nature auxquels sont exposées les entités des Etats membres fournissant des biens ou services nécessaires au fonctionnement du marché intérieur et, en particulier, leurs infrastructures, dans onze secteurs d'activité qu'elle énumère (énergie, transports, banque, marchés financiers, santé, eau potable, eaux résiduaires, numérique, administration publique, espace et alimentation). Elle prévoit à son article 26 que les dispositions nécessaires à sa transposition

devront être publiées au plus tard le 17 octobre 2024 en vue d'une application à compter du lendemain.

Pour procéder à sa transposition, le projet de loi met plusieurs obligations à la charge des opérateurs publics ou privés exerçant des activités « *d'importance vitale* », définies comme celles qui sont indispensables au fonctionnement de l'économie et de la société ainsi qu'à la défense ou à la sécurité de la Nation. Conformément à la directive, ces opérateurs, désignés comme « *opérateurs d'importance vitale* » (OIV) par l'autorité ministérielle, doivent ainsi élaborer une analyse de leurs risques et une analyse de leurs dépendances ainsi qu'un « *plan de résilience opérateur* » (PRO) détaillant, au vu de ces risques, les mesures destinées à assurer la continuité de leurs activités d'importance vitale et, pour chacun de leurs « *points d'importance vitale* » (PIV), un « *plan particulier de résilience* » (PPR) précisant notamment les mesures de protection (surveillance, conditions d'accès) mises en place. Les OIV devront en outre notifier à l'autorité administrative tout incident susceptible de compromettre leurs activités d'importance vitale. Par ailleurs, certains opérateurs seront identifiés comme « *entités critiques d'importance européenne particulière* » dans les conditions prévues par la directive et pourront notamment, à ce titre, faire l'objet d'une « *mission de conseil* » organisée par la Commission européenne.

Le projet de loi comporte les dispositions nécessaires au contrôle par des agents spécialement habilités du respect par les OIV de ces obligations. Il crée une commission des sanctions placée auprès du Premier ministre qui pourra, en cas de manquement, infliger des amendes administratives pouvant aller jusqu'à dix millions d'euros ou, lorsqu'il s'agit d'une entreprise, 2 % du chiffre d'affaires annuel mondial.

Sur le cadre de la transposition et le champ d'application

8. Le droit national comportant déjà un dispositif, issu de l'ordonnance n° 58-1371 du 29 décembre 1958 tendant à renforcer la protection des installations d'importance vitale et de la loi n° 2005-1550 du 12 décembre 2005, et aujourd'hui inscrit au code de la défense, qui poursuit des objectifs similaires à ceux de la directive (UE) 2022/2557 et prévoit des obligations de même nature pour les opérateurs, le choix que traduit le projet de loi consiste à modifier et compléter ce dispositif, dont l'économie générale est connue et maîtrisée par les opérateurs, dans la seule mesure nécessaire à la prise en compte des prescriptions de la directive.

En conséquence de ce choix, les termes employés par le projet de loi restent le plus souvent ceux du dispositif national actuel (opérateurs et installations « *d'importance vitale* ») et ne coïncident donc pas nécessairement avec ceux de la directive, qui retient ceux de « *entité critique* », « *infrastructure critique* » et « *service essentiel* ». Le Conseil d'Etat estime que cela ne soulève toutefois pas de difficulté, dès lors que le champ personnel et matériel retenu par le projet de loi inclut bien celui de la directive et que toutes les obligations qu'elle prévoit sont reprises.

S'agissant du champ d'application, le Conseil d'Etat note que si, selon les indications de l'étude d'impact, le nombre d'OIV concernés, qui est actuellement d'environ 300, n'augmentera pas significativement par l'effet de cette réforme, il inclura pour partie des opérateurs qui ne sont pas dans le champ de la directive mais relèvent des dispositions actuelles du droit national, tels les propriétaires ou exploitants d'établissements mentionnés à l'article L. 511-1 du code de l'environnement (installations classées pour la protection de l'environnement) ou comprenant une installation nucléaire de base mentionnée à l'article

L. 593-2 du même code, lorsque la destruction ou l'avarie d'une ou plusieurs installations de ces établissements peut présenter un danger d'une particulière gravité pour la population ou l'environnement.

Le Conseil d'Etat observe également, sans que cela appelle de sa part de remarque, que ne sont reprises par le projet de loi, en les adaptant le cas échéant, que les définitions figurant dans la directive qui sont nécessaires à la compréhension et à la bonne application du dispositif national révisé. Il suggère toutefois de compléter cette courte liste de définitions par celle de la notion de « résilience » telle que donnée par la directive, car, incluant la prévention et la protection, elle ne correspond pas à l'usage habituel de ce mot.

Sur le régime des sanctions

9. Le projet de loi exclut les collectivités territoriales, leurs groupements et leurs établissements publics administratifs du champ des OIV susceptibles de faire l'objet d'amendes administratives en cas de manquement aux obligations mises à leur charge. Il en résulte que la méconnaissance de ces obligations ne pourra pas, en ce qui les concerne, faire l'objet de sanctions.

S'il est vrai que, comme le fait valoir le Gouvernement, ces collectivités ne sont pas placées dans la même situation que les opérateurs privés en ce qui concerne les conditions de leur financement et leur capacité à absorber et répercuter des charges, cette différence de situation ne paraît pas pouvoir justifier une telle différence de traitement au regard de l'objet de la loi, qui est en l'espèce de faire en sorte que la sécurité et la continuité des activités d'importance vitale pour le pays soient assurées, quel que soit le statut de l'opérateur qui les exerce. Le Conseil d'Etat observe à cet égard que certaines activités d'importance vitale, telles que celles relatives à la fourniture d'eau potable, peuvent être assurées soit pas des opérateurs privés dans le cadre d'une concession, soit en régie par des collectivités territoriales.

Il considère, en outre, qu'une telle exemption ne serait pas compatible avec les termes de la directive (UE) 2022/2557, qui prévoit à son article 22 que les Etats membres « *déterminent le régime des sanctions applicables aux violations des dispositions nationales adoptées conformément à la présente directive et prennent toutes les mesures nécessaires pour assurer la mise en œuvre de ces sanctions* » qui « *doivent être effectives, proportionnées et dissuasives* ».

Dès lors, à défaut d'un dispositif d'effet équivalent à ces amendes administratives, permettant de garantir le respect par les collectivités territoriales de leurs obligations en qualité d'OIV, tel qu'un pouvoir de substitution exercé par l'Etat, le Conseil d'Etat estime que leur exclusion du champ des sanctions méconnaît à la fois le principe d'égalité et les objectifs de la directive et qu'en conséquence cette exclusion ne peut être admise.

Sur les règles relatives à la commande publique

10. Le projet de loi prévoit que ne sont pas soumis aux règles du code de la commande publique relatives à la publicité et à la mise en concurrence certains marchés publics et contrats de concession conclus par les OIV relevant de ce code.

Le Conseil d'Etat considère, comme il l'avait fait à propos de marchés portant sur les installations nucléaires (avis du 14 décembre 2023 sur un projet de loi relatif à l'organisation de la gouvernance de la sûreté nucléaire et de la radioprotection, n° 407671), que cette

dispense peut être admise au regard des directives 2014/24/UE et 2024/25 UE du 26 février 2014 relatives à la passation des marchés publics et des concessions, qui prévoient une exclusion de leur application pour des raisons de sécurité, notamment « *dans la mesure où la protection des intérêts essentiels de la sécurité d'un État membre ne peut être garantie par des mesures moins intrusives* », et de la jurisprudence de la Cour de justice de l'Union européenne faisant application de cette disposition (CJUE 7 septembre 2023, aff. C-601/21). Il estime cependant nécessaire, pour garantir sa conformité au droit de l'Union européenne, de retenir, en accord avec le Gouvernement, une définition plus resserrée du champ de cette dérogation, consistant à la limiter aux marchés et concessions concernant les structures, équipements, systèmes, matériels, composants ou logiciels nécessaires à la protection des infrastructures critiques ou dont le détournement de l'usage porterait atteinte aux intérêts essentiels de l'Etat.

Sur l'entrée en vigueur

11. Le Conseil d'Etat note que le projet de loi prévoit, pour l'élaboration de l'analyse des risques et de l'analyse des dépendances à l'égard des tiers, un délai de neuf mois à compter de la désignation de l'opérateur par l'autorité administrative en qualité d'OIV, et, pour l'élaboration du document dénommé « plan de résilience opérateur », un délai de dix mois à compter de cette même désignation. S'il n'est pas prévu de délai pour l'élaboration par les opérateurs du document dénommé « plan particulier de résilience » détaillant, pour chaque point d'importance vitale, les mesures de protection et de résilience, un tel plan doit nécessairement comporter les éléments résultant de l'analyse des risques menée par l'opérateur, pour laquelle est prévu le délai de neuf mois déjà mentionné. Le Conseil d'Etat relève par ailleurs que, s'agissant des OIV désignés comme tels au titre du dispositif actuel, qui n'ont pas à faire l'objet d'une nouvelle désignation, les obligations qui leur sont applicables restent celles prévues avant la date d'entrée en vigueur de la loi, et cela jusqu'à l'accomplissement des obligations prévues par celle-ci.

Le Conseil d'Etat estime, dans ces conditions, qu'alors même qu'il ne prévoit aucun différé d'entrée en vigueur pour les obligations nouvelles qu'il institue dans son titre I^{er}, le projet de loi ne méconnaît pas les exigences découlant du principe de sécurité juridique.

12. Au bénéfice des observations qui précèdent, et sous réserve de ce qui est indiqué au point 9, le Conseil d'Etat estime que le titre I^{er} du projet de loi assure la transposition fidèle et complète de la directive REC et ne soulève pas de difficulté d'ordre constitutionnel ou conventionnel.

Dispositions relatives à la cybersécurité

En ce qui concerne les dispositions relatives à la transposition de 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 (ci-après directive NIS2)

13. La directive NIS2 définit un nouveau cadre juridique visant à assurer un niveau commun sensiblement plus élevé de cybersécurité dans l'ensemble de l'Union afin d'améliorer le fonctionnement du marché intérieur. Elle remplace à cet effet la directive (UE) 2016/1148 du Parlement européen et du Conseil du 6 juillet 2016, dite NIS1, qu'elle abroge.

Ce nouveau cadre juridique comporte des exigences renforcées en matière de mesures de gestion des risques et de partage d'informations, élargit considérablement le périmètre des secteurs d'activités régulés et des entités concernées, dont le nombre pour la France passera d'environ 600 à 15 000, désormais classées en « entités essentielles » et « entités importantes » en fonction de leur criticité au regard de leur secteur d'activité ou du type de service qu'elles fournissent et de leur taille. Il élargit également le champ des systèmes d'information de ces entités soumis à ces exigences. Il prévoit de soumettre ces entités à des obligations tendant à assurer la sécurité des réseaux et systèmes d'information, par la mise en place de mesures de gestion des risques, à caractère technique, opérationnel et organisationnel, ainsi que par la notification des incidents et des vulnérabilités qui ont été détectées. Des obligations particulières sont prévues pour les offices et bureaux d'enregistrement des noms de domaine. Pour assurer le respect de l'ensemble de ces obligations, la directive NIS2 implique la mise en place d'une ou plusieurs autorités nationales dotées de larges pouvoirs de supervision, de contrôle et de sanction. Elle renforce également les échanges d'informations et la coopération au niveau de l'Union européenne.

La directive NIS2 prévoit à son article 41 que les dispositions nécessaires à sa transposition doivent être publiées au plus tard le 17 octobre 2024 en vue d'une application à compter du lendemain.

Sur le cadre de la transposition

14. Le Gouvernement fait le choix d'abroger le titre I^{er} de la loi n° 2018-133 du 26 février 2018 portant diverses dispositions d'adaptation au droit de l'Union européenne dans le domaine de la sécurité, par lequel a été transposée la directive NIS1, et de procéder à la transposition de la directive NIS2 dans les quatre premiers chapitres du titre II, non codifiés, du présent projet de loi.

Le Conseil d'Etat estime que, compte tenu de l'importance des changements qu'il y a lieu d'opérer, le remplacement complet des dispositions antérieures est justifié. Il observe en revanche que, du point de vue de l'accessibilité de la norme, il est dommage qu'il n'ait pas été prévu d'insérer cette législation dans le code de la défense, alors que ce code donne une acception large aux notions de défense et de sécurité nationale et comporte déjà des dispositions relatives à la sécurité des systèmes d'information.

Sur le champ d'application du dispositif

15. Le Conseil d'Etat relève que le projet de loi mobilise dans un sens extensif les possibilités d'options offertes par la directive, notamment en incluant dans le champ du dispositif des collectivités territoriales autres que les régions, à savoir tous les départements ainsi que les communes et groupements de communes de plus de trente mille habitants, et, s'agissant d'un dispositif de défense et de sécurité nationale, en le rendant applicable à toutes les collectivités d'outre-mer, y compris celles auxquelles la directive n'est pas applicable. Il soumet en outre à un régime proche les services régaliens entendus au sens large.

Ces choix, qui vont au-delà de ce qu'appelle strictement la transposition de la directive NIS2, trouvent leur justification dans la volonté du Gouvernement d'assurer en France un haut niveau de cybersécurité. Ils n'appellent pas plus de remarques de la part du Conseil d'Etat, qui s'est toutefois attaché, pour faciliter l'intelligibilité et donc la bonne application de la loi, et en accord avec le Gouvernement, à clarifier et à préciser les critères d'identification des

entités essentielles et importantes ; en effet, ces entités ne seront plus toutes désignées par l'autorité administrative mais, pour beaucoup d'entre elles, devront s'identifier elles-mêmes.

Au regard de ce champ très vaste, le projet de loi fait le choix, que n'impose pas la directive, de confier à une autorité unique le soin de piloter et coordonner la mise en œuvre de la politique du Gouvernement en matière de cybersécurité et, en particulier, d'assurer le contrôle des obligations mises à la charge des opérateurs. Cette autorité unique sera l'Agence nationale de la sécurité des systèmes d'information (ANSSI), service rattaché au Secrétariat général de la défense et de la sécurité nationale (SGDSN) et déjà chargé de la défense des systèmes d'information par l'article L. 2321-1 du code de la défense. Toutefois, dans la mesure où le projet de loi soumet à une partie des obligations qu'il prévoit en application de la directive NIS2 des services de l'Etat exerçant en matière de défense des activités appelant un traitement particulier, le Conseil d'Etat propose d'ajouter au projet de loi, en accord avec le Gouvernement, une disposition permettant au Premier ministre de désigner, pour ces activités, une autre autorité.

Sur les contrôles et les sanctions

16. Le Conseil d'Etat relève qu'en ce qui concerne le contrôle des obligations qu'il institue, le projet de loi transpose exactement, sans aller au-delà de ce qu'elle impose, l'ensemble des mesures prévues par la directive NIS2 : types de contrôles, mesures d'exécution, régime de sanctions et niveau des amendes administratives. Le projet de loi confie à la commission des sanctions créée au titre I^{er} dans le cadre de la transposition de la directive REC, dans une composition adaptée à la cybersécurité, le soin de prononcer ces sanctions.

S'agissant du régime des sanctions, le Conseil d'Etat considère que la possibilité ouverte par la directive d'aménager voire d'exempter les entités administratives des amendes administratives peut être mobilisée à l'égard des administrations de l'Etat et de ses établissements publics, dans la mesure où le Gouvernement dispose à leur égard d'autres moyens que ces amendes pour garantir le respect de leurs obligations. Il estime en revanche, pour les raisons déjà exposées au point 9, qu'il n'en va pas de même des collectivités territoriales et de leurs groupement et établissements, en l'absence de dispositif d'effet équivalent et qu'en conséquence cette exemption ne peut être admise.

Sur l'entrée en vigueur

17. Le Conseil d'Etat observe que le projet de loi ne comporte pas de dispositions transitoires ou d'entrée en vigueur différée alors qu'il impose à de nombreuses entités de nouvelles obligations. Or, même si les mesures les plus contraignantes qu'il prévoit ne pourront prendre effet qu'après publication des textes réglementaires d'application appelés par le projet de loi, la charge pour les entités qui devront s'identifier elles-mêmes et se mettre en conformité sera un défi pour nombre d'entre elles, ainsi que le soulignent les avis de l'ARCEP, du CNEN et de la CSNP, en termes financiers mais aussi de compétences à acquérir ou développer. Le Conseil d'Etat ne remet pas en cause ce choix, compte tenu tant de l'objectif du projet de loi, qui est de renforcer rapidement la cybersécurité face aux menaces croissantes et multiformes, que des exigences de la directive elle-même, qui prévoit ainsi qu'il a été dit une entrée en vigueur des dispositions prises pour sa transposition au plus tard le 18 octobre 2024. Il estime toutefois indispensable, dans ce contexte, un effort d'information et d'accompagnement soutenu et réactif de l'Etat au profit des entités concernées.

18. Au bénéfice des observations qui précèdent, et sous réserve de ce qui est indiqué au point 16, le Conseil d'Etat estime que les quatre premiers chapitres du titre II du projet de loi assurent la transposition fidèle et complète de la directive NIS2 et ne soulèvent pas de difficulté d'ordre constitutionnel ou conventionnel.

En ce qui concerne les demandes d'assignation de fréquence déposées par la France auprès de l'Union Internationale des Télécommunications

19. Le projet de loi modifie les conditions dans lesquelles un opérateur de systèmes satellitaires peut demander que l'Agence nationale des fréquences dépose, au nom de la France, une assignation de fréquence auprès de l'Union Internationale des Télécommunications (UIT), puis lui déclare qu'elle a autorisé cet opérateur à exploiter cette fréquence. Il prévoit, notamment, que l'autorisation d'exploiter une fréquence ne peut être octroyée qu'à une entité de droit français ou à un établissement immatriculé au registre du commerce et des sociétés en France.

Le Conseil d'Etat relève qu'une telle assignation prévoit non seulement la bande de fréquence utilisée par le système satellitaire mais aussi sa position en orbite, qui n'est pas régie par la directive (UE) 2018/1972 du Parlement européen et du Conseil du 11 décembre 2018 établissant le code des communications électroniques européen. En outre, elle est déposée au nom de la France auprès de l'UIT, en coordination avec les Etats identifiés comme pouvant être affectés par le système satellitaire proposé, et relève de la conduite des relations internationales. Enfin, une telle assignation ne porte que sur l'utilisation de fréquences par un système satellitaire, alors que son emploi ultérieur à des fins de fourniture de services de communications électroniques et la commercialisation de tels services sur le territoire de l'Union européenne ne présentent qu'un caractère hypothétique. Par suite, le Conseil d'Etat considère que sa déclaration par la France auprès de l'UIT ne peut être regardée comme portant, par elle-même, sur une activité de prestations de services sur le territoire de l'Union européenne.

Dans ces conditions, le Conseil d'Etat estime que l'obligation d'établissement prévue par le projet de loi pour exploiter une assignation de fréquence déposée par la France ne relève du champ ni de la directive du 11 décembre 2018 mentionnée ci-dessus ni de l'article 56 du traité sur le fonctionnement de l'Union européenne qui garantit la libre prestation de services.

Dispositions relatives à la résilience opérationnelle numérique du secteur financier

20. Le Conseil d'Etat relève que ces dispositions, très techniques, ont pour objet principal de transposer 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.

Cette directive vise à introduire, dans les huit directives qu'elle modifie, relatives à la réglementation des entités du secteur financier (établissements de crédit, assurances notamment), les mesures de coordination rendues nécessaires par l'intervention du règlement (UE) 2022/2554 du Parlement européen et du Conseil du 14 décembre 2022 sur la résilience opérationnelle numérique du secteur financier, dit règlement « DORA ».

Le Conseil d'Etat note que la transposition de ces dispositions de coordination conduit à ce que certaines dispositions nationales prévoient des obligations identiques à celles instituées

par le règlement « DORA », en les définissant par référence à ce dernier. Toutefois, cette situation résulte directement de la directive transposée, qui laisse subsister les dispositions des directives existantes tout en les complétant pour prévoir que les obligations qu'elles énoncent doivent être mises en œuvre conformément à ce règlement.

En outre, le Conseil d'Etat relève que les dispositions du projet de loi prévoient d'appliquer aux sociétés de financement les dispositions de la directive relatives aux établissements de crédit, alors que cette extension du champ de ces dispositions n'est pas requise par le droit de l'Union européenne. Il estime toutefois que leur application aux sociétés de financement se justifie au regard de l'objectif poursuivi, dans la mesure où ces sociétés sont confrontées aux mêmes risques en matière de sécurité des systèmes d'information. De plus, cette application lui apparaît cohérente avec les choix déjà effectués en matière de réglementation prudentielle, visant à traiter ces sociétés de la même manière que les établissements de crédit, bien qu'elles soient souvent de taille inférieure. Enfin, le Conseil d'Etat note que l'entrée en vigueur de la mesure est différée d'un an pour celles des sociétés de financement qui remplissent certaines conditions tenant à leur petite taille et au caractère non complexe des opérations qu'elles effectuent, prenant ainsi en compte leur spécificité.

Autres dispositions du projet de loi

Le projet de loi comporte d'autres dispositions qui ont pour objet :

- d'alléger le régime de contrôle des moyens et prestations de cryptologie ;
- de renforcer les sanctions pénales pour certaines infractions d'atteinte aux fréquences.

Ces dispositions n'appellent pas d'observations particulières de la part du Conseil d'Etat, sous réserve d'améliorations de rédaction qu'il suggère au Gouvernement de retenir.

Cet avis a été délibéré et adopté par l'assemblée générale du Conseil d'Etat dans sa séance du 6 juin 2024.