N° 79

SÉNAT

SESSION ORDINAIRE DE 2017-2018

Enregistré à la Présidence du Sénat le 9 novembre 2017

PROPOSITION DE RÉSOLUTION EUROPÉENNE

au nom de la commission des affaires européennes, en application de l'article 73 octies *du Règlement, portant avis motivé sur la conformité au principe de subsidiarité de la proposition de règlement 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,*

PRÉSENTÉE

Par M. René DANESI et Mme Laurence HARRIBEY,

Sénateurs

(Envoyée à la commission des affaires étrangères, de la défense et des forces armées.)

EXPOSÉ DES MOTIFS

Mesdames, Messieurs,

Lors de son discours sur l'état de l'Union le 13 septembre 2017, Jean-Claude Juncker, le président de la Commission européenne, a déclaré ; « *les cyberattaques sont parfois plus dangereuses pour la stabilité des démocraties et des économies que les fusils et les chars* » ; « *Les cyberattaques ne connaissent pas de frontières; elles n'épargnent personne* ». C'est pourquoi, le 19 septembre, la Commission a annoncé une série de mesures visant à renforcer la résilience de l'Union européenne dans le domaine de la cybersécurité.

Au centre de ces mesures, figure une proposition de règlement qui fait de l'Agence européenne chargée de la sécurité des réseaux et de l'information, l'ENISA, le pivot de la cybersécurité en Europe. Or, ce règlement n'est pas sans poser de difficultés au regard du principe de subsidiarité.

I - L'Union européenne en évolution constante face à l'enjeu grandissant de la cybersécurité

La Commission européenne dresse le constat qu'en 2016, il y a eu 4 000 attaques par *rançongiciel* par jour, soit une hausse de 300 % par rapport à 2015. Au total, c'est 80 % des entreprises européennes qui auraient été touchées par une cyberattaque en 2016. 2017 a apporté la preuve des difficultés à se protéger : au premier semestre, les virus *Wannacry* et *Petya* se sont propagés à l'échelle mondiale et ont causé des dégâts à de nombreuses entreprises ainsi qu'à des services publics. Plus récemment, les autorités estoniennes ont découvert une faille de sécurité sur la puce électronique des cartes d'identité de leurs citoyens. Celle-ci les oblige à retirer de la circulation près de 800 000 cartes, dans un pays dont la population est inférieure à 1 300 000 habitants.

Dans le même temps, on estime qu'il y aura près de 6 milliards d'appareils ménagers connectés à l'internet dans l'Union en 2020. Ils constitueront demain autant de sources de menaces nouvelles s'ils ne font pas l'objet d'une certification de sécurité satisfaisante.

Face à ces évolutions rapides et conséquentes, l'Union européenne s'adapte. La directive sur la sécurité des réseaux d'information, la directive SRI (ou NIS en anglais) devrait être transposée au début de 2018. Elle prévoit notamment que :

– chaque État membre doit se doter d'une agence spécialisée dans la cybersécurité, à l'image de l'Agence nationale pour la sécurité des systèmes d'information en France, l'ANSSI ;

– le renforcement par chaque État de la cybersécurité d'« opérateurs de services essentiels » au fonctionnement de l'économie et de la société – les administrations, mais aussi les grandes entreprises et celles travaillant dans des secteurs sensibles. Et ces opérateurs auront l'obligation de signaler les attaques dont ils sont victimes ;

– la participation volontaire à une coopération entre États membres ;

– l'adoption de règles européennes communes en matière de cybersécurité pour certains prestataires de services numériques dans des domaines comme l'informatique en nuage pour le stockage des données, les moteurs de recherche et les places de marché en ligne.

Présentant un embryon d'organisation européenne, ce texte s'appuie sur l'idée forte que chaque État doit se doter des moyens d'assurer sa cybersécurité afin de contribuer, par une coopération volontaire, au renforcement de la cybersécurité européenne. C'est un partage des rôles justifié, car la cybersécurité comporte des éléments de protection – de défense – de la sûreté nationale. Or, cette compétence ne peut, par nature, échoir à l'Union.

Parallèlement, près de la moitié des États membres ont mis en place un processus de certification de cybersécurité des produits et des services du numérique, sur la base de normes internationales communément admises et mutuellement reconnues. Il fonctionne selon un système *bottom up*, dans lequel, sans qu'elles y soient obligées, les entreprises viennent dans les pays dont le niveau de contrôle est le meilleur pour faire valider leurs produits et services. Le certificat qu'elles obtiennent ainsi est un gage supplémentaire

de la sécurité et donc de la qualité de leurs produits pour les consommateurs. De plus, la reconnaissance mutuelle des certificats par plusieurs États permet de vendre ces produits dans tous les pays signataires. Le système repose sur un niveau de sécurité élevé et un processus qui garantit qu'il est respecté, comprenant trois acteurs principaux : le fournisseur de produits ou de services, le laboratoire chargé d'étudier ces derniers et l'autorité qui certifie.

Il semble qu'en ce domaine, l'Europe connaisse une certaine avance sur le reste du monde. Des entreprises américaines et asiatiques font certifier leurs produits en Europe, car les standards y sont plus élevés. Une véritable expertise européenne de la certification de cybersécurité, qui est un atout dans la compétition économique mondiale, s'est développée depuis une vingtaine d'années. Et, au sein de l'Union, la France figure parmi les tous meilleurs avec l'Allemagne, notamment. Des entreprises comme Apple ou Siemens font certifier certains de leurs produits dans notre pays. L'ANSSI joue un rôle moteur dans ce processus et dispose à ses côtés d'un secteur privé performant.

Aussi, il convient de remarquer qu'en ce qui concerne la certification de sécurité informatique, l'avance de l'Europe est surtout due à l'exigence en termes de niveau de sécurité et à l'expertise développée au sein des États membres. La Commission européenne et l'ENISA n'ont, pour leur part, aucune expérience ni expertise en ce secteur.

II - La proposition de règlement sur la cybersécurité proposée par la Commission européenne

La proposition fixe cinq objectifs : développer les moyens et la préparation des États membres ; améliorer la coopération et la coordination entre les États membres et les institutions européennes ; accroître les moyens au niveau de l'Union pour compléter les actions des États membres en cas de crise transfrontalière ; davantage sensibiliser particuliers et entreprises aux questions de cybersécurité ; accroître globalement la transparence et l'assurance de la cybersécurité ; éviter la multiplication des systèmes de certification dans l'Union, ainsi que des exigences de sécurité et des critères d'évaluation dans les différents États membres.

Pour les mettre en œuvre, le texte présente deux grandes parties principales : la première porte sur l'ENISA, pour laquelle il

fixe les objectifs, les missions et l'organisation ; la seconde instaure un cadre européen pour la certification de cybersécurité des produits et services des technologies de l'information et de la communication.

A - Une ENISA réformée et plus opérationnelle

L'ENISA a été créée par un règlement de 2004 pour renforcer la sécurité des réseaux de l'information dans l'Union et assurer un niveau élevé de protection. Son rôle est limité, il consiste principalement à assister les États membres dans cette mission. Cela est dû au fait que la cybersécurité a des implications sur les questions de défense nationale et des intérêts stratégiques des États membres. L'Union ne peut avoir qu'un rôle complémentaire de l'action des États membres. Néanmoins, ce rôle n'est pas négligeable, car, par son soutien à l'amélioration des capacités des États membres, l'Union contribue pleinement à l'élévation générale du niveau de la cybersécurité en Europe.

L'ENISA est une agence aux moyens modestes, de seulement 80 salariés, et au mandat limité dans le temps, car il s'achèvera en juin 2020. Par conséquent, elle s'appuie beaucoup sur les experts de certains États membres. Elle fournit une expertise sur les questions de sécurité des réseaux, elle contribue à l'élaboration des politiques de l'Union en la matière et à leur mise en œuvre, elle aide les États par des formations, des recommandations ou des campagnes de sensibilisation comme le mois de la cybersécurité en Europe, elle coordonne et promeut la communauté de la sécurité des réseaux et de l'information.

La proposition de règlement propose d'aller au-delà du dispositif prévu par la directive SRI et de placer l'ENISA au cœur de la cybersécurité dans l'Union. Elle se verrait désormais dotée d'un mandat permanent, mais ses objectifs et missions seraient régulièrement mis à jour. En conséquence, ses moyens humains, financiers et matériels seraient augmentés. Son champ d'action serait étendu à de nouvelles missions liées au marché et à la certification de cybersécurité ainsi qu'à la normalisation et à l'assistance technique en cas d'incidents significatifs. Elle conserverait ses missions concernant, d'une part, l'élaboration et la mise en œuvre de la politique de l'Union européenne en matière de cybersécurité, et, d'autre part, le soutien au renforcement des capacités (moyens et compétences) des États membres, à la coopération opérationnelle et à la gestion des crises.

Plus particulièrement, l'ENISA pourrait mener des enquêtes techniques au sein des États membres, suite à la signalisation d'un incident de cybersécurité d'ampleur européenne, sur demande de certains États membres ou de la Commission. Elle pourrait également apporter une assistance technique à certains États membres en cas de cyberattaque, grâce à une équipe d'intervention, qui serait créée.

B - Un cadre européen unique pour la certification de cybersécurité des produits et services des technologies de l'information et de la communication

Face au paysage morcelé des certifications nationales, la Commission prévoit la mise en place d'un cadre de certification de cybersécurité unique dans l'Union. C'est l'ENISA, donc la Commission européenne, qui serait chargée de préparer et d'adopter les schémas européens de certification. Les États et leurs représentants, comme l'Agence nationale pour la sécurité des systèmes d'information en France, n'auraient tout au plus qu'un rôle consultatif.

Par conséquent, non seulement les systèmes nationaux de certification cesseraient de s'appliquer à partir de la date d'entrée en vigueur du nouveau système, mais, de plus, les États membres devraient s'abstenir d'instaurer de nouveaux systèmes nationaux de certification. *De facto*, cela interdirait aux États membres d'adopter des certificats plus protecteurs que les certificats européens.

Cette mesure s'appuierait sur un guichet unique à disposition des entreprises souhaitant faire certifier leurs produits : il leur suffirait d'obtenir un certificat dans un seul pays de l'Union et celui-ci sera valable dans tous les États membres. La Commission propose de créer trois niveaux d'assurance selon le type de produits (élémentaire, substantiel et élevé), sur la base de normes, de critères d'évaluation et de méthodes d'essai communs.

III - L'appréciation au regard du principe de subsidiarité

Alors que la plupart des États membres sont encore en train de transposer la directive SRI, la Commission européenne propose de franchir une nouvelle étape importante. C'est vrai sur le fond du texte et ça l'est également dans la forme, puisque on passe d'une directive à un règlement. Or, cela n'est pas sans poser de difficulté quant au principe de subsidiarité et quant aux prérogatives des États membres dans les nouveaux dispositifs envisagés.

Il est important de renforcer les capacités européennes en matière de cybersécurité. Et il est nécessaire de disposer d'un cadre européen unique de certification de sécurité pour les produits et services des technologies de l'information et de la communication, ainsi que pour les systèmes de cybersécurité. Toutefois, il s'agit de deux sujets de natures différentes et rien ne justifie qu'ils fassent l'objet d'un seul et même règlement. La Commission se fonde uniquement sur le fait que l'ENISA est au centre du projet de certification qu'elle présente. Or cela est contestable comme il est démontré ci-après. Par conséquent, il serait préférable que les deux sujets fassent l'objet de deux textes distincts.

En outre, alors que la transposition de la directive SRI vise à augmenter les capacités opérationnelles des États membres en matière de cybersécurité, rien ne justifie, aujourd'hui, que l'ENISA dispose elle-même de telles capacités et se substitue aux États membres dans certaines missions. La cybersécurité c'est autant la sécurité des États que celle des entreprises. En outre, quand ces dernières relèvent de secteurs sensibles comme par exemple l'énergie, les transports ou le secteur bancaire, c'est bien de sécurité nationale dont il s'agit.

Or, l'article 4 du traité sur l'Union européenne énonce que l'Union « *respecte les fonctions essentielles de l'État, notamment celles qui ont pour objet d'assurer son intégrité territoriale, de maintenir l'ordre public et de sauvegarder la sécurité nationale. En particulier, la sécurité nationale reste de la seule responsabilité de chaque État membre* ». Il en découle que la Commission européenne ne peut se substituer aux États membres et qu'il n'y a aucune raison pour que l'ENISA dispose d'une équipe d'intervention et de pouvoirs d'enquête en cas de crise. Ces attributions relèvent des États membres et les mesures proposées ne respectent pas la subsidiarité.

En ce qui concerne la certification, l'ENISA et l'Union européenne n'ont actuellement ni la compétence ni l'expertise, qui sont au sein des États. Or, la Commission propose non seulement de placer l'ENISA au centre du système de certification unique, mais en plus de ne confier qu'un rôle consultatif aux États membres et aux autorités nationales de contrôle de certification. En outre, un système complètement nouveau et inconnu remplacerait des normes connues de tous et qui ont fait leurs preuves dans plusieurs États membres. Cela n'est pas justifié. Ce faisant, on va saper la confiance gagnée auprès des acteurs économiques au fil des années. La Commission serait mieux inspirée d'envisager une extension des normes reconnues par près de la moitié d'entre eux aux États membres qui ne les appliquent pas encore. De plus, pour les raisons exposées précédemment, les États membres ne peuvent être cantonnés à un rôle purement consultatif et ils doivent, ainsi que les autorités nationales de contrôle de certification, conserver leur légitime place au sein du futur processus de certification.

Par conséquent, la commission des affaires européennes a estimé que la proposition de règlement ne respecte pas le principe de subsidiarité. Elle a en ce sens, adopté, à l'unanimité, l'avis motivé suivant :

PROPOSITION DE RÉSOLUTION EUROPÉENNE PORTANT AVIS MOTIVÉ

① La proposition de règlement COM (2017) 477 final sur la cybersécurité vise à renforcer l'Agence européenne chargée de la sécurité des réseaux et de l'information (ENISA) et à établir un cadre européen de certification de cybersécurité des produits et services des technologies de l'information et de la communication.

② Elle fixe six objectifs :

③ – développer les moyens et la préparation des États membres ;

④ – améliorer la coopération et la coordination entre les États membres et les institutions européennes ;

⑤ – accroître les moyens au niveau de l'Union pour compléter les actions des États membres en cas de crise transfrontalière ;

⑥ – davantage sensibiliser particuliers et entreprises aux questions de cybersécurité ;

⑦ – accroître globalement la transparence et l'assurance de la cybersécurité ;

⑧ – éviter la multiplication des systèmes de certification dans l'Union, ainsi que des exigences de sécurité et des critères d'évaluation dans les différents États membres.

⑨ Pour atteindre ces objectifs, la Commission propose de renforcer l'ENISA et d'en faire l'acteur incontournable de la cybersécurité européenne, alors qu'elle est actuellement une agence aux moyens limités et dont le mandat doit s'achever en 2020.

⑩ L'ENISA serait dotée d'un mandat permanent. Son champ d'action serait étendu à de nouvelles missions liées au marché et à la certification de cybersécurité ainsi qu'à la normalisation et à l'assistance technique en cas d'incidents significatifs. Elle

conserverait ses missions concernant, d'une part, l'élaboration et la mise en œuvre de la politique de l'Union européenne en matière de cybersécurité, et, d'autre part, le soutien au renforcement des capacités (moyens et compétences) des États membres, à la coopération opérationnelle et à la gestion des crises.

⑪ L'ENISA serait donc pérennisée et verrait ses compétences grandement élargies. Elle pourrait notamment mener des enquêtes techniques au sein des États membres, suite à la signalisation d'un incident de cybersécurité d'ampleur européenne, sur demande de certains États membres ou de la Commission. Elle pourrait également apporter une assistance technique à certains États membres en cas de cyberattaque, grâce à une équipe d'intervention.

⑫ La proposition prévoit dans une seconde partie l'instauration d'un cadre unique de certification reflétant le niveau de sécurité des produits et services des technologies de l'information et de la communication dans l'Union européenne, dont l'ENISA serait l'autorité de référence. Un guichet unique permettrait aux entreprises de faire certifier leurs produits.

⑬ Alors qu'aujourd'hui la compétence et l'expertise en matière d'évaluation de sécurité se situent au niveau des États membres, la proposition octroie cette compétence à l'ENISA. En outre, dès lors qu'un schéma européen serait créé, tout certificat national se verrait supprimé et il ne serait plus possible à l'avenir d'en adopter un, alors même qu'il proposerait un niveau de sécurité plus élevé. Pour tous les produits et services, le cadre proposé prévoit trois niveaux d'assurance : élémentaire, substantiel et élevé.

⑭ Vu l'article 88-6 de la Constitution,

⑮ Le Sénat fait les observations suivantes :

⑯ – le Sénat soutient un renforcement des capacités européennes en matière de cybersécurité et la nécessité de disposer d'un cadre européen unique de certification de cybersécurité pour les produits et les services des technologies de l'information et de la communication, ainsi que pour les systèmes de cybersécurité ;

⑰ – cependant, il estime que ces deux sujets devraient faire l'objet de deux textes différents, l'un fixant le mandat de l'ENISA, l'autre établissant un cadre pour la certification ;

⑱ **Concernant les compétences des États en matière de sécurité :**

⑲ – le Sénat souligne que la cybersécurité, de par l'importance qu'elle revêt pour la sécurité des États membres, relève par plusieurs aspects de la souveraineté nationale ;

⑳ – par conséquent, les États membres doivent conserver, d'une part, leur faculté d'adopter des normes et des standards apportant un plus haut niveau de sécurité, et, d'autre part, toute leur place dans le nouveau dispositif européen, fondée sur leur participation volontaire à une cybersécurité européenne ;

㉑ – pour cette raison, concernant la base juridique de la proposition, il estime qu'un règlement sur la cybersécurité ne peut relever uniquement du fonctionnement du marché intérieur (articles 26 et 114 du traité sur le fonctionnement de l'Union européenne), mais qu'il doit aussi intégrer les enjeux de sécurité (article 4 du traité sur l'Union européenne) ;

㉒ **Concernant le mandat révisé de l'ENISA :**

㉓ – le Sénat estime que les États membres doivent tous disposer de capacités techniques et opérationnelles suffisantes en matière de cybersécurité et qu'il est bienvenu que l'ENISA les soutienne et les accompagne dans cette démarche. Cela implique que l'ENISA ne se substitue pas aux capacités opérationnelles des États membres et qu'elle ne dispose pas d'une équipe d'intervention en cas de crise, dont la création n'est pas justifiée ;

㉔ – le Sénat rappelle que la coopération européenne dans la cybersécurité doit continuer à se faire sur la base de la participation des États membres et de la transmission volontaire d'informations sensibles, voire relevant de la sécurité nationale et que, par conséquent, l'ENISA ne peut disposer de pouvoirs d'enquête tels que prévus à l'article 7, point 5 de la proposition de règlement ;

㉕ **Concernant la certification de cybersécurité :**

㉖ – le Sénat relève que la proposition de règlement place l'ENISA au cœur du processus de certification, alors que cette agence n'a aucune expertise en la matière ;

㉗ – il rappelle que l'action menée depuis plusieurs années par une majorité d'États membres, dont la France, a permis de faire de l'Europe une référence mondiale en termes de certification de cybersécurité ;

㉘ – pour ces raisons, le Sénat estime que la place prépondérante envisagée pour l'ENISA dans la certification de cybersécurité, alors qu'elle ne dispose d'aucune expertise, n'est pas justifiée et qu'elle pourrait entraîner un affaiblissement de la cybersécurité dans l'Union, ce qui est contraire à l'objectif de la proposition ;

㉙ – en outre, il convient que les États membres et les autorités nationales de contrôle de la certification conservent leur légitime place au sein du futur processus de certification européen et qu'ils ne soient pas cantonnés à un rôle uniquement consultatif ;

㉚ Pour ces raisons, le Sénat estime que la proposition de règlement COM (2017) 477 final ne respecte pas le principe de subsidiarité.