Avis du Comité économique et social européen sur la proposition de directive du Parlement européen et du Conseil concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union, abrogeant la directive (UE) 2016/1148

[COM(2020) 823 final — 2020/0359(COD)]

et sur la

proposition de directive du Parlement européen et du Conseil sur la résilience des entités critiques

[COM(2020) 829 final — 2020/0365(COD)]

(2021/C 286/28)

Rapporteur: **Maurizio MENSI**

Consultation	Parlement européen, 21.1.2021-11.2.2021
	Conseil, 26.1.2021-19.2.2021
Base juridique	Article 114 du traité sur le fonctionnement de l'Union européenne
Compétence	Section «Transports, énergie, infrastructures et société de l'information»
Adoption en section	14.4.2021
Adoption en session plénière	27.4.2021
Session plénière n°	560
Résultat du vote	
(pour/contre/abstentions)	243/0/5

1. **Conclusions et recommandations**

1.1. Le Comité économique et social européen (CESE) apprécie les efforts déployés par la Commission pour accroître la résilience des entités publiques et privées face aux incidents et menaces informatiques et physiques et convient de la nécessité de renforcer l'industrie et la capacité d'innovation de l'Union européenne de manière inclusive, selon une stratégie axée sur quatre piliers: la protection des données, les droits fondamentaux, la sécurité et la cybersécurité.

1.2. Toutefois, en ce qui concerne le choix de l'instrument, le CESE fait observer qu'un règlement aurait été préférable à une directive, eu égard à l'importance et à la complexité des objectifs poursuivis par les deux propositions. Par ailleurs, rien n'explique pourquoi la Commission n'évoque pas cette hypothèse, pas même parmi les diverses options envisagées.

1.3. Le CESE constate que certaines dispositions des deux propositions de directive se recoupent dans la mesure où ces dernières sont étroitement liées et complémentaires, l'une portant principalement sur la cybersécurité et l'autre sur la sécurité physique. Il demande donc d'évaluer l'opportunité d'une fusion des deux propositions en un seul texte, dans un souci de simplification et de concentration fonctionnelle.

1.4. Le CESE souscrit à l'approche proposée qui consiste à supprimer la distinction entre les opérateurs de services essentiels et les fournisseurs de services numériques prévue dans la directive SRI d'origine, mais souligne qu'il convient de fournir des indications plus précises et plus claires à propos du champ d'application, pour déterminer quelles sont les entités devant se conformer à la directive. En particulier, les critères de distinction entre entités «essentielles» et «importantes», ainsi que les exigences à respecter, doivent être définis plus précisément, afin d'éviter que des approches divergentes au niveau national n'entraînent des entraves à la concurrence et à la libre circulation des biens et des services, qui risqueraient de porter préjudice aux entreprises et de nuire aux échanges commerciaux.

1.5. Le CESE juge donc essentiel, eu égard à la complexité objective du système mis en place par les deux propositions, que la Commission clarifie avec précision le champ d'application des deux actes législatifs, en particulier lorsque les dispositions régissent des situations ou des entités identiques.

1.6. Le CESE fait observer que la clarté de toute disposition législative constitue un objectif incontournable, qui vient s'ajouter à la volonté de réduire les formalités administratives et la fragmentation en simplifiant les procédures, les exigences de sécurité et les obligations en matière de notification des incidents. C'est également la raison pour laquelle il pourrait être opportun, dans l'intérêt des citoyens et des entreprises, de fusionner les deux propositions de directive en un seul texte, de manière à éviter un exercice d'interprétation et d'application parfois compliqué.

1.7. Le CESE reconnaît le rôle crucial, souligné dans la proposition de directive, des organes de direction des entités «essentielles» et «importantes», dont les membres sont tenus de suivre régulièrement des formations spécifiques afin d'acquérir des connaissances et des compétences suffisantes pour appréhender et gérer les différents risques en matière de cybersécurité et évaluer leur incidence. À cet égard, il estime que la proposition devrait définir le contenu minimal de ces connaissances et compétences, de manière à fournir des orientations au niveau européen sur les compétences de formation jugées appropriées et à éviter que le contenu des formations ne diffère d'un pays à l'autre.

1.8. Le CESE approuve le rôle important conféré à l'ENISA dans le cadre institutionnel et opérationnel global de cybersécurité au niveau européen. Il considère à ce propos que, outre le rapport bisannuel sur l'état de la cybersécurité dans l'Union, cet organe devrait publier en ligne des informations régulières et actualisées sur les incidents de cybersécurité, en plus des évaluations sectorielles, afin de fournir aux parties prenantes concernées par la directive SRI 2 un outil d'information supplémentaire utile pour leur permettre de mieux protéger leurs entreprises.

1.9. Le CESE soutient dès lors la proposition de confier à l'ENISA la mise en place d'un registre européen des vulnérabilités et estime que la communication de ces informations, en ce qui concerne les vulnérabilités et les incidents majeurs, devrait être obligatoire plutôt que volontaire, de manière à devenir un instrument utile également pour les entités adjudicatrices dans le cadre des procédures de passation de marchés au niveau européen, y compris en ce qui concerne les produits et technologies 5G.

2. **Observations générales**

2.1. Le 16 décembre 2020, la nouvelle stratégie de cybersécurité de l'Union a été présentée en même temps que deux propositions législatives, portant respectivement sur la révision de la directive (UE) 2016/1148 ([1]) concernant la sécurité des réseaux et des systèmes d'information (SRI 2) et sur une nouvelle directive relative à la résilience des entités critiques (REC). Cette stratégie, qui constitue un élément clé de la communication intitulée «Façonner l'avenir numérique de l'Europe» ([2]), du plan de relance pour l'Europe et de la stratégie de l'UE pour l'union de la sécurité, vise à renforcer la résilience collective de l'Europe face aux cybermenaces et à faire en sorte que tous les citoyens et toutes les entreprises puissent bénéficier pleinement de services et d'outils numériques sûrs et fiables.

2.2. Il y a lieu d'actualiser les mesures prises par l'Union pour protéger les services et infrastructures critiques contre les risques informatiques et physiques. Les risques de cybersécurité continuant d'évoluer à mesure que la numérisation et l'interconnexion augmentent, il est nécessaire de réviser le cadre réglementaire existant selon la logique de la stratégie de l'UE pour l'union de la sécurité, en surmontant la dichotomie entre «en ligne» et «hors ligne» et en délaissant l'approche fondée sur une compartimentation stricte.

2.3. Les deux propositions de directive couvrent un large éventail de domaines et s'attaquent aux risques actuels et futurs, en ligne et hors ligne, découlant des attaques informatiques et criminelles, des catastrophes naturelles et des autres incidents, et s'appuient également sur les enseignements tirés de la pandémie en cours, qui a montré que les sociétés et les économies qui dépendent de plus en plus du numérique sont vulnérables et exposées à des cybermenaces en constante évolution et toujours plus nombreuses, en particulier en ce qui concerne les groupes menacés d'exclusion sociale, comme les personnes handicapées. L'Union propose donc des mesures pour préserver un cyberespace mondial et ouvert, mais fondé sur des garanties solides en matière de sécurité, de souveraineté technologique et de leadership, et entend développer des capacités opérationnelles de prévention, de dissuasion et de réaction aux menaces éventuelles grâce à une coopération accrue, dans le respect des prérogatives des États membres en matière de sécurité nationale.

3. **Proposition de révision de la directive sur la sécurité des réseaux et des systèmes d'information**

3.1. La directive (UE) 2016/1148 (ou «directive SRI»), premier instrument réglementaire «horizontal» de l'Union en matière de cybersécurité, visait à améliorer la résilience des réseaux et des systèmes d'information de l'Union face aux cyber-risques. Toutefois, malgré les bons résultats obtenus, la directive SRI a également montré certaines limites, alors que la transformation numérique de la société, intensifiée par la crise de la COVID-19, a étendu le paysage des menaces et accru la vulnérabilité de nos sociétés, de plus en plus interdépendantes face à des risques importants et imprévus. De nouveaux défis

([1]) JO L 194 du 19.7.2016, p. 1.
([2]) COM(2020) 67 final.

sont apparus, nécessitant des réponses adaptées et novatrices. La vaste consultation des parties prenantes a mis en évidence le niveau insuffisant de cybersécurité au sein des entreprises européennes, l'application incohérente des règles par les États membres dans les différents secteurs et le manque de compréhension des principaux enjeux et dangers.

3.2. La proposition SRI 2 est étroitement liée à deux autres initiatives: la proposition de règlement sur la finance numérique (l'*acte législatif sur la résilience opérationnelle numérique*, ou DORA) et la proposition de directive sur la résilience des entités critiques (REC), qui étend à de nouveaux secteurs le champ d'application de la directive 2008/114/CE ([3]), lequel se limitait à l'énergie et aux transports, en se concentrant par exemple sur le secteur de la santé et sur les entités exerçant des activités de recherche et de développement de médicaments. La proposition REC, dont le champ d'application couvre les mêmes secteurs que celui de la directive SRI 2 en ce qui concerne les entités essentielles (annexe I de la directive SRI 2), met l'accent non plus sur la protection des actifs physiques, mais sur la résilience des entités qui les exploitent, et porte sur le recensement des infrastructures critiques au niveau national plutôt que des infrastructures critiques européennes présentant une dimension transfrontière. La directive SRI 2 est également cohérente et complémentaire par rapport à d'autres instruments juridiques existants, tels que le code des communications électroniques européen, le règlement général sur la protection des données et le règlement eIDAS sur l'identification électronique et les services de confiance.

3.3. La proposition de directive SRI 2, conformément au programme pour une réglementation affûtée et performante (REFIT), a pour objectif de réduire les charges réglementaires pesant sur les autorités compétentes ainsi que les coûts de mise en conformité pour les entités publiques et privées, et modernise le cadre juridique de référence. Elle renforce également les exigences de sécurité imposées aux entreprises, traite de la sécurité des chaînes d'approvisionnement, rationalise les exigences en matière de déclaration, introduit des mesures de surveillance plus strictes pour les autorités nationales et vise à harmoniser les régimes de sanctions dans les États membres.

3.4. La directive SRI 2 contribue par ailleurs à accroître le partage d'informations et la coopération en matière de gestion des cybercrises aux niveaux national et européen. Elle abolit la distinction entre les opérateurs de services essentiels et les fournisseurs de services numériques prévue par la directive SRI. Son champ d'application englobe les entreprises de taille moyenne à grande dans les secteurs recensés sur la base de leur niveau de criticité pour l'économie et la société. Ces entités, publiques ou privées, sont classées en deux catégories — «entités essentielles» et «entités importantes» — soumises à des régimes de surveillance différents. Les États membres ont toutefois la possibilité de prendre également en considération des entités de plus petite taille présentant des profils de risque élevés.

3.5. Il est proposé de mettre en place un nouveau réseau de centres des opérations de sécurité axés sur l'intelligence artificielle à l'échelle de l'Union, qui constituera un véritable «bouclier de cybersécurité» capable de détecter les signaux d'une cyberattaque suffisamment à l'avance pour pouvoir intervenir avant que des dommages ne surviennent. L'importance de l'intelligence artificielle pour la cybersécurité est également soulignée dans le rapport qui a été présenté le 1er mars 2021 aux États-Unis par la commission nationale de sécurité sur l'intelligence artificielle (NSCAI). En conséquence, les États membres et les exploitants d'infrastructures critiques auront directement accès aux informations sur les menaces dans le cadre d'un réseau européen de sécurité, sous la forme de «renseignements sur les menaces» (*threat intelligence*).

3.6. La Commission aborde en outre le problème de la sécurité des chaînes d'approvisionnement et des rapports avec les fournisseurs: les États membres, en coopération avec la Commission et l'Agence de l'Union européenne pour la cybersécurité (ENISA), peuvent procéder à des évaluations coordonnées des risques inhérents aux chaînes d'approvisionnement critiques, en se fondant sur l'approche qui a fait ses preuves pour les réseaux 5G, prévue par la recommandation du 26 mars 2019 ([4]).

3.7. La proposition renforce et rationalise les obligations des entreprises en matière de sécurité et de communication d'informations, en imposant une approche commune de la gestion des risques, assortie d'une liste minimale des principaux éléments de sécurité à appliquer. Elle prévoit des dispositions plus précises en ce qui concerne la notification des incidents, le contenu des rapports et les délais. À cet égard, la proposition définit une approche en deux étapes: les entreprises sont tenues de présenter une première notification sommaire dans les 24 heures, suivie d'un rapport final détaillé au maximum un mois plus tard.

([3]) JO L 345 du 23.12.2008, p. 75.
([4]) JO L 88 du 29.3.2019, p. 42.

3.8. Il est prévu que les États membres désignent des autorités nationales chargées de la gestion des crises, au moyen de plans spécifiques, et qu'un nouveau réseau de coopération opérationnelle, le «réseau européen Cyber Crisis Liaison Organisation Network» («UE-CyCLONe»), soit institué. Le rôle du groupe de coopération dans l'élaboration des décisions stratégiques est renforcé et un registre européen des vulnérabilités constatées, géré par l'ENISA, est créé; le partage d'informations et la coopération entre les autorités des États membres, y compris la coopération opérationnelle en matière de gestion des crises de cybersécurité, sont également intensifiés.

3.9. La proposition introduit des mesures de surveillance plus strictes pour les autorités nationales, ainsi que des exigences plus sévères en matière d'application de la législation, et vise à harmoniser les régimes de sanctions entre les États membres.

3.10. À cet égard, la proposition de directive établit une liste de sanctions administratives pour violation des obligations de gestion des risques et de notification en matière de cybersécurité. Elle prévoit des dispositions relatives à la responsabilité des personnes physiques qui exercent des fonctions de représentation ou de direction dans les sociétés relevant du champ d'application de la directive. Elle améliore à cette fin la manière dont l'Union prévient et gère les incidents et crises de cybersécurité majeurs et y réagit, grâce à des responsabilités claires, une planification adéquate et une coopération renforcée au niveau de l'Union.

3.11. La proposition permet aux États membres de suivre conjointement la mise en œuvre des règles de l'Union et de s'entraider en cas de problèmes transfrontières, d'établir un dialogue plus structuré avec le secteur privé, de coordonner la divulgation des vulnérabilités des logiciels et du matériel mis sur le marché intérieur, d'évaluer de manière coordonnée les risques et menaces pour la sécurité liés aux nouvelles technologies, comme c'est le cas pour la 5G.

4. **Proposition de directive sur la résilience des entités critiques**

4.1. L'Union a établi le programme européen de protection des infrastructures critiques (EPCIP) en 2006 et adopté, en 2008, la directive sur les infrastructures critiques européennes (ICE), qui s'applique aux secteurs de l'énergie et des transports. Tant la stratégie 2020-2025 de l'UE pour l'union de la sécurité ([5]) adoptée par la Commission européenne que le récent programme de lutte antiterroriste soulignent l'importance de garantir la résilience des infrastructures critiques face aux risques physiques et numériques. Toutefois, l'évaluation de la mise en œuvre de la directive ICE réalisée en 2019 ainsi que les conclusions de l'analyse d'impact de la proposition à l'examen montrent que les mesures européennes et nationales existantes n'apportent pas de garanties suffisantes quant à la capacité des opérateurs à faire face aux risques actuels. C'est pourquoi le Conseil et le Parlement ont invité la Commission à revoir l'approche actuelle en matière de protection des infrastructures critiques.

4.2. La stratégie de l'UE pour l'union de la sécurité, adoptée par la Commission le 24 juillet 2020, reconnaît l'interconnexion et l'interdépendance croissantes des infrastructures physiques et numériques, et souligne la nécessité d'une cohérence et d'une homogénéité accrues des directives ICE et SRI. Dans cette perspective, la proposition de directive sur la résilience des entités critiques, dont la portée objective est identique à celle de la directive SRI 2 relative aux entités essentielles, élargit le champ d'application initial de la directive 2008/114/CE sur les infrastructures critiques européennes, qui se limitait à l'énergie et aux transports, à d'autres secteurs — les services bancaires, les infrastructures de marchés financiers, la santé, l'eau potable, les eaux usées, les infrastructures numériques, l'administration publique et l'espace — et prévoit en outre des responsabilités claires, une planification adéquate et une coopération accrue. Il convient à cet égard de créer un cadre de référence pour tous les risques et de soutenir les États membres dans leurs efforts visant à s'assurer que les entités critiques soient en mesure de prévenir les incidents, d'y résister et d'en gérer les conséquences, indépendamment du fait que les risques découlent d'aléas naturels, d'accidents, de terrorisme, de menaces internes ou d'urgences de santé publique comme c'est le cas actuellement.

4.3. Tout État membre est tenu d'adopter une stratégie nationale pour garantir la résilience des entités critiques, de procéder régulièrement à des évaluations des risques et, sur cette base, de recenser les entités critiques. Les entités critiques doivent quant à elles procéder à des évaluations des risques, prendre les mesures techniques et organisationnelles appropriées pour accroître la résilience et signaler les incidents aux autorités nationales. Les entités qui fournissent des services à au moins un tiers des États membres ou dans au moins un tiers d'entre eux font l'objet d'une surveillance spécifique, qui comprend des missions d'assistance spécifiques organisées par la Commission.

4.4. La proposition de directive REC prévoit différentes formes de soutien aux États membres et aux entités critiques, notamment la fourniture d'une vue d'ensemble des risques au niveau de l'Union, l'élaboration de bonnes pratiques et de méthodologies, ainsi que des formations et des exercices visant à tester la résilience des entités critiques. Un groupe d'experts ad hoc est en outre créé dans le cadre de la coopération transfrontière: le groupe sur la résilience des entités critiques, chargé de faciliter la coopération stratégique et l'échange d'informations entre les États membres.

([5]) COM(2020) 605 final.

5. **Modifications préconisées pour la proposition législative à l'examen**

5.1. Le CESE apprécie les efforts déployés par la Commission pour accroître la résilience des entités publiques et privées face aux menaces informatiques et physiques. Cette démarche revêt une importance et un intérêt particuliers compte tenu de la transformation numérique rapide induite par la pandémie de COVID-19. Le CESE convient également de la nécessité, évoquée dans la communication «Façonner l'avenir numérique de l'Europe», que l'Union tire parti de l'ère numérique et renforce son industrie — notamment les petites et moyennes entreprises — et sa capacité d'innovation de manière inclusive, selon une stratégie axée sur quatre piliers: la protection des données, les droits fondamentaux, la sécurité et la cybersécurité, conditions préalables essentielles d'une société fondée sur les données.

5.2. Toutefois, à la lumière des résultats de l'analyse d'impact et de la consultation qui a précédé la proposition SRI 2, et étant donné qu'il a été souligné à plusieurs reprises, notamment dans la communication du 4 octobre 2017 sur la mise en œuvre de la directive SRI ([6]), qu'il y avait lieu d'éviter la fragmentation des règles adoptées au niveau national, le CESE relève que rien n'explique pourquoi la Commission ne propose pas l'adoption d'un règlement plutôt que d'une directive, pas même parmi les options envisagées.

5.3. Le CESE constate que certaines dispositions des deux propositions de directive se recoupent dans la mesure où ces dernières sont étroitement liées et complémentaires, l'une portant principalement sur la cybersécurité et l'autre sur la sécurité physique. Il convient par ailleurs de noter que les entités critiques visées par la directive REC relèvent des mêmes secteurs que les entités «essentielles» mentionnées dans la directive SRI 2 ([7]) et coïncident avec celles-ci. À cela s'ajoute le fait que toutes les entités critiques couvertes par la directive REC sont soumises aux obligations prévues par la directive SRI 2 en matière de cybersécurité. Pour assurer la connexion entre elles, les deux propositions prévoient également un certain nombre de clauses passerelles portant sur le renforcement de la coopération entre les autorités, l'échange d'informations sur les activités de surveillance, la notification, aux autorités compétentes désignées en vertu de la directive SRI 2, de l'identité des entités critiques recensées au titre de la directive REC, ainsi que l'organisation de réunions régulières entre les groupes de coopération respectifs, au moins une fois par an. Elles partagent également la même base juridique, à savoir l'article 114 du TFUE, tel qu'interprété, entre autres, par la Cour de justice de l'Union européenne dans son arrêt dans l'affaire C-58/08, Vodafone e.a., qui vise à la réalisation du marché intérieur par le rapprochement des règles nationales. Le Comité demande donc d'évaluer l'opportunité d'une fusion des deux propositions en un seul texte, dans un souci de simplification et de concentration fonctionnelle.

5.4. Le CESE souscrit à l'approche proposée qui consiste à supprimer la distinction entre les opérateurs de services essentiels et les fournisseurs de services numériques prévue dans la directive SRI d'origine, mais souligne qu'il convient de fournir des indications plus précises et plus claires à propos du champ d'application, pour déterminer quelles sont les entités devant se conformer à la directive. En effet, outre les éléments figurant aux annexes I et II, la directive SRI 2 fait référence à un certain nombre de critères hétérogènes, impliquant des évaluations qualitatives et quantitatives délicates susceptibles d'être effectuées différemment selon les États membres, ce qui risque de donner lieu à nouveau à la situation fragmentée que cette législation visait à éviter. Or, il importe de veiller à ce que des approches divergentes au niveau national n'entraînent pas des entraves à la concurrence et à la libre circulation des biens et des services, qui risqueraient de porter préjudice aux entreprises et de nuire aux échanges commerciaux.

5.5. La directive SRI 2 prévoit que les opérateurs critiques dans les domaines considérés comme «essentiels» au titre de la proposition à l'examen sont également soumis à des obligations générales d'amélioration de la résilience, axées plus particulièrement sur les risques non liés au cyberespace au sens de la directive REC. Toutefois, il est indiqué expressément dans cette dernière qu'elle ne s'applique pas aux matières couvertes par la directive SRI 2. En effet, la directive REC prévoit que, la cybersécurité étant suffisamment prise en compte par la directive SRI 2, les questions couvertes par cette dernière devraient être exclues du champ d'application de la directive REC, sans préjudice du régime spécial applicable aux entités du secteur des infrastructures numériques. La proposition de directive REC fait en outre observer que les entités appartenant au secteur des infrastructures numériques s'appuient essentiellement sur des réseaux et systèmes d'information et relèvent du champ d'application de la directive SRI 2, qui traite également de la sécurité physique de ces systèmes dans le cadre de leurs obligations en matière de gestion des risques liés à la cybersécurité et de notification. Dans le même temps, le texte précise qu'il n'est pas exclu que des dispositions spécifiques de la directive REC puissent leur être applicables.

5.6. Dans ce cadre complexe, le CESE juge donc essentiel que la Commission clarifie avec précision le champ d'application des deux actes législatifs, en particulier lorsque les dispositions régissent des situations ou des entités identiques.

5.7. La clarté de toute disposition législative, d'autant plus lorsqu'elle s'insère dans des textes aussi vastes et complexes que les propositions à l'examen, doit constituer un objectif incontournable à tous les niveaux, qui vient s'ajouter à la volonté de réduire les formalités administratives et la fragmentation en simplifiant les procédures, les exigences de sécurité et les obligations en matière de notification des incidents. Il convient également de veiller à ce que la multiplication des

([6]) COM(2017) 476 final.
([7]) JO L 194 du 19.7.2016, p. 1 [Annexe II].

organismes chargés de tâches spécifiques n'empêche pas de définir clairement leurs compétences et ne compromette pas les objectifs poursuivis. C'est pourquoi il pourrait être opportun, dans l'intérêt des citoyens et des entreprises, de fusionner les deux propositions de directive en un seul texte, de manière à éviter un exercice d'interprétation et d'application parfois compliqué.

5.8. En plusieurs endroits, la directive SRI 2 fait référence à des dispositions d'autres instruments juridiques, comme la directive (UE) 2018/1972 ([8]) établissant le code des communications électroniques européen, dont l'application est régie par le principe de spécialité. Certaines dispositions de cette directive sont expressément abrogées (articles 40 et 41), tandis que d'autres doivent s'appliquer selon le principe précité, sans qu'aucune précision ne soit donnée à cet égard. Le CESE espère que tout doute sera dissipé sur ce point, afin d'éviter les problèmes d'interprétation. Le CESE approuve également l'objectif de la Commission consistant à harmoniser le système des sanctions prévues en cas de non-respect des dispositions relatives à la gestion des risques, en améliorant le partage d'informations et la coopération au niveau de l'Union.

5.9. Le CESE reconnaît le rôle crucial, souligné dans la proposition de directive, que jouent les organes de direction des entités «essentielles» et «importantes» dans la stratégie de cybersécurité et la gestion des risques, étant donné qu'ils sont tenus d'approuver les mesures relatives aux risques, de superviser leur mise en œuvre et de réagir à tout non-respect des dispositions. À cet égard, il est prévu que les membres de ces organes suivront régulièrement des formations spécifiques afin d'acquérir des connaissances et des compétences suffisantes pour appréhender et gérer les différents risques en matière de cybersécurité et évaluer leur incidence. Le CESE estime cependant que la proposition devrait définir le contenu de ces connaissances et compétences, de manière à fournir des orientations au niveau européen sur les compétences de formation jugées appropriées pour satisfaire aux obligations prévues dans la proposition, et à éviter que les exigences et le contenu des formations ne diffèrent d'un pays à l'autre.

5.10. Le CESE approuve le rôle important conféré à l'ENISA dans le cadre institutionnel et opérationnel global de cybersécurité au niveau européen. Il considère à ce propos que, outre le rapport bisannuel sur l'état de la cybersécurité dans l'Union, cet organe devrait publier en ligne des informations actualisées sur les incidents de cybersécurité ainsi que des évaluations sectorielles, afin de fournir aux parties prenantes concernées par la directive SRI 2 un outil d'information utile pour leur permettre de mieux protéger leurs entreprises.

5.11. Le CESE partage le point de vue selon lequel l'accès en temps utile à des informations correctes relatives aux vulnérabilités touchant les produits et services informatiques contribue à une meilleure gestion des risques en matière de cybersécurité. À cet égard, les sources d'informations publiquement accessibles concernant les vulnérabilités sont des outils importants pour les autorités nationales compétentes, les CSIRT, les entreprises et les utilisateurs. Le CESE soutient dès lors la proposition de confier à l'ENISA la mise en place d'un registre des vulnérabilités dans lequel les entités essentielles et importantes et leurs fournisseurs peuvent communiquer des informations, afin que les utilisateurs puissent prendre les mesures d'atténuation appropriées. Il estime par ailleurs que la communication de ces informations, en ce qui concerne les vulnérabilités et les incidents majeurs, devrait être obligatoire plutôt que volontaire, de manière à devenir un instrument utile également pour les entités adjudicatrices dans le cadre des différentes procédures de passation de marchés au niveau européen, y compris en ce qui concerne les produits et technologies 5G. Un tel registre contiendrait alors des éléments utilisables lors de l'évaluation des offres, aux fins de la vérification de la qualité des offres et de la fiabilité des contractants européens et non européens, du point de vue de la sécurité des produits et services couverts par l'appel d'offres, conformément à la recommandation du 26 mars 2019 sur la cybersécurité des réseaux 5G. Il conviendrait également de garantir la mise à disposition, sans aucune forme de discrimination, des informations contenues dans ce registre.

Bruxelles, le 27 avril 2021.

La présidente
du Comité économique et social européen
Christa SCHWENG

([8]) JO L 321 du 17.12.2018, p. 36.