RÉPUBLIQUE FRANÇAISE

SÉNAT

COMMISSION
DES
AFFAIRES EUROPÉENNES

Paris, le 13 décembre 2023

AVIS POLITIQUE

Avis politique relatif à la proposition de règlement européen établissant des mesures destinées à renforcer la solidarité et les capacités dans l'Union afin de détecter les menaces et incidents de cybersécurité, de s'y préparer et d'y réagir COM(2023) 209 final

La commission des affaires européennes du Sénat,

Vu le traité sur l'Union européenne, en particulier son article 4,

Vu le traité sur le fonctionnement de l'Union européenne, en particulier ses articles 173 et 322,

Vu le règlement (UE) 182/2011 du Parlement européen et du Conseil du 16 février 2011 établissant les règles et principes généraux relatifs aux modalités de contrôle par les États membres de l'exercice des compétences d'exécution par la Commission,

Vu le règlement (UE) 2019/881 du Parlement européen et du Conseil du 17 avril 2019 relatif à l'ENISA (Agence de l'Union européenne pour la cybersécurité) et à la certification de cybersécurité des technologies de l'information et des communications, et abrogeant le règlement (UE) n° 526/2013 (règlement sur la cybersécurité),

Vu le règlement (UE) 2021/694 du Parlement européen et du Conseil du 29 avril 2021 établissant le programme pour une Europe numérique et abrogeant la décision (UE) 2015/2240,

Vu le règlement (UE) 2021/887 du Parlement européen et du Conseil du 20 mai 2021 établissant le Centre de compétences européen pour l'industrie, les technologies et la recherche en matière de cybersécurité et le Réseau de centres nationaux de coordination,

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 proposition de règlement du Parlement européen et du Conseil établissant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans les institutions, organes et organismes de l'Union COM(2022) 122 final,

Vu la proposition de règlement du Parlement européen et du Conseil concernant des exigences horizontales en matière de cybersécurité pour les produits comportant des éléments numériques et modifiant le règlement (UE) 2019/1020, COM(2022) 454 final,

Vu la proposition de règlement tendant à étendre le champ de la certification européenne de cybersécurité, COM(2023) 208 final,

Vu la proposition de règlement ayant pour objectif d'améliorer la solidarité européenne dans le domaine de la cybersécurité, COM(2023) 209 final,

Vu la communication du 18 avril 2023 annonçant la création d'une Académie européenne de cybersécurité, COM(2023) 207 final,

Vu l'avis 02/2023 du 5 octobre 2023 de la Cour des Comptes de l'Union européen sur une proposition de règlement du Parlement européen et du Conseil établissant des mesures destinées à renforcer la solidarité et les capacités dans l'Union afin de détecter les menaces et incidents de cybersécurité,

Vu la résolution européenne du Sénat n° 109 (2017-2018) du 26 mai 2018 sur la proposition de règlement du Parlement européen et du Conseil relatif à l'ENISA, Agence de l'Union européenne pour la cybersécurité, et abrogeant le règlement (UE)

n° 526/2013, et relatif à la certification des technologies de l'information et des communications en matière de cybersécurité (règlement sur la cybersécurité), COM(2017) 477 final,

Vu le rapport d'information n° 458 (2017-2018) de M. René DANESI et Mme Laurence HARRIBEY, au nom de la commission des affaires européennes du Sénat, intitulé la cybersécurité : un pilier robuste pour l'Europe numérique,

Vu la communication en date du 5 juillet 2023 de Mme Laurence HARRIBEY, sénatrice, devant la commission des affaires européennes du Sénat, sur la conformité au principe de subsidiarité de la proposition de règlement européen établissant des mesures pour renforcer la solidarité et les capacités dans l'Union européenne à détecter les menaces et les incidents liés à la cybersécurité, à s'y préparer et à y répondre COM(2023) 209,

Sur la proposition de règlement et ses objectifs

Considérant que la cybersécurité est un enjeu politique majeur d'autant plus fort que le recours au numérique est massif dans les sociétés contemporaines ;

Considérant en effet que l'une des conséquences du développement de la numérisation de l'économie et des sociétés européennes est la vulnérabilité croissante de l'Union européenne et de ses États membres à l'égard des cyberattaques ;

Considérant que, selon l'ENISA, la menace cyber pesant sur l'Union européenne est aujourd'hui substantielle, et que ce niveau s'est accru depuis le début de la guerre en Ukraine ;

Considérant que, pour la France, selon l'Agence nationale de la sécurité des systèmes d'information (ANSSI), les cyberattaques touchent particulièrement les administrations publiques, les établissements de santé, les PME-TPE, mais fragilisent également les démarches du quotidien de nos concitoyens ;

Considérant que ces menaces et ces attaques sont le fait, non seulement de « pirates » et de réseaux criminels mais également d'acteurs étatiques hostiles aux États membres de l'Union européenne désireux de fragiliser cette dernière ;

Considérant, par conséquent, que la coopération et l'entraide entre les États membres en matière de cybersécurité sont nécessaires et constituent un prérequis pour tendre vers un espace numérique sûr ;

Salue le fait que l'Union européenne a pris conscience de cette nécessité et a su se doter d'un cadre juridique solide et complet pour bâtir une architecture européenne de cybersécurité ;

Rappelle que cette architecture a été établie par le règlement (UE) 2019/881 du 17 avril 2019, qui a renforcé l'ENISA, et la directive (UE) 2022/2555 du 14 décembre 2022, dite SRI 2, qui, d'une part, a imposé des obligations de cybersécurité aux entités essentielles et, d'autre part, institué des organes opérationnels pour la coopération et l'échange d'informations ;

Prend acte du souhait de la Commission européenne de renforcer de nouveau cette architecture avec la présente proposition de règlement ; s'interroge sur l'opportunité de la présentation d'un nouveau texte européen modifiant les relations et les missions des acteurs de la cybersécurité seulement quatre mois après l'adoption définitive de la directive SRI 2 ; soutient néanmoins l'objectif de cette dernière en ce qu'elle traduit la volonté d'une coopération accrue et pérenne en matière de cybersécurité à l'échelle européenne ;

Sur l'absence d'analyse d'impact accompagnant la proposition et ses conséquences sur l'évaluation de la nécessité de la réforme

Déplore l'absence d'analyse d'impact accompagnant la proposition de règlement car cette absence fragilise la sincérité de la présentation de la Commission européenne, empêche l'estimation des financements nécessaires à la mise en œuvre de la réforme et rend difficile l'évaluation de la valeur ajoutée du dispositif envisagé ;

Sur le champ d'application du règlement proposé

Considérant que la rédaction des articles 1er et 2 de la proposition de règlement est ambiguë en ce qu'elle n'exclut pas

explicitement les domaines de la sécurité nationale et de la défense nationale de son champ d'application ;

Considérant en outre que l'article 1er, paragraphe 3, précité évoque une « responsabilité première » des États membres et non exclusive dans le domaine de la sécurité nationale ;

Rappelle que conformément aux traités, et en particulier, l'article 4 du traité sur l'Union européenne (TUE) qui stipule que « la sécurité nationale reste de la seule responsabilité de chaque État membre », la sécurité nationale et la défense nationale demeurent des domaines relevant de la compétence exclusive des États membres ; considère qu'il ne saurait être question d'inclure les États membres dans un dispositif d'échange massif et obligatoire d'informations avec un nombre étendu de partenaires, qui, paradoxalement, affaiblirait la cybersécurité de l'Union européenne ;

Invite la Commission européenne à s'assurer de la compatibilité des dispositions de la présente proposition avec celles de la directive SRI 2 ; et demande la reprise explicite, au sein de son article 1er, des paragraphes 6 et 7 de la directive SRI 2 précitée, afin de préciser, d'une part, que son dispositif serait « sans préjudice de la responsabilité des États membres en matière de sauvegarde de la sécurité nationale et de leur pouvoir de garantir d'autres fonctions essentielles de l'État, notamment celles qui ont pour objet d'assurer l'intégrité territoriale de l'État et de maintenir l'ordre public », et, d'autre part, qu'il ne s'appliquerait pas « aux entités de l'administration publique qui exercent leurs activités dans les domaines de la sécurité nationale, de la sécurité publique, de la défense ou de l'application des lois » ;

Sur le financement de la présente proposition de règlement

Considérant que le budget des actions de cybersécurité dans le cadre du programme pour une Europe numérique a été augmenté de 100 millions d'euros par une réaffectation des fonds, passant ainsi de 743 à 843 millions d'euros ;

Constate, comme le confirme l'avis 02/2023 rendu par la Cour des comptes de l'Union européenne, que l'information sur le financement de cette réforme est partielle et, en particulier, que la

proposition ne contient pas d'estimation du coût total escompté de l'établissement et de la mise en œuvre des mesures envisagées ; demande en conséquence, à la Commission européenne de faire toute la transparence sur ces coûts ;

Observe également que la Commission européenne souhaite pouvoir déroger au principe d'annualité budgétaire dans l'utilisation des fonds européens dédiés à ce dispositif ; incite la Commission européenne à limiter cette dérogation au principe d'annualité aux seules activités non planifiables, à savoir la réserve européenne de cybersécurité et l'assistance mutuelle, puisque ces dernières ne seraient mises en œuvre que pour faire face à des évènements imprévisibles ;

Rappelle la nécessité de financements pérennes, nationaux et européens, pour garantir l'efficacité de la coopération européenne dans le domaine de la cybersécurité ;

Regrette que la réorientation des fonds visant à financer le présent dispositif se fasse au détriment d'autres actions essentielles comme l'éducation digitale ou le programme Erasmus+, qui ont pour objectif de développer les compétences numériques de nos concitoyens et d'éviter « l'exclusion numérique » ;

Sur la création d'un « cyberbouclier » européen

Considérant que la cybermenace ne peut, par nature, être complètement contrée et que le « risque zéro » n'existe pas dans le domaine de la cybersécurité ;

Considérant que l'architecture européenne actuelle, résultant de la directive précitée SRI 2, comporte déjà de multiples acteurs chargés de la coordination politique, tels que le groupe de coopération européen, de la prévention et de la gestion des crises cyber, tels que le réseau EU-CyCLONe, et de la réponse aux incidents, tels que les centres de réponse aux incidents de sécurité informatique (CSIRT) ;

Considérant que la présente proposition prévoit la mise en place d'un « cyberbouclier » européen, infrastructure paneuropéenne qui serait constituée de centres opérationnels de sécurité (COS), nationaux et transfrontières, et devrait doter l'Union européenne de capacités avancées de détection, d'analyse et de traitement des données relatives aux cybermenaces ;

Considérant que chaque État membre devrait mettre en place un organisme public dénommé COS national, qui aurait une double fonction de « radar » pour détecter en amont les incidents de cybersécurité et de point de référence pour d'autres organisations publiques et privées au niveau national ;

Considérant que ces COS nationaux pourraient procéder à des acquisitions d'outils et d'infrastructures en matière de cybersécurité conjointement avec le Centre de compétences européen en matière de cybersécurité (CECC), et, à cette occasion, bénéficier d'une aide financière européenne couvrant jusqu'à 50 % des coûts d'acquisition et 50 % des coûts opérationnels ;

Considérant que trois États membres au moins, représentés par leurs COS nationaux, pourraient s'unir au sein d'un consortium d'hébergement pour former un COS transfrontière ;

Considérant que ces COS transfrontières, en cas d'acquisition conjointe avec le CECC, pourraient bénéficier d'aides financières d'un montant à hauteur de 75 % des coûts d'acquisition des outils et infrastructures et de 50 % des coûts opérationnels ;

Considérant que ces COS transfrontières seraient tenus d'échanger des informations pertinentes, y compris sur les vulnérabilités, les incidents évités, et les cybermenaces, non seulement entre eux mais également, « sans retard injustifié », avec le réseau des CSIRT, le réseau EU-CyCLONe et la Commission européenne, en cas d'information relative à un incident de cybersécurité majeur ;

Considérant qu'à défaut de rejoindre un COS transfrontière dans les deux ans, un COS national perdrait le bénéfice de toute aide européenne ;

Approuve la volonté exprimée par la Commission européenne d'améliorer la détection des cyberincidents et des cybermenaces au niveau européen ;

Estime que la notion de « cyberbouclier » est trompeuse et qu'il devrait lui être préférée celle, plus honnête, de « cybersentinelle » ;

Observe que la Cour des comptes de l'Union européenne, dans son avis 02/2023 précité, a indiqué que la présente proposition était de nature à « rendre plus complexe l'ensemble du paysage de l'Union européenne en matière de cybersécurité » et précisé qu'il existait un risque de « double emploi entre les centres opérationnels de sécurité (COS) et le réseau des CSIRT déjà en place » ;

Souligne également que l'appel de Nevers des ministres de l'Union européenne en charge des télécommunications, rendu public le 9 mars 2022 sous présidence française du Conseil de l'Union européenne (PFUE), a encouragé le renforcement de la coopération et de la solidarité européennes dans le domaine de la cybersécurité en s'appuyant sur les réseaux existants ;

Rappelle à cet égard la nécessité pour les collectivités territoriales comme pour les administrations et les entreprises d'anticiper les crises de cybersécurité en élaborant un plan de continuité des activités (PCA) ;

Estime enfin que l'architecture européenne de cybersécurité, pour être pleinement efficace, doit être compréhensible par tous les acteurs de la société, citoyens comme entreprises ;

Demande la préservation de l'architecture européenne de cybersécurité existante et le renforcement des organes de coopération déjà en place ;

Recommande en conséquence le retrait du dispositif des COS, dont la nécessité et la pertinence n'apparaissent pas évidentes, et l'intégration explicite des fonctions envisagées pour ces structures au sein des compétences des CSIRT ; insiste sur la pertinence de l'échelon régional pour la mission de réponse aux incidents informatiques confiée aux CSIRT ; souhaite le développement de la coopération entre CSIRT régionaux d'États membres frontaliers ;

S'interroge sur la pertinence de la présence systématique de la Commission européenne dans les échanges d'informations sensibles prévus par l'article 7 de la proposition, eu égard à son absence de compétence opérationnelle dans le domaine de la

cybersécurité et alors même qu'elle siège déjà en tant qu'observateur au sein du réseau EU-CyCLONe ;

Sur le mécanisme d'urgence

Considérant que la présente proposition prévoit l'institution d'un mécanisme d'urgence, composé à titre principal d'une réserve européenne de cybersécurité, appelée à intervenir en cas de crise, à la demande d'un État membre, sur décision de la Commission européenne, et en dernier recours ;

Considérant que la réserve européenne de cybersécurité pourrait également bénéficier, sur demande, aux pays tiers ayant désigné un point de contact unique et fourni des informations suffisantes sur leurs capacités et actions de cybersécurité ;

Considérant que la réserve européenne de cybersécurité serait constituée d'entreprises privées sélectionnées par appels d'offres en tant que fournisseurs de confiance, sous réserve que les intéressées remplissent des critères de compétence technique et de garantie de la confidentialité des données ;

Considérant que les entreprises intervenant dans le cadre de la réserve bénéficieraient d'un préfinancement destiné à garantir leur disponibilité en cas d'incident et que, en cas de non utilisation de ces fonds, ces derniers pourraient être réorientés vers des actions de préparation ;

Prend acte de ce mécanisme d'urgence fondé sur une alliance public/privé, qui s'inspire de l'organisation française de cybersécurité constituée autour de l'ANSSI ; constate néanmoins que ce modèle résulte d'une insuffisance des moyens dévolus aux autorités nationales compétentes en matière de cybersécurité ;

Prend note de la possibilité laissée à des entreprises extra-européennes d'intervenir au sein de la réserve européenne de cybersécurité dans les infrastructures critiques d'un État membre faisant face à une crise cyber ; relève que cette possibilité représente un risque non négligeable d'ingérence étrangère dans le fonctionnement de ces entités ; constate que l'instauration d'une telle possibilité répond à la dépendance actuelle de l'Union européenne ; observe que cette dépendance ne saurait subsister au regard de ses ambitions d'autonomie stratégique ;

Recommande par conséquent de n'inclure dans la réserve que des prestataires ayant leur siège social dans l'Union européenne, dans l'Espace économique européen ou dans un pays tiers associé à l'Union européenne et partie à l'accord sur les marchés publics de l'Organisation mondiale du commerce (OMC) ;

Appelle en conséquence l'Union européenne à soutenir les prestataires européens et à favoriser leur « montée en puissance », en vue d'assurer son autonomie stratégique ; demande en complément, une augmentation des ressources de l'ENISA par un plan de recrutement de cyber-experts européens ; ajoute que la France doit elle-même poursuivre le renforcement de ses capacités à prévenir les cyberattaques et à y répondre ;

Souhaite en outre que le dispositif envisagé impose aux États membres de fixer des sanctions effectives, proportionnées et dissuasives afin de punir le vol, la diffusion non autorisée d'informations confidentielles et l'espionnage qui pourraient découler de l'activation du mécanisme d'urgence ;

Constate que l'article 17 de la présente proposition prévoit que la réserve européenne de cybersécurité pourrait également intervenir dans un pays tiers associé à l'Union européenne, à la demande de ce pays et à condition que l'accord d'association signé entre les deux parties mentionne une telle intervention ; estime cependant nécessaire de préciser dans la présente proposition, les modalités d'intervention de la réserve en cas de demandes simultanées d'États membres et de pays tiers, en prévoyant en particulier une priorité pour les États membres puis, pour les pays tiers candidats à l'adhésion à l'Union européenne ;

Sur le mécanisme d'analyse des incidents de cybersécurité

Considérant que la proposition tend à confier à l'ENISA une mission d'analyse des incidents de cybersécurité, à la demande de la Commission européenne, du réseau EU-CyCLONe et du réseau des CSIRT ;

Approuve le principe d'un tel mécanisme qui favorise la coordination des organes mentionnés en les faisant bénéficier mutuellement de « retours d'expérience » sur les crises et en leur permettant d'en tirer des enseignements pour l'avenir ;

Remarque toutefois que la directive SRI 2 confie déjà une telle mission au réseau EU-CyCLONe et souhaite en conséquence une clarification de la rédaction du dispositif envisagé afin d'éviter les « doublons » ;

Souhaite confirmation de la pleine intégration des États membres à cette revue des incidents de cybersécurité effectuée par l'ENISA, via leur contribution à l'analyse des incidents et leur information sur les conclusions de cette analyse ;

Sur l'ampleur des renvois aux actes d'exécution

Relève que le recours aux actes d'exécution est prévu à l'article 291 du traité sur le fonctionnement de l'Union européenne (TFUE) ; souligne que ce recours est justifié quand il est nécessaire d'assurer des conditions uniformes d'exécution des actes juridiquement contraignants de l'Union européenne ; constate cependant, qu'en renvoyant à des actes d'exécution la fixation des types et du nombre de « services de réaction aux incidents » nécessaires pour activer la réserve de cybersécurité de l'Union européenne, jusqu'à celle des modalités d'attribution des services d'aide fournis par cette réserve, les articles 12 et 13 de la proposition confèrent à la Commission européenne des compétentes d'exécution abusives ;

Sur l'état de préparation des institutions européennes aux menaces de cybersécurité

Rappelle que la Cour des comptes de l'Union européenne constatait en 2022 que l'état de préparation des institutions européennes aux menaces de cybersécurité était « globalement insuffisant », insistant en particulier sur l'absence de lignes directrices et de protocoles opérationnels, ainsi que sur la rareté des formations délivrées à leurs personnels ;

Salue en conséquence l'adoption définitive de la proposition de règlement COM(2022) 122 final établissant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans les institutions, organes et organismes de l'Union européenne.