Conseil de
l'Union européenne

Bruxelles, le 26 novembre 2021
(OR. en)

14337/21

Dossier interinstitutionnel:
2020/0359(COD)

CODEC 1541
CSC 416
CSCI 147
CYBER 312
DATAPROTECT 269
JAI 1295
MI 891
TELECOM 435

NOTE

Origine:	Secrétariat général du Conseil
Destinataire:	Conseil
Nº doc. préc.:	9583/2/21, 11724/21
N° doc. Cion:	14150/20
Objet:	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 *- Orientation générale*

I. INTRODUCTION

1. Le 16 décembre 2020, la Commission a adopté la proposition de directive concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union (ci-après dénommée "directive SRI révisée" ou "directive SRI 2")[1], dans le but de remplacer l'actuelle directive sur la sécurité des réseaux et des systèmes d'information (ci-après dénommée "directive SRI")[2].

[1] 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

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

Cette proposition était l'une des mesures prévues dans la stratégie de cybersécurité de l'UE pour la décennie numérique[3] en vue de faire en sorte que les citoyens et les entreprises bénéficient de technologies numériques dignes de confiance.

2. La proposition est fondée sur l'article 114 du traité sur le fonctionnement de l'Union européenne (TFUE) et a pour objectif d'améliorer encore la résilience et les capacités de réaction aux incidents des entités publiques et privées, des autorités compétentes et de l'Union dans son ensemble.

3. Au Parlement européen, la commission de l'industrie, de la recherche et de l'énergie (ITRE) est compétente pour la proposition. Elle a adopté le rapport du rapporteur le 28 octobre 2021.

4. Le Comité économique et social européen a adopté son avis le 28 avril 2021.

5. Le 3 février 2021, le Comité des représentants permanents a décidé de consulter le Comité européen des régions sur la proposition[4]. À ce jour, le Comité européen des régions n'a pas rendu son avis.

6. Le Contrôleur européen de la protection des données a rendu son avis le 11 mars 2021[5].

7. Dans ses conclusions[6] du 22 mars 2021 sur la stratégie de cybersécurité de l'UE pour la décennie numérique, le Conseil a pris acte de la nouvelle proposition, qui s'appuie sur la directive SRI, et a réaffirmé son soutien au renforcement et à l'harmonisation des cadres nationaux de cybersécurité et à une coopération soutenue entre les États membres.

8. Dans ses conclusions des 21 et 22 octobre 2021, le Conseil européen a appelé à faire avancer les travaux sur la proposition de directive SRI révisée.

---

3 14133/20
4 5573/21
5 Avis 5/2021 sur la stratégie de cybersécurité et la directive SRI 2.0
6 6722/21

II. TRAVAUX AU SEIN DES INSTANCES PRÉPARATOIRES DU CONSEIL

9. Au Conseil, l'examen de la proposition est mené par le groupe horizontal "Questions liées au cyberespace" (ci-après dénommé "groupe horizontal"). L'examen de la proposition a débuté le 19 janvier, pendant la présidence portugaise, par une lecture attentive de l'ensemble de la proposition, permettant aux États membres de présenter leurs questions, de mettre en évidence leurs principales préoccupations et de recevoir de la Commission des explications détaillées sur les modifications apportées à la directive révisée.

10. Au cours de la présidence portugaise, le groupe horizontal a consacré 17 réunions à la présentation et à la lecture de l'ensemble de la proposition. Un rapport sur l'état d'avancement de la lecture a été présenté au Conseil TTE le 4 juin 2021.

11. Depuis lors, les travaux se sont poursuivis et intensifiés pendant la présidence slovène, l'objectif étant de dégager une orientation générale lors de la session du Conseil "Transports, télécommunications et énergie" du 3 décembre 2021. La présidence slovène a consacré 15 réunions à la révision de la proposition SRI 2 ainsi que de nombreuses discussions bilatérales à tous les niveaux.

12. Le groupe horizontal a axé ses travaux sur la refonte du texte de la proposition, dans un premier temps en ce qui concerne l'interaction entre la directive SRI 2 et la législation sectorielle et son son champ d'application, en particulier pour ce qui est de l'administration publique, les serveurs racines du DNS ainsi que la clause d'exclusion, et dans un second temps, entre autres, les évaluations par les pairs, la juridiction et l'assistance mutuelle, la divulgation coordonnée des vulnérabilités, les bases de données des noms de domaine et les données d'enregistrement, ainsi que la coopération internationale.

13. Une première proposition de compromis sur le texte de la proposition de directive a été présentée le 21 septembre 2021[7], sur la base des observations écrites et des documents officieux reçus des États membres, ainsi que des propositions de compromis préalables sur l'interaction entre la directive SRI 2 et la législation sectorielle ainsi que sur le champ d'application de la directive SRI 2.

---

7 12019/21

14. La dernière révision en date[8] de la proposition de compromis de la présidence a été examinée au niveau du groupe le 22 novembre 2021. Si, d'une manière générale, les délégations ont accueilli favorablement le texte de compromis, quelques-unes ont encore émis des réserves d'examen ou formulé des observations sur certaines parties de la proposition de compromis. Quelques remaniements techniques ont encore été suggérés dans certaines parties du texte.

III. SUR LE FOND

15. Sur la base des discussions menées au niveau du groupe, les points suivants ont été identifiés comme constituant les principales questions politiques:

a) Champ d'application (article 2)

Depuis le début des discussions sur la proposition SRI 2, la principale préoccupation exprimée par les États membres a concerné l'augmentation significative du nombre d'entités couvertes par la directive et, en particulier, l'introduction de la règle du plafond, en vertu de laquelle toutes les entreprises de taille moyenne et de grande taille actives dans les secteurs ou fournissant le type de services couverts par la directive SRI 2 relèvent de son champ d'application. Si la proposition de compromis maintient cette règle générale, elle contient des dispositions supplémentaires pour garantir la proportionnalité nécessaire, un niveau plus élevé de gestion des risques et des critères de criticité clairs pour déterminer les entités qui relèvent du champ d'application de la directive. En outre, la proposition de compromis contient des dispositions spécifiques sur la fixation des priorités pour le recours aux mesures de surveillance selon une approche fondée sur les risques.

[8] 12019/5/21 REV 5

b) Administration publique (article 2, paragraphe 2 bis)

L'inclusion de l'administration publique dans le champ d'application de la directive SRI 2 a fait l'objet d'un vif débat, étant donné que le secteur de l'administration publique est plus distinct que les autres secteurs couverts par la directive SRI 2. La présidence s'est efforcée d'adopter une approche équilibrée, qui tienne compte des spécificités des cadres nationaux de l'administration publique et qui garantisse aux États membres une certaine souplesse pour déterminer quelles sont les entités de l'administration publique qui relèvent du champ d'application de la directive SRI 2. Par conséquent, dans le texte de compromis, la directive SRI 2 s'applique aux entités de l'administration publique des pouvoirs publics centraux, les États membres pouvant décider qu'elle s'applique aussi aux entités de l'administration publique aux niveaux régional et local.

c) Clause d'exclusion (article 2, paragraphes 3 bis et 3 bis bis)

Les États membres ont souhaité clarifier davantage la clause d'exclusion en ce sens que la directive ne s'applique pas aux entités qui exercent principalement leurs activités dans les domaines de la défense, de la sécurité nationale, de la sécurité publique ou de l'application de la loi, ni aux activités concernant la sécurité ou la défense nationales. L'appareil judiciaire, les parlements et les banques centrales sont également exclus.

d) Interaction avec la législation sectorielle

Les États membres ont souligné la nécessité d'un alignement entre la directive SRI 2 et la législation sectorielle, notamment le règlement sur la résilience opérationnelle numérique du secteur financier et la directive sur la résilience des entités critiques. La directive SRI 2, qui devrait servir de référence pour une harmonisation minimale en matière de cybersécurité, contient un article spécifiquement consacré aux actes sectoriels de l'Union (article 2 ter). En ce qui concerne l'interaction avec la directive sur la résilience des entités critiques, la proposition de compromis assure une plus grande clarté quant à l'approche "tous risques". D'autres ajouts importants concernent les arrangements de coopération entre autorités compétentes au titre des actes juridiques concernés.

e) Apprentissage par les pairs (article 16)

À quelques exceptions près, les États membres se sont opposés à la mise en place par la Commission d'évaluations par les pairs obligatoires. Le compromis proposé offre des garanties pour que le nouveau mécanisme d'apprentissage par les pairs s'appuie sur la confiance mutuelle et soit un processus volontaire mis en œuvre par les États membres.

f) Compétence et territorialité (article 24) et assistance mutuelle (article 34)

Les États membres ont fait part de leurs préoccupations quant aux conséquences d'une compétence différenciée pour les entités du secteur des TIC, comme l'a proposé la Commission. Le texte de compromis a clarifié la compétence sur la base du type d'entités et renforcé les termes relatifs à l'assistance mutuelle.

g) Obligations concernant le signalement (article 20

À la suite des préoccupations exprimées par les États membres selon lesquelles cette procédure ferait peser une charge excessive sur les entités couvertes par la directive SRI 2 et entraînerait un excès de signalements, la communication obligatoire d'informations sur les cybermenaces importantes a été exclue dans le texte de compromis.

IV. CONCLUSION

16. Le 24 novembre 2021, le Comité des représentants permanents est parvenu à un accord sur le texte de compromis figurant en annexe et a décidé de le soumettre au Conseil "Transports, télécommunications et énergie" en vue de l'adoption d'une orientation générale.

17. Le Conseil est dès lors invité à approuver le texte de compromis présenté par la présidence qui figure en annexe et à adopter une orientation générale lors de sa session du 3 décembre 2021.

ANNEXE

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, modifiant le règlement (UE) n° 910/2014 ainsi que la directive (UE) 2018/1972, et abrogeant la directive (UE) 2016/1148

(Texte présentant de l'intérêt pour l'EEE)

LE PARLEMENT EUROPÉEN ET LE CONSEIL DE L'UNION EUROPÉENNE,

vu le traité sur le fonctionnement de l'Union européenne, et notamment son article 114,

vu la proposition de la Commission européenne,

après transmission du projet d'acte législatif aux parlements nationaux,

vu l'avis du Comité économique et social européen[9],

vu l'avis du Comité des régions[10],

statuant conformément à la procédure législative ordinaire,

[9] JO C du , p. .
[10] JO C du , p. .

considérant ce qui suit:

(1) La directive (UE) 2016/1148 du Parlement européen et du Conseil[11] avait pour objectif de créer des capacités en matière de cybersécurité dans toute l'Union, d'atténuer les menaces pesant sur les réseaux et les systèmes d'information servant à fournir des services essentiels dans des secteurs clés et d'assurer la continuité de ces services en cas d'incidents de cybersécurité, contribuant ainsi au fonctionnement efficace de l'économie et de la société de l'Union.

(2) Depuis l'entrée en vigueur de la directive (UE) 2016/1148, des progrès significatifs ont été réalisés concernant l'amélioration du niveau de cyber-résilience de l'Union. Le réexamen de cette directive a montré qu'elle avait joué le rôle de catalyseur dans l'approche institutionnelle et réglementaire de la cybersécurité dans l'Union, ouvrant la voie à une évolution importante des mentalités. Cette directive a veillé à ce que les cadres nationaux soient achevés en définissant des stratégies nationales en matière de […] **sécurité des réseaux et des systèmes d'information**, en créant des capacités nationales et en mettant en œuvre des mesures réglementaires couvrant les infrastructures et les acteurs essentiels recensés par chacun des États membres. Elle a également contribué à la coopération au niveau de l'Union par la création du groupe de coopération[12] et du réseau des centres de réponse aux incidents de sécurité informatique (ci-après le "réseau des CSIRT")[13]. En dépit de ces accomplissements, le réexamen de la directive (UE) 2016/1148 a montré que certaines insuffisances intrinsèques l'empêchaient de répondre efficacement aux défis actuels et émergents liés à la cybersécurité.

---

11 Directive (UE) 2016/1148 du Parlement européen et du Conseil du 6 juillet 2016 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union (JO L 194/1 du 19.7.2016, p. 1).

12 Article 11 de la directive (UE) 2016/1148.

13 Article 12 de la directive (UE) 2016/1148.

(3) Les réseaux et systèmes d'information sont devenus une caractéristique essentielle de la vie quotidienne en raison de la transformation numérique rapide et de l'interconnexion de la société, notamment dans le cadre des échanges transfrontières. Cette évolution a conduit à une expansion du paysage des menaces qui pèsent sur la cybersécurité et à l'émergence de nouveaux défis, qui nécessitent des réponses adaptées, coordonnées et novatrices dans tous les États membres. Le nombre, l'ampleur, la sophistication, la fréquence et les effets des incidents de cybersécurité ne cessent de croître et représentent une menace considérable pour le fonctionnement des réseaux et des systèmes d'information. En conséquence, les incidents de cybersécurité peuvent nuire à la poursuite des activités économiques sur le marché intérieur, entraîner des pertes financières importantes, entamer la confiance des utilisateurs et causer un préjudice majeur à l'économie et la société de l'Union. La préparation à la cybersécurité et l'effectivité de la cybersécurité sont dès lors plus importantes que jamais pour le bon fonctionnement du marché intérieur.

(4) La base juridique de la directive (UE) 2016/1148 était l'article 114 du traité sur le fonctionnement de l'Union européenne (TFUE), dont l'objectif est la création et le fonctionnement du marché intérieur par l'amélioration de mesures pour le rapprochement des règles nationales. Les exigences en matière de cybersécurité imposées aux entités fournissant des services ou des activités pertinentes d'un point de vue économique varient grandement d'un État membre à l'autre en ce qui concerne le type d'exigence, le niveau de précision et la méthode de surveillance: ces disparités entraînent des coûts supplémentaires et créent des difficultés pour les entreprises qui fournissent des biens ou des services en mode transfrontière. Les exigences imposées par un État membre et qui diffèrent des exigences imposées par un autre État membre, voire qui les contredisent, peuvent avoir une incidence considérable sur ces activités transfrontières.

De surcroît, il est probable qu'une conception ou une mise en œuvre sous-optimales des […] **mesures** de cybersécurité dans un État membre ait des répercussions sur le niveau de cybersécurité d'un autre État membre, notamment en raison des échanges transfrontières intenses. Le réexamen de la directive (UE) 2016/1148 a montré l'existence de fortes divergences dans sa mise en œuvre par les États membres, notamment eu égard à son champ d'application, dont la délimitation a dans une grande mesure été laissée à l'appréciation des États membres. La directive (UE) 2016/1148 laissait également un large pouvoir d'appréciation aux États membres en ce qui concerne la mise en œuvre des obligations qu'elle prévoyait en matière de sécurité et de signalement des incidents: partant, ces obligations ont été mises en œuvre de manières considérablement différentes au niveau national. Des divergences de mise en œuvre similaires ont été constatées s'agissant des dispositions de cette directive relatives à la surveillance et à l'application.

(5) L'ensemble de ces divergences donnent lieu à une fragmentation du marché intérieur et sont susceptibles de produire un effet nuisible sur le fonctionnement de celui-ci, affectant plus particulièrement la fourniture transfrontière de services et le niveau de cyber-résilience en raison de l'adoption de […] **mesures** différentes. La présente directive a pour objectif de supprimer ces divergences importantes entre les États membres, notamment en définissant des règles minimales concernant le fonctionnement d'un cadre réglementaire coordonné, en établissant des mécanismes permettant une coopération efficace entre les autorités compétentes de chaque État membre, en mettant à jour la liste des secteurs et activités soumis à des obligations en matière de cybersécurité, et en prévoyant des recours et des sanctions effectifs qui sont essentiels à l'application effective de ces obligations. Il convient, par conséquent, que la directive (UE) 2016/1148 soit abrogée et remplacée par la présente directive.

(6) […] **Les** États membres devraient pouvoir adopter les mesures nécessaires pour garantir la protection des intérêts essentiels de leur sécurité, assurer l'action publique et la sécurité publique et permettre la recherche, la détection et la poursuite d'infractions pénales […]. […] **La directive ne devrait pas s'appliquer à certaines entités publiques ou privées qui exercent leurs activités dans ces domaines. Elle ne devrait pas non plus s'appliquer aux activités que les entités mènent dans ces domaines. Par ailleurs**, aucun État membre n'est tenu de fournir des renseignements dont la divulgation serait contraire aux intérêts essentiels de sa sécurité intérieure. […] Les règles nationales […] **ou** de l'Union visant à protéger les informations classifiées, les accords de non-divulgation et les accords informels de non-divulgation, tels que le protocole d'échange d'information "Traffic Light Protocol"[14], sont pertinentes.

(6 bis) Le droit de l'Union relatif à la protection des données à caractère personnel et de la vie privée s'applique à tout traitement de données à caractère personnel au titre de la présente directive. En particulier, la présente directive est sans préjudice du règlement (UE) 2016/679 et de la directive 2002/58/CE du Parlement européen et du Conseil et, notamment, elle ne devrait donc pas affecter les missions et pouvoirs des autorités de contrôle indépendantes compétentes pour contrôler le respect du droit de l'Union applicable en matière de protection des données.

---

14 Le protocole "Traffic Light Protocol" permet à une personne partageant des informations d'indiquer à son public des limitations applicables à la diffusion plus large de ces informations. Il est utilisé par la quasi-totalité des communautés des CSIRT et par certains centres d'échange et d'analyse d'informations (ISAC).

(7) Avec l'abrogation de la directive (UE) 2016/1148, le champ d'application par secteur devrait être étendu à une plus grande partie de l'économie au regard des considérations exposées aux considérants 4 à 6. Les secteurs couverts par la directive (UE) 2016/1148 devraient dès lors être étendus pour assurer une couverture complète des secteurs et des services revêtant une importance cruciale pour les activités économiques et sociales essentielles au sein du marché intérieur. Les règles ne devraient pas être différentes selon que les entités sont des opérateurs de services essentiels ou des fournisseurs de services numériques: cette différenciation s'est avérée obsolète puisqu'elle ne reflète pas l'importance réelle des secteurs ou des services pour les activités économiques et sociales sur le marché intérieur.

(8) Conformément à la directive (UE) 2016/1148, les États membres étaient chargés de déterminer quelles entités remplissaient les critères établis pour être qualifiées d'opérateurs de services essentiels (ci-après le "processus d'identification"). Afin d'éliminer les divergences importantes entre les États membres à cet égard et de garantir la sécurité juridique concernant les exigences en matière de gestion des risques et les obligations de signalement pour toutes les entités concernées, il convient d'établir un critère uniforme déterminant les entités qui relèvent du champ d'application de la présente directive. Ce critère devrait consister en l'application de la règle du plafond, en vertu de laquelle toutes les entreprises de taille moyenne et de grande taille, au sens de la recommandation 2003/361/CE de la Commission[15], actives dans les secteurs ou fournissant le type de services couverts par la présente directive relèvent de son champ d'application.
[…]

[15] Recommandation 2003/361/CE de la Commission du 6 mai 2003 concernant la définition des micro, petites et moyennes entreprises (JO L 124 du 20.5.2003, p. 36).

(8 *bis*) Afin de garantir une vue d'ensemble claire des entités relevant du champ d'application de la présente directive, les États membres devraient pouvoir mettre en place des mécanismes nationaux d'autonotification, selon lesquels les entités relevant de la présente directive devraient communiquer, aux autorités compétentes en vertu de la présente directive ou aux organismes désignés à cet effet par les États membres, au minimum leur nom, leur adresse et leurs coordonnées, ainsi que le secteur dans lequel elles exercent leurs activités ou le type de service qu'elles fournissent, et, le cas échéant, une liste des États membres dans lesquels elles fournissent leurs services. Les États membres peuvent décider des mécanismes appropriés, lorsqu'il existe, au niveau national, des registres permettant d'identifier les entités relevant du champ d'application de la présente directive.

(9) […] Les microentités ou les entités de petite taille qui remplissent certains critères indiquant qu'elles jouent un rôle essentiel pour les économies ou les sociétés des États membres ou pour des secteurs ou des types de services particuliers devraient également être couvertes par la présente directive, et les États membres devraient être chargés d'établir une liste de ces entités, et de la transmettre à la Commission. Les États membres devraient être chargés **de soumettre à la Commission, au minimum, des informations pertinentes sur le nombre d'entités identifiées, le secteur auquel elles appartiennent ou le type de service qu'elles fournissent, ainsi que les critères en fonction desquels elles ont été identifiées**. **Les États membres peuvent également décider, lorsque les règles nationales de sécurité le prévoient, de communiquer à la Commission le nom de ces entités.**

(9 *bis*) Les entités de l'administration publique qui exercent des activités dans les domaines de la sécurité nationale, de la défense, de la sécurité publique, de l'application de la loi et du pouvoir judiciaire, ainsi que les parlements et les banques centrales sont exclus du champ d'application de la présente directive. Aux fins de la présente directive, les entités disposant d'une compétence réglementaire ne sont pas considérées comme exerçant des activités dans le domaine de l'application de la loi et, par conséquent, elles ne sont pas exclues du champ d'application de la présente directive pour ce motif. En outre, les entités de l'administration publique des pouvoirs publics centraux, qui sont établies conjointement avec un pays tiers en vertu d'un accord international, ne relèvent pas du champ d'application de la présente directive.

(9 *bis bis*) Les États membres devraient pouvoir établir que les entités identifiées, avant l'entrée en vigueur de la présente directive, comme opérateurs de services essentiels conformément à la directive (UE) 2016/1148 doivent être considérées comme des entités essentielles.

(9 *bis bis bis*) La présente directive ne s'applique pas aux missions diplomatiques et consulaires des États membres à l'étranger ni aux infrastructures TIC utilisées par ces missions, dans la mesure où ces infrastructures sont situées à l'étranger ou sont exploitées pour des utilisateurs à l'étranger.

(10) La Commission, en coopération avec le groupe de coopération, peut publier des lignes directrices concernant la mise en œuvre des critères applicables aux microentreprises et aux entreprises de petite taille.

(11) […] **Les entités qui relèvent du champ d'application de la présente directive devraient être classées en deux catégories (essentielles et importantes) en fonction du niveau de criticité du secteur dans lequel elles sont actives ou du type de services qu'elles fournissent et de leur taille**. **À cet égard, il convient également de tenir dûment compte, le cas échéant, de toute évaluation des risques ou orientation sectorielle pertinente réalisée par les autorités compétentes.** Les entités tant essentielles qu'importantes devraient être soumises aux […] exigences en matière de gestion des risques et obligations de signalement. Les régimes de surveillance et de sanction applicables à ces deux catégories d'entités devraient être différenciés afin de garantir un juste équilibre entre les exigences et les obligations **fondées sur les risques**, d'une part, et la charge administrative qui découle du contrôle de la conformité, d'autre part.

(12) **La présente directive définit les valeurs de référence pour les mesures de gestion des risques et les obligations de signalement en matière de cybersécurité dans tous les secteurs relevant de son champ d'application. Afin d'éviter la fragmentation des dispositions en matière de cybersécurité des actes juridiques de l'Union, lorsque des dispositions sectorielles supplémentaires relatives aux mesures de gestion des risques et aux obligations de signalement en matière de cybersécurité sont jugées nécessaires pour garantir un niveau élevé de cybersécurité, la Commission devrait évaluer si de telles dispositions pourraient être prévues dans un acte d'exécution au titre de l'habilitation prévue par la présente directive**. **Si de tels actes ne conviennent pas à cette fin,** la législation […] sectorielle **pourrait** contribuer à garantir **un** […] niveau élevé de cybersécurité tout en tenant pleinement compte du caractère spécifique et complexe […] **des** secteurs **concernés**. **Les raisons pour lesquelles un acte d'exécution au titre de l'habilitation prévue par la présente directive n'était pas approprié doivent être expliquées dans la législation sectorielle. Dans le même temps, ces dispositions sectorielles des actes juridiques de l'Union devraient tenir dûment compte de la nécessité d'un cadre complet et harmonisé en matière de cybersécurité.** […] **Ceci** est sans préjudice des compétences de mise en œuvre existantes qui ont été conférées à la Commission dans un certain nombre de secteurs, notamment les transports et l'énergie.

(12 *bis*) Lorsqu'un acte juridique sectoriel de l'Union **contient des dispositions qui** imposent aux entités essentielles ou importantes d'adopter des mesures **ayant un effet au moins équivalent aux obligations prévues dans la présente directive en ce qui concerne la** gestion des risques en matière de cybersécurité […] **et le signalement** des incidents ou des cybermenaces importantes […], il convient d'appliquer ces dispositions sectorielles, y compris en matière de surveillance et d'application. **Pour déterminer si les obligations énoncées dans les dispositions sectorielles d'un acte juridique de l'Union ont un effet équivalent, les aspects suivants devraient être pris en considération: i) les mesures de gestion des risques en matière de cybersécurité devraient consister en des mesures techniques et organisationnelles appropriées et proportionnées permettant de gérer les risques pour la sécurité des réseaux et des systèmes d'information que les entités concernées utilisent pour fournir leurs services, et devraient inclure au minimum tous les éléments prévus par la présente directive; ii) l'obligation de signaler les incidents et les cybermenaces importants devrait être au moins équivalente aux obligations énoncées dans la présente directive en ce qui concerne le contenu, le format et les délais des signalements; iii) les modalités prévues dans les actes juridiques sectoriels de l'Union selon lesquelles les entités et les autorités concernées effectuent le signalement devraient être au moins équivalentes aux obligations énoncées dans la présente directive en ce qui concerne leur contenu, leur format et leurs délais, et devraient tenir compte du rôle des CSIRT; iv) les exigences en matière de coopération transfrontalière applicables aux autorités concernées devraient être au moins équivalentes à celles énoncées dans la présente directive. Si les dispositions sectorielles d'un acte juridique de l'Union ne couvrent pas toutes les entités d'un secteur spécifique relevant du champ d'application de la présente directive, les dispositions pertinentes de la présente directive devraient continuer de s'appliquer aux entités non couvertes par ces dispositions sectorielles.**

(12 *bis bis*) La Commission **devrait réexaminer périodiquement l'application de l'exigence selon laquelle les dispositions sectorielles d'un acte juridique de l'Union devraient avoir un effet équivalent** […]. **La Commission devrait consulter le groupe de coopération lorsqu'elle prépare ce réexamen périodique.**

(12 *bis bis bis*) Les futurs actes juridiques sectoriels de l'Union devraient tenir dûment compte des définitions figurant à l'article 4 de la présente directive ainsi que du cadre de surveillance et d'exécution défini au chapitre VI de la présente directive.

(12 *bis ter*) Lorsque des dispositions sectorielles d'actes juridiques de l'Union imposent aux entités essentielles ou importantes d'adopter des mesures ayant un effet au moins équivalent aux obligations de signalement prévues dans la présente directive, il convient d'éviter le chevauchement des obligations de signalement et de garantir la cohérence et l'efficacité du traitement des signalements de cybermenaces ou d'incidents. À cette fin, ces dispositions sectorielles peuvent autoriser les États membres à mettre en place un mécanisme commun, automatique et direct de signalement des incidents importants et des cybermenaces à la fois aux autorités dont les tâches sont définies dans les dispositions sectorielles respectives et aux autorités compétentes, y compris, selon le cas, le point de contact unique et les CSIRT, chargées des missions de cybersécurité prévues par la présente directive, ou un mécanisme garantissant un partage systématique et immédiat d'informations et une coopération entre les autorités concernées et les CSIRT en ce qui concerne le traitement de ces signalements. Aux fins de la simplification du signalement et de la mise en œuvre du mécanisme commun, automatique et direct de signalement, les États membres peuvent, conformément aux actes juridiques sectoriels, utiliser le point d'entrée unique qu'ils établissent conformément à l'article 11, paragraphe 5 bis, de la présente directive. Dans un souci d'harmonisation, les obligations en matière de signalement prévues dans les actes juridiques sectoriels de l'Union devraient être alignées sur celles prévues par la présente directive. Les États membres peuvent déterminer que les autorités compétentes en vertu de la présente directive ou les CSIRT nationaux sont les destinataires du signalement, conformément à la législation sectorielle.

(13) Le règlement XXXX/XXXX du Parlement européen et du Conseil devrait être considéré comme un acte juridique sectoriel de l'Union en lien avec la présente directive en ce qui concerne les entités du secteur financier. Les dispositions du règlement XXXX/XXXX portant sur les mesures de gestion des risques concernant les technologies de l'information et de la communication (TIC), la gestion des risques liés aux TIC et notamment le signalement des incidents, ainsi que sur le test de la résilience opérationnelle numérique, les accords de partage d'informations et les risques liés aux tiers en matière de TIC devraient s'appliquer au lieu de celles prévues par la présente directive. Les États membres ne devraient par conséquent pas appliquer aux entités financières couvertes par le règlement XXXX/XXXX les dispositions de la présente directive concernant la gestion des risques de cybersécurité et les obligations de signalement, […] **ainsi que** la surveillance et l'application. Dans le même temps, il est important de conserver une relation forte et de maintenir le partage d'informations avec le secteur financier dans le cadre de la présente directive. À cet effet, le règlement XXXX/XXXX permet […] **aux** autorités européennes de surveillance (AES) pour le secteur financier et […] **aux** autorités nationales compétentes au titre du règlement XXXX/XXXX de participer aux […] travaux […] du groupe de coopération, ainsi que d'échanger des informations et de coopérer avec les points de contact uniques désignés en vertu de la présente directive […] **ainsi qu'**avec les CSIRT nationaux. Les autorités compétentes en vertu du règlement XXXX/XXXX devraient également communiquer les détails des incidents importants liés aux TIC **et des cybermenaces importantes** aux points de contact uniques, **aux autorités compétentes et aux CSIRT nationaux** désignés en vertu de la présente directive. **Cet objectif peut être atteint grâce à la transmission automatique et directe des signalements d'incidents ou grâce à une plateforme de signalement commune.** De plus, les États membres devraient continuer de couvrir le secteur financier dans leurs stratégies de cybersécurité et les CSIRT nationaux peuvent inclure le secteur financier dans leurs activités.

(13 *bis*) Afin d'éviter les écarts et les doubles emplois en ce qui concerne les obligations en matière de cybersécurité imposées aux entités du secteur de l'aviation visées au point 2 a) de l'annexe I, les autorités nationales désignées en vertu des règlements (CE) n° 300/2008[16] et (UE) 2018/1139[17] du Parlement européen et du Conseil et les autorités compétentes au titre de la présente directive devraient coopérer pour la mise en œuvre des mesures de gestion des risques en matière de cybersécurité et la surveillance de ces mesures au niveau national. Le respect par une entité des mesures de gestion des risques en matière de cybersécurité prévues par la présente directive pourrait être considéré par les autorités nationales désignées en vertu des règlements (CE) n° 300/2008 et (UE) 2018/1139 comme équivalent au respect des exigences énoncées dans ces règlements ainsi que dans les actes délégués et d'exécution pertinents adoptés en vertu de ces règlements.

---

16 Règlement (CE) n° 300/2008 du Parlement européen et du Conseil du 11 mars 2008 relatif à l'instauration de règles communes dans le domaine de la sûreté de l'aviation civile et abrogeant le règlement (CE) n° 2320/2002 (JO L 97 du 9.4.2008, p. 72).

17 Règlement (UE) 2018/1139 du Parlement européen et du Conseil du 4 juillet 2018 concernant des règles communes dans le domaine de l'aviation civile et instituant une Agence de l'Union européenne pour la sécurité aérienne, et modifiant les règlements (CE) n° 2111/2005, (CE) n° 1008/2008, (UE) n° 996/2010, (UE) n° 376/2014 et les directives 2014/30/UE et 2014/53/UE du Parlement européen et du Conseil, et abrogeant les règlements (CE) n° 552/2004 et (CE) n° 216/2008 du Parlement européen et du Conseil ainsi que le règlement (CEE) n° 3922/91 du Conseil (JO L 212 du 22.8.2018, p. 1).

(14) Vu les liens qui existent entre la cybersécurité et la sécurité physique des entités, il convient d'assurer la cohérence des approches entre la directive (UE) XXXX/XXXX du Parlement européen et du Conseil et la présente directive. À cet effet, les États membres devraient veiller à ce que les entités critiques **[**et les entités équivalentes**]**, au titre de la directive (UE) XXXX/XXXX, soient considérées comme des entités essentielles en vertu de la présente directive. Les États membres devraient également veiller à ce que leurs stratégies de cybersécurité prévoient un cadre politique pour une coordination renforcée entre l'autorité compétente en vertu de la présente directive et l'autorité compétente en vertu de la directive (UE) XXXX/XXXX dans le cadre du partage d'informations relatives aux incidents et aux cybermenaces ainsi que de l'exercice des tâches de surveillance. Les autorités **compétentes** en vertu des deux directives devraient coopérer et échanger des informations, notamment en ce qui concerne le recensement des entités critiques, les menaces, risques **et** incidents en matière de cybersécurité**, ainsi que les risques, menaces et incidents non liés à la cybersécurité** affectant les entités critiques **ou les entités équivalant aux entités critiques, y compris** […] les mesures **physiques et** de cybersécurité adoptées par les entités critiques **ainsi que des résultats des activités de surveillances réalisées à l'égard de ces entités**. **En outre, afin de rationaliser les activités de surveillance entre les autorités compétentes désignées en vertu des deux directives et de réduire au minimum la charge administrative pour les entités concernées, les autorités compétentes devraient s'efforcer d'harmoniser les modèles de signalement des incidents et les processus de surveillance.** […] **Lorsqu'il y a lieu,** les autorités compétentes au titre de la directive (UE) XXX/XXX […] **peuvent demander aux** autorités compétentes au titre de la présente directive […] **d'**exercer leurs pouvoirs de surveillance et d'exécution […] en ce qui concerne une entité essentielle définie comme critique. […]

(14 *bis*) Les entités appartenant au secteur des infrastructures numériques sont par nature fondées sur les réseaux et les systèmes d'information et, par conséquent, les obligations qui leur incombent en vertu de la présente directive devraient porter, de manière globale, sur la sécurité physique de ces systèmes, en vertu des obligations qui sont les leurs pour la gestion des risques et le signalement en matière de cybersécurité. Ces questions étant régies par la présente directive, les obligations prévues aux chapitres III à VI de la directive (UE) XXX/XXX [directive sur la résilience des entités critiques] ne s'appliquent pas à ces entités.

(15) Le fait de maintenir et préserver un système de noms de domaines (DNS) fiable, résilient et sécurisé constitue un facteur crucial pour la protection de l'intégrité d'internet et est essentiel à son fonctionnement continu et stable, dont dépendent l'économie numérique et la société. Par conséquent, la présente directive devrait s'appliquer **aux** fournisseurs de services DNS, **tout au long de la chaîne d'avitaillement et de résolution**, **qui sont importants pour le marché intérieur,** y compris les […] **registres** de noms de domaines de premier niveau (TLD), […] **les entités fournissant des services d'enregistrement de noms de domaine**, **les opérateurs de** serveurs d'autorité pour les noms de domaines et […] **les opérateurs de** résolveurs récursifs. **Le terme "fournisseur de services DNS" ne devrait pas s'appliquer aux services DNS exploités à des fins propres à l'entité concernée et à ses entités affiliées. Les obligations en matière de cybersécurité découlant de la présente directive pour cette catégorie de fournisseurs sont strictement limitées aux mesures de gestion des risques et aux signalements en matière de cybersécurité et sont donc sans préjudice de la gouvernance du DNS mondial par la communauté multipartite.**

(16) Les services d'informatique en nuage devraient couvrir les services qui permettent l'accès sur demande et l'accès large à distance à un ensemble modulable et variable de ressources informatiques distribuées et pouvant être partagées. Ces ressources informatiques comprennent des ressources telles que les réseaux, les serveurs ou les autres infrastructures, les systèmes d'exploitation, les logiciels, le stockage, les applications et les services. **Les modèles de services liés à l'informatique en nuage comprennent, entre autres, les infrastructures services (IaaS), les plateformes services (PaaS), les logiciels services (SaaS) et les réseaux services (NaaS).** Les modèles de déploiement de l'informatique en nuage devraient inclure les modèles privés, communautaires, publics et hybrides en nuage. Les services et modèles de déploiement susmentionnés revêtent le même sens que celui des conditions de service et des modèles de déploiement défini dans la norme ISO/CEI 17788:2014. La capacité des utilisateurs de l'informatique en nuage de s'autofournir unilatéralement des capacités informatiques, comme du temps de serveur ou du stockage en réseau, sans aucune intervention humaine de la part du fournisseur de service d'informatique en nuage pourrait être décrite comme une gestion sur demande. Le terme "accès large à distance" est utilisé pour décrire le fait que les capacités en nuage sont fournies sur le réseau et que l'accès à celles-ci se fait par des mécanismes encourageant le recours à des plateformes clients légères ou lourdes disparates (y compris les téléphones mobiles, les tablettes, les ordinateurs portables et les postes de travail).

Le terme "modulable" renvoie aux ressources informatiques qui sont attribuées d'une manière souple par le fournisseur de services en nuage, indépendamment de la localisation géographique de ces ressources, pour gérer les fluctuations de la demande. Les termes "ensemble variable" sont utilisés pour décrire les ressources informatiques qui sont mobilisées et libérées en fonction de la demande pour pouvoir augmenter ou réduire rapidement les ressources disponibles en fonction de la charge de travail. Les termes "pouvant être partagées" sont utilisés pour décrire les ressources informatiques qui sont mises à disposition de nombreux utilisateurs qui partagent un accès commun au service, le traitement étant effectué séparément pour chaque utilisateur bien que le service soit fourni à partir du même équipement électronique. Le terme "distribué" est utilisé pour décrire les ressources informatiques qui se trouvent sur des ordinateurs ou des appareils en réseau différents, qui communiquent et se coordonnent par transmission de messages.

(17) Vu l'émergence de technologies innovantes et de nouveaux modèles commerciaux, de nouveaux modèles de déploiement et de service d'informatique en nuage devraient apparaître sur le marché en cause en réaction aux besoins changeants des clients. Dans un tel contexte, les services d'informatique en nuage peuvent être fournis sous une forme extrêmement distribuée, toujours plus près de l'endroit où les données sont générées ou collectées, entraînant ainsi une transition du modèle traditionnel vers un modèle très distribué (le traitement des données à la périphérie, ou "edge computing").

(18) Les services proposés par les fournisseurs de services de centre de données ne sont pas toujours fournis sous la forme de service d'informatique en nuage. En conséquence, les centres de données ne font pas toujours partie d'une infrastructure d'informatique en nuage. Afin de gérer l'ensemble des risques qui menacent la sécurité des réseaux et des systèmes d'information, la présente directive devrait également couvrir les fournisseurs de services de centre de données qui ne sont pas des services d'informatique en nuage. Aux fins de la présente directive, le terme "service de centre de données" devrait couvrir la fourniture d'un service qui englobe les structures, ou les groupes de structures, dédiées à l'hébergement, l'interconnexion et l'exploitation centralisés des équipements de traitement de l'information et de réseau fournissant des services de stockage, de traitement et de transport des données, ainsi que l'ensemble des installations et des infrastructures de distribution d'électricité et de contrôle environnemental. Le terme "service de centre de données" ne s'applique pas aux centres de données internes propres à une entreprise et exploités pour les besoins de l'entité concernée.

(19) Les fournisseurs de services postaux au sens de la directive 97/67/CE du Parlement européen et du Conseil[18], […] **y compris** les fournisseurs de services […] de messagerie, devraient être soumis à la présente directive s'ils fournissent au moins l'une des étapes de la chaîne postale de livraison, notamment la levée, le tri ou la distribution, y compris les services d'enlèvement. Les services de transport qui ne sont pas réalisés en lien avec l'une de ces étapes devraient sortir de la portée des services postaux.

---

18 Directive 97/67/CE du Parlement européen et du Conseil du 15 décembre 1997 concernant des règles communes pour le développement du marché intérieur des services postaux de la Communauté et l'amélioration de la qualité du service (JO L 15 du 21.1.1998, p. 14).

(20) Ces interdépendances croissantes découlent d'un réseau de fourniture de services de plus en plus transfrontière et interdépendant, qui utilise des infrastructures essentielles dans toute l'Union dans les secteurs de l'énergie, des transports, des infrastructures numériques, de l'eau potable, des eaux usées, de la santé, de certains aspects de l'administration publique et de l'espace, dans la mesure où la fourniture de certains services dépendant de structures terrestres détenues, gérées et exploitées par des États membres ou par des parties privées est concernée, ce qui ne couvre donc pas les infrastructures détenues, gérées ou exploitées par ou au nom de l'Union dans le cadre de ses programmes spatiaux. Ces interdépendances signifient que toute perturbation, même initialement limitée à une entité ou un secteur, peut produire des effets en cascade plus larges, entraînant éventuellement des incidences négatives durables et de grande ampleur pour la fourniture de services dans l'ensemble du marché intérieur. La pandémie de COVID-19 a mis en évidence la vulnérabilité de nos sociétés de plus en plus interdépendantes face à des risques peu probables.

(20 *bis*) **Afin d'atteindre et de maintenir un niveau élevé de cybersécurité, les stratégies nationales de cybersécurité requises par la présente directive devraient consister en cadres cohérents qui prévoient une gouvernance dans le domaine de la cybersécurité. Ces stratégies peuvent être composées d'un ou de plusieurs documents législatifs ou non.**

(21) Compte tenu des divergences entre les structures de gouvernance nationales et en vue de sauvegarder les accords existants au niveau sectoriel ou les autorités de surveillance et de régulation de l'Union, les États membres devraient pouvoir désigner plusieurs autorités nationales compétentes chargées d'accomplir les tâches liées à la sécurité des réseaux et des systèmes d'information des entités essentielles et importantes dans le cadre de la présente directive. Les États membres devraient pouvoir attribuer cette mission à une autorité existante.

(22) Afin de faciliter la coopération et la communication transfrontalières entre les autorités et pour permettre la mise en œuvre effective de la présente directive, il est nécessaire que chaque État membre désigne un point de contact national unique chargé de coordonner les tâches liées à la sécurité des réseaux et des systèmes d'information et de la coopération transfrontalière au niveau de l'Union.

(23) Les autorités compétentes ou les CSIRT devraient recevoir les signalements d'incidents provenant des entités de manière efficace et efficiente, **également en vue de faciliter une réaction rapide aux incidents, le cas échéant, et d'apporter une réponse à l'entité signalante**. Les points de contact uniques devraient être chargés de transmettre les notifications d'incidents aux points de contact uniques des autres États membres touchés. […]

(23 *bis*) **Les actes juridiques sectoriels de l'Union qui imposent des mesures de gestion des risques ou des obligations de signalement en matière de cybersécurité ayant un effet au moins équivalent à celles prévues dans la présente directive pourraient prévoir que leurs autorités compétentes désignées exercent leurs pouvoirs de surveillance et d'exécution à l'égard de ces mesures ou obligations avec l'assistance des autorités compétentes désignées conformément à la présente directive. Les autorités compétentes concernées pourraient établir des arrangements de coopération à cet effet. Ces accords de coopération pourraient préciser, entre autres, les procédures relatives à la coordination des activités de surveillance, y compris les procédures d'enquête et d'inspection sur place conformément au droit national ainsi qu'un mécanisme d'échange des informations pertinentes entre les autorités chargées de la surveillance et de l'exécution, y compris l'accès aux informations relatives au cyberespace demandées par les autorités compétentes désignées conformément à la présente directive.**

(24) Les États membres devraient disposer de moyens suffisants, sur les plans technique et organisationnel, pour prévenir et détecter les incidents et risques liés aux réseaux et systèmes d'information et prendre les mesures d'intervention et d'atténuation nécessaires. Les États membres devraient dès lors veiller à disposer de CSIRT, également connus sous la dénomination de centres de réponse aux urgences informatiques (CERT), opérationnels et conformes aux exigences essentielles afin de garantir l'existence de moyens effectifs et compatibles pour gérer les incidents et les risques et d'assurer une coopération efficace au niveau de l'Union. Afin d'améliorer la relation de confiance entre les entités et les CSIRT, dans les cas où un CSIRT fait partie de l'autorité compétente, les États membres […] **peuvent** envisager de mettre en place une séparation fonctionnelle entre d'une part les tâches opérationnelles assurées par les CSIRT, notamment en lien avec le partage d'informations et l'assistance aux entités, et d'autre part les activités de surveillance des autorités compétentes.

(25) En ce qui concerne les données à caractère personnel, les CSIRT devraient être en mesure de réaliser, conformément au règlement (UE) 2016/679 du Parlement européen et du Conseil[19] relatif aux données à caractère personnel, au nom et sur demande d'une entité en vertu de la présente directive, une analyse des réseaux et des systèmes d'information utilisés pour la fourniture de leurs services. **Lorsqu'il y a lieu,** les États membres devraient avoir pour but d'assurer l'égalité du niveau des capacités techniques de tous les CSIRT sectoriels. Les États membres peuvent solliciter l'assistance de l'agence européenne pour la cybersécurité (ENISA) pour la mise en place des CSIRT nationaux.

(26) Compte tenu de l'importance de la coopération internationale en matière de cybersécurité, les CSIRT devraient pouvoir participer à des réseaux de coopération internationaux en plus du réseau des CSIRT institué par la présente directive. **Par conséquent, les CSIRT et les autorités compétentes pourraient échanger des informations, y compris des données à caractère personnel, avec les CSIRT de pays tiers ou leurs autorités aux fins de l'exécution de leurs tâches conformément au règlement (UE) 2016/679. En l'absence d'une décision d'adéquation adoptée conformément à l'article 45 du règlement (UE) 2016/679 ou de garanties appropriées conformément à l'article 46 dudit règlement, l'échange de données à caractère personnel jugé nécessaire pour atténuer les cybermenaces importantes et réagir à un incident important en cours pourrait être considéré comme constituant un motif important d'intérêt public au sens de l'article 49, paragraphe 1, point d), du règlement (UE) 2016/679.**

[19] Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données) (JO L 119 du 4.5.2016, p. 1).

(27) Conformément à l'annexe de la recommandation (UE) 2017/1584 de la Commission sur la réaction coordonnée aux incidents et crises de cybersécurité majeurs ("plan d'action")[20], un incident majeur signifie un incident qui frappe plusieurs États membres ou qui provoque des perturbations dépassant les capacités d'action du seul État membre concerné. En fonction de leur cause et de leurs conséquences, les incidents majeurs peuvent dégénérer et se transformer en crises à part entière, empêchant le bon fonctionnement du marché intérieur. Vu la large portée et, dans la plupart des cas, la nature transfrontalière de ces incidents, les États membres et les institutions, organes et agences compétents de l'Union devraient coopérer au niveau technique, opérationnel et politique afin de coordonner correctement la réaction dans toute l'Union.

(28) Puisque l'exploitation des vulnérabilités dans les réseaux et les systèmes d'information peut causer des perturbations et des dommages considérables, l'identification et la correction rapide de ces vulnérabilités est un facteur important de la réduction du risque en matière de cybersécurité. Les entités qui mettent au point **ou administrent** de tels systèmes devraient dont établir des procédures appropriées pour gérer les vulnérabilités découvertes. Puisque les vulnérabilités sont souvent découvertes et signalées (divulguées) par des tiers (les entités effectuant le signalement), le fabricant de produits ou le fournisseur de services TIC devraient également mettre en place les procédures nécessaires pour recevoir les informations relatives aux vulnérabilités communiquées par les tiers. À cet égard, les normes internationales ISO/CEI 30111 et ISO/CEI […] **29147** fournissent des orientations sur la gestion des vulnérabilités et la divulgation des vulnérabilités respectivement. En ce qui concerne la divulgation des vulnérabilités, la coordination entre les entités effectuant le signalement et les fabricants ou les fournisseurs de produits ou de services TIC est particulièrement importante. La divulgation coordonnée des vulnérabilités consiste en un processus structuré dans lequel les vulnérabilités sont signalées aux organisations de manière à leur donner la possibilité de diagnostiquer la vulnérabilité et d'y remédier avant que des informations détaillées à ce sujet soient divulguées à des tiers ou au public. La divulgation coordonnée des vulnérabilités devrait également comprendre la coordination entre l'entité effectuant le signalement et l'organisation en ce qui concerne le calendrier des corrections et la publication des vulnérabilités.

---

[20] Recommandation (UE) 2017/1584 de la Commission du 13 septembre 2017 sur la réaction coordonnée aux incidents et crises de cybersécurité majeurs (JO L 239 du 19.9.2017, p. 36).

(29) Les États membres devraient par conséquent adopter des mesures destinées à faciliter la divulgation coordonnée des vulnérabilités en créant une politique nationale pertinente. **Dans le cadre de leur politique nationale, les États membres devraient s'efforcer de relever, dans la mesure du possible, les défis auxquels sont confrontés les experts qui recherchent les vulnérabilités, y compris le risque lié à la responsabilité pénale potentielle, conformément à leur ordre juridique national.** […] Les États membres devraient désigner un CSIRT pour jouer le rôle de "coordinateur" et agir comme un intermédiaire entre les entités effectuant le signalement et les fabricants ou les fournisseurs de produits ou de services TIC lorsque cela est nécessaire. Les missions du CSIRT agissant en tant que coordinateur devraient notamment impliquer d'identifier et de contacter les entités concernées, d'apporter une assistance aux entités effectuant le signalement, de négocier des délais de divulgation et de gérer les vulnérabilités qui touchent plusieurs organisations (divulgation multipartite **coordonnée** de vulnérabilité). Lorsque les vulnérabilités **signalées pourraient avoir une incidence importante sur des entités de** […] plusieurs États membres, les CSIRT désignés […] devraient coopérer au sein du réseau des CSIRT **selon qu'il y a lieu**.

(30) L'accès en temps utile à des informations correctes relatives aux vulnérabilités touchant les produits et services TIC 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 entités et leurs utilisateurs, mais également pour les autorités nationales compétentes et les CSIRT. C'est pour cette raison que l'ENISA devrait mettre en place un registre des vulnérabilités dans lequel les entités essentielles et importantes et leurs fournisseurs, ainsi que les entités qui ne relèvent pas du champ d'application de la présente directive, **ou les CSIRT désignés**, peuvent, à titre volontaire, divulguer les vulnérabilités et fournir des informations à cet égard afin de permettre aux utilisateurs de prendre les mesures d'atténuation appropriées.

(31) Bien que des registres ou des bases de données similaires sur les vulnérabilités existent, ils sont hébergés et gérés par des entités qui ne sont pas établies dans l'Union. Un registre européen des vulnérabilités géré par l'ENISA améliorerait la transparence du processus de publication avant la divulgation officielle d'une vulnérabilité et la résilience en cas de perturbation ou d'interruption de la fourniture de services similaires. Afin d'éviter la duplication des efforts déployés et de viser la complémentarité dans la mesure du possible, l'ENISA devrait étudier la possibilité de conclure des accords de coopération structurés avec les registres existants sur le territoire de pays tiers. **En particulier, l'ENISA devrait étudier la possibilité d'une coopération étroite avec les opérateurs du registre mondial Common Vulnerabilities and Exposures (CVE), y compris la possibilité de devenir une "autorité de numérotation racine de la CVE".**

(32) **Le groupe de coopération devrait continuer de soutenir et de faciliter la coopération stratégique ainsi que l'échange d'informations, et de renforcer la confiance entre les États membres.** Tous les deux ans, le groupe de coopération devrait élaborer un programme de travail qui inclurait les actions qu'il doit réaliser afin de mettre en œuvre ses objectifs et ses tâches. Le calendrier du premier programme adopté au titre de la présente directive devrait être aligné sur le calendrier du dernier programme adopté au titre de la directive (UE) 2016/1148 afin d'éviter de perturber les travaux du groupe.

(33) Lorsqu'il met au point les documents d'orientation, le groupe de coopération devrait toujours: dresser l'état des lieux des solutions et des expériences nationales, évaluer les effets produits par les éléments livrables du groupe de coopération sur les approches nationales, discuter des défis en matière de mise en œuvre et formuler des recommandations spécifiques auxquelles il convient de répondre par une meilleure application des règles existantes.

(34) Le groupe de coopération devrait conserver sa forme de forum flexible et continuer d'être en mesure de réagir aux priorités politiques et aux difficultés nouvelles et en évolution, tout en tenant compte de la disponibilité des ressources. Il devrait régulièrement organiser des réunions conjointes avec les parties intéressées privées de toute l'Union en vue de discuter des activités menées par le groupe et de recueillir des informations sur les nouveaux défis politiques. Afin d'améliorer la coopération au niveau de l'Union, le groupe devrait envisager d'inviter les organes et agences de l'Union participant à la politique de cybersécurité, comme le Centre européen de lutte contre la cybercriminalité (EC3), l'Agence de l'Union européenne pour la sécurité aérienne (AESA) et l'Agence de l'Union européenne pour le programme spatial (EUSPA), à participer à ses travaux.

(35) Les autorités compétentes et les CSIRT devraient pouvoir participer aux programmes d'échange d'agents provenant d'autres États membres afin d'améliorer la coopération. Elles devraient prendre les mesures nécessaires pour que les agents d'autres États membres puissent jouer un rôle effectif dans les activités de l'autorité compétente hôte.

(35 *bis*) Le réseau des CSIRT devrait continuer de contribuer à renforcer la confiance et à promouvoir une coopération opérationnelle rapide et efficace entre les États membres. Afin de renforcer la coopération opérationnelle au niveau de l'Union, le réseau des CSIRT devrait envisager d'inviter les organes et organismes de l'Union associés à la politique de cybersécurité, tels qu'Europol, à participer à ses travaux.

(36) […]

(36 *bis*) **Afin de faciliter la mise en œuvre effective des dispositions de la présente directive, par exemple en ce qui concerne la gestion des vulnérabilités, la gestion des risques en matière de cybersécurité, les mesures liées au signalement et les arrangements en matière d'échange d'informations, les États membres peuvent coopérer avec des pays tiers et entreprendre des activités jugées appropriées à cette fin, y compris des échanges d'informations sur les menaces, les incidents, les vulnérabilités, les outils et méthodes, les tactiques, les techniques et les procédures, la préparation et les exercices pour la gestion des crises de cybersécurité, la formation, le renforcement de la confiance ainsi que les arrangements permettant de partager les informations de façon structurée. Ces arrangements de coopération devraient être conformes au droit de l'Union en matière de protection des données.**

(37) Les États membres devraient contribuer à la création du cadre de l'Union européenne pour la réaction aux crises de cybersécurité défini dans la recommandation (UE) 2017/1584 via les réseaux de coopération existants, notamment le réseau **européen** pour la préparation et la gestion des crises cyber (UE-CyCLONe), le réseau des CSIRT et le groupe de coopération. UE-CyCLONe et le réseau des CSIRT devraient coopérer sur la base de modalités de procédure définissant les conditions de cette coopération **et éviter toute duplication des tâches**. Le règlement intérieur d'UE-CyCLONe devrait préciser plus en détail les modalités selon lesquelles le réseau devrait fonctionner, y compris, mais sans s'y limiter, les rôles, les modes de coopération, les interactions avec les autres acteurs pertinents et les modèles de partage d'informations, ainsi que les moyens de communication. Pour la gestion des crises au niveau **politique** de l'Union, les parties concernées devraient s'appuyer sur le dispositif intégré pour une réaction au niveau politique dans les situations de crise (IPCR).
La Commission devrait avoir recours au processus intersectoriel de premier niveau ARGUS pour la coordination en cas de crise. Si la crise comporte d'importantes implications liées à la politique extérieure ou à la politique de sécurité et de défense commune (PSDC), le système de réponse aux crises (SRC) du Service européen pour l'action extérieure (SEAE) devrait être activé.

(37 *bis*) **UE-CyCLONe devrait servir de réseau intermédiaire entre les niveaux technique et politique lors d'incidents et de crises de cybersécurité importants. Le réseau devrait renforcer la coopération au niveau opérationnel, en s'appuyant sur les résultats obtenus par le réseau des CSIRT et en utilisant ses propres capacités pour réaliser une analyse d'impact des incidents et crises majeurs, et en soutenant la prise de décision au niveau politique. Les institutions, organes et organismes de l'UE devraient désigner une autorité compétente qui serait chargée de la gestion des incidents et des crises de sécurité majeurs et deviendrait membre du réseau UE-CyCLONe.**

(38) […]

(39) […]

(39 *bis*) **Dans une large mesure, il incombe aux entités essentielles et importantes de garantir la sécurité des réseaux et des systèmes d'information. Il convient de promouvoir et de faire évoluer une culture de la gestion des risques impliquant une analyse des risques et l'application de mesures de sécurité adaptées aux risques encourus.**

(40) […] Les mesures de gestion des risques devraient **tenir compte de la mesure dans laquelle l'entité dépend des réseaux et des systèmes d'information, et comprendre des mesures** […] permettant de déterminer tous les risques d'incidents, de prévenir, de repérer et de gérer les incidents et d'en atténuer les effets. La sécurité des réseaux et des systèmes d'information devrait inclure la sécurité des données stockées, transmises et traitées.

(40 *bis*) **Étant donné que les menaces pesant sur la sécurité des réseaux et des systèmes d'information peuvent avoir des origines différentes, la présente directive applique une approche "tous risques" qui inclut la protection des réseaux et des systèmes d'information ainsi que de leur environnement physique contre toute éventualité telle que vol, incendie, inondation, défaillance des télécommunications ou défaillance électriques, ou contre tout accès physique non autorisé et toute atteinte aux informations détenues par l'entité et aux installations de traitement de l'information de l'entité, ou toute interférence avec ces informations et installations, susceptibles de compromettre la disponibilité, l'authenticité, l'intégrité ou la confidentialité des données stockées, transmises ou traitées ou des services offerts par les réseaux et systèmes d'information ou accessibles par ceux-ci. Les mesures de gestion des risques devraient donc également porter sur la sécurité physique et de l'environnement, en incluant des mesures visant à protéger les réseaux et systèmes d'information de l'entité contre les défaillances du système, les erreurs humaines, les actes malveillants ou les phénomènes naturels, conformément aux normes européennes ou internationales reconnues, par exemple celles figurant dans la série ISO 27000. À cet égard, les entités devraient, dans le cadre de leurs mesures de gestion des risques, tenir également compte de la sécurité liée aux ressources humaines et mettre en place des politiques appropriées en matière de contrôle de l'accès. Ces mesures devraient être compatibles avec la directive XXXX [directive sur la résilience des entités critiques].**

(40 *ter*) **En l'absence de schémas européens de certification de cybersécurité appropriés adoptés conformément au règlement (UE) 2019/881, les États membres pourraient imposer aux entités, aux fins du respect des exigences en matière de gestion des risques liés à la cybersécurité prévues par la présente directive, d'utiliser des produits, services et processus TIC certifiés ou d'obtenir un certificat au titre des schémas nationaux de cybersécurité disponibles.**

(41) Pour éviter que la charge financière et administrative imposée aux entités essentielles et importantes ne soit excessive, il convient que les exigences en matière de gestion des risques de cybersécurité soient proportionnées aux risques […] **pour** le réseau et le système d'information concernés, compte tenu de l'état le plus avancé de la technique en ce qui concerne ces mesures, **et au coût de leur mise en œuvre**. **Il convient également de tenir dûment compte de la taille de l'entité, ainsi que de la probabilité de survenue d'incidents et de leur gravité.**

(41 *bis*) En vue d'alléger les charges réglementaires, les exigences liées à la mise en œuvre des mesures de gestion des risques en matière de cybersécurité pour les entités de taille moyenne, les petites entités ou les micro-entités devraient en principe être moins astreignantes, à moins que des critères de criticité ou des évaluations nationales des risques ne justifient des exigences plus strictes, en particulier en ce qui concerne les entités qui satisfont aux critères de criticité énoncés dans la présente directive.

(42) Les entités essentielles et importantes devraient garantir la sécurité des réseaux et des systèmes d'information qu'elles utilisent dans le cadre de leurs activités. Il s'agit principalement de réseaux et de systèmes d'information privés qui sont gérés par leurs propres services informatiques ou dont la gestion de la sécurité a été sous-traitée. Les exigences en matière de gestion des risques de cybersécurité et de signalement prévues par la présente directive devraient s'appliquer aux entités essentielles et importantes que la maintenance de leurs réseaux et systèmes d'information soit assurée en interne ou qu'elle soit sous-traitée.

(42 *bis bis*) Compte tenu de leur nature transfrontière, les fournisseurs de services DNS, les registres de noms de domaines de premier niveau (TLD) et les entités fournissant des services d'enregistrement de noms de domaine pour les TLD, les fournisseurs de services d'informatique en nuage, les fournisseurs de services de centre de données, les fournisseurs de réseaux de diffusion de contenu, les fournisseurs de services gérés ainsi que les fournisseurs de services de sécurité gérés devraient faire l'objet d'un degré d'harmonisation plus élevé au niveau de l'Union. La mise en œuvre des mesures de cybersécurité devrait donc être facilitée par un acte d'exécution.

(43) Il est tout particulièrement important de répondre aux risques de cybersécurité découlant de la chaîne d'approvisionnement d'une entité et de ses relations avec ses fournisseurs vu la prévalence d'incidents dans le cadre desquels les entités ont été victimes de cyberattaques et des acteurs malveillants ont réussi à compromettre la sécurité des réseaux et systèmes d'information d'une entité en exploitant les vulnérabilités touchant les produits et les services de tiers. Les entités devraient donc évaluer et prendre en compte la qualité globale des produits et des pratiques de cybersécurité de leurs fournisseurs et fournisseurs de services, y compris de leurs procédures de développement sécurisées.

(44) Parmi tous les fournisseurs de services, les fournisseurs de services gérés de sécurité dans des domaines comme la réaction aux incidents, les tests de pénétration, les audits de sécurité et le conseil jouent un rôle particulièrement important s'agissant de soutenir les efforts mis en œuvre par les entités pour détecter les incidents et y réagir. Ces fournisseurs de services gérés de sécurité ont également été eux-mêmes la cible de cyberattaques et, du fait de leur grande intégration dans les activités des opérateurs, ils représentent un risque considérable en matière de cybersécurité. Les entités doivent donc faire preuve d'une diligence renforcée lorsqu'elles sélectionnent leurs fournisseurs de services gérés de sécurité.

(44 *bis*) Les autorités nationales compétentes, dans le cadre de leurs missions de surveillance, peuvent également bénéficier de services de cybersécurité, par exemple en matière d'audits de sécurité et de tests de pénétration ou de réaction en cas d'incident. Afin d'aider les entités, ainsi que les autorités nationales compétentes, à sélectionner des fournisseurs de services de cybersécurité qualifiés et fiables, la Commission, avec l'aide du groupe de coopération et de l'ENISA, devrait envisager de demander des schémas européens de certification de cybersécurité conformément à l'article 48 du règlement (UE) 2019/881.

(45) Les entités devraient également répondre aux risques de cybersécurité découlant de leurs interactions et de leurs relations avec d'autres parties intéressées dans le cadre d'un écosystème plus large. Plus particulièrement, les entités devraient prendre des mesures appropriées pour veiller à ce que leur coopération avec les institutions universitaires et de recherche se déroule dans le respect de leurs politiques en matière de cybersécurité et des bonnes pratiques concernant l'accès et la diffusion d'informations en toute sécurité de manière générale et la protection des droits de propriété intellectuelle de manière spécifique. De même, vu l'importance et la valeur que représentent les données pour leurs activités, les entités devraient prendre toutes les mesures de cybersécurité appropriées lorsqu'elles ont recours à des services de transformation et d'analyse des données fournis par des tiers.

(46) Afin de mieux répondre aux risques principaux liés aux chaînes d'approvisionnement et d'aider les entités actives dans les secteurs couverts par la présente directive à bien gérer les risques de cybersécurité liés aux chaînes d'approvisionnement et aux fournisseurs, le groupe de coopération impliquant les autorités nationales compétentes, en collaboration avec la Commission et l'ENISA, devrait réaliser des évaluations coordonnées sectorielles des risques liés aux chaînes d'approvisionnement, comme cela a été le cas pour les réseaux 5G suite à la recommandation (UE) 2019/534 sur la cybersécurité des réseaux 5G[21], dans le but de déterminer, secteur par secteur, les services, systèmes ou produits TIC critiques, les menaces pertinentes et les vulnérabilités.

[21] Recommandation (UE) 2019/534 de la Commission du 26 mars 2019 Cybersécurité des réseaux 5G (JO L 88 du 29.3.2019, p. 42).

(47) Les évaluations des risques liés aux chaînes d'approvisionnement, à la lumière des caractéristiques du secteur concerné, devraient tenir compte des facteurs techniques et, le cas échéant, non techniques, y compris ceux définis dans la recommandation (UE) 2019/534, dans l'évaluation coordonnée à l'échelle de l'Union des risques concernant la sécurité des réseaux 5G et dans la boîte à outils de l'UE pour la cybersécurité 5G convenue par le groupe de coopération. Afin de déterminer quelles chaînes d'approvisionnement devraient être soumises à une évaluation coordonnée des risques, il convient de tenir compte des critères suivants: i) la mesure dans laquelle les entités essentielles et importantes utilisent des services, systèmes ou produits TIC critiques spécifiques et en dépendent; ii) la pertinence des services, systèmes ou produits TIC critiques spécifiques pour la réalisation des fonctions sensibles ou critiques, notamment le traitement de données à caractère personnel; iii) la disponibilité d'autres services, systèmes ou produits TIC; iv) la résilience de la chaîne d'approvisionnement générale des services, systèmes ou produits TIC face aux événements perturbateurs et v) concernant les services, systèmes ou produits TIC émergents, leur potentielle importance à l'avenir pour les activités des entités.

(48) Afin de rationaliser les obligations juridiques imposées aux fournisseurs de réseaux de communications électroniques publics ou de services de communications électroniques accessibles au public et aux prestataires de services de confiance en lien avec la sécurité de leurs réseaux et systèmes d'information, ainsi que de permettre à ces entités et à leurs autorités compétentes respectives de bénéficier du cadre juridique établi par la présente directive (y compris la désignation du CSIRT chargé de la gestion des risques et des incidents, la participation des autorités et organes compétents aux travaux du groupe de coopération et le réseau des CSIRT), il convient de les inclure dans le champ d'application de la présente directive. Il convient donc d'abroger les dispositions correspondantes prévues par le règlement (UE) n° 910/2014 du Parlement européen et du Conseil[22] et par la directive (UE) 2018/1972 du Parlement européen et du Conseil[23] portant sur l'imposition d'exigences en matière de sécurité et de notification à ce type d'entités.

---

22 Règlement (UE) n° 910/2014 du Parlement européen et du Conseil du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/CE (JO L 257 du 28.8.2014, p. 73).

23 Directive (UE) 2018/1972 du Parlement européen et du Conseil du 11 décembre 2018 établissant le code des communications électroniques européen (JO L 321 du 17.12.2018, p. 36).

(48 *bis*) **Les obligations en matière de sécurité énoncées dans la présente directive devraient être considérées comme complémentaires des exigences imposées aux prestataires de services de confiance en vertu du règlement (UE) n° 910/2014 (règlement eIDAS). Il conviendrait de demander aux prestataires de services de confiance de prendre toutes les mesures appropriées et proportionnées pour gérer les risques qui pèsent sur leurs services, y compris en ce qui concerne les clients et les tiers utilisateurs, et de signaler les incidents de sécurité au titre de la présente directive. Ces obligations en matière de sécurité et de signalement devraient également concerner la protection physique du service fourni. L'article 24 du règlement (UE) n° 910/2014 continue de s'appliquer.**

(48 *bis bis*) **Les États membres peuvent confier le rôle des autorités compétentes pour les services de confiance aux organes de contrôle établis en vertu du règlement eIDAS afin d'assurer le maintien des pratiques actuelles et de tirer parti des connaissances et de l'expérience acquises dans le cadre de l'application du règlement eIDAS. Lorsque ce rôle est confié à un autre organe, les autorités nationales compétentes au titre de la présente directive devraient coopérer étroitement, en temps utile, en échangeant les informations pertinentes afin de garantir une surveillance efficace et le respect, par les prestataires de services de confiance, des exigences énoncées dans la présente directive et dans le règlement [XXXX/XXXX].**

Le cas échéant, l'autorité nationale compétente en vertu de la présente directive devrait informer immédiatement l'organe de contrôle établi en vertu du règlement eIDAS de toute menace ou incident important signalé dans le domaine de la cybersécurité ayant une incidence sur les services de confiance, ainsi que de tout manquement d'un prestataire de services de confiance aux exigences de la présente directive. Pour le signalement, les États membres peuvent utiliser, le cas échéant, le point d'entrée unique mis en place pour effectuer un signalement commun et automatique à la fois à l'organe de contrôle établi en vertu du règlement eIDAS et à l'autorité compétente en vertu de la présente directive. Les règles relatives aux obligations de signalement devraient être sans préjudice du règlement (UE) 2016/679 et de la directive 2002/58/CE du Parlement européen et du Conseil[24].

---

[24] Directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive vie privée et communications électroniques) (JO L 201 du 31.7.2002, p. 37).

(49) Lorsque cela est approprié et afin d'éviter toute perturbation inutile, […] les lignes directrices nationales […] existantes adoptées en vue de la transposition des règles portant sur les mesures de sécurité prévues par **les articles** 40 […] **et 41** de la directive (UE) 2018/1972 **devraient être prises en compte dans les modalités de transposition de la présente directive mises en œuvre par les États membres, ce qui permettrait de tirer parti des connaissances et des compétences déjà acquises, lors de l'application de la directive (UE) 2018/1972, en ce qui concerne les mesures de gestion des risques et les signalements d'incidents**. **L'ENISA peut également élaborer des orientations sur les obligations en matière de sécurité et de signalement qui incombent aux fournisseurs de réseaux de communication électronique publics ou de services de communication électronique accessibles au public afin de faciliter l'harmonisation et la transition et de réduire au minimum les perturbations. Les États membres peuvent confier le rôle des autorités compétentes pour les communications électroniques aux autorités de régulation nationales afin d'assurer le maintien des pratiques actuelles et de tirer parti des connaissances et de l'expérience acquises dans le cadre de l'application de la directive (UE) 2018/1972.**

(50) Étant donné l'importance croissante des services de communications interpersonnelles non fondés sur la numérotation, il convient de veiller à ce que ceux-ci soient également soumis à des exigences de sécurité appropriées au regard de leur nature spécifique et de leur importance économique. Les fournisseurs de tels services devraient par conséquent également garantir un niveau de sécurité des réseaux et des systèmes d'information correspondant au risque encouru. Étant donné que les fournisseurs de services de communications interpersonnelles non fondés sur la numérotation n'exercent normalement pas de contrôle effectif sur la transmission de signaux sur les réseaux, le degré de risque pour ces services peut être considéré, à certains égards, comme étant inférieur à ce qu'il est pour les services de communications électroniques traditionnels. Il en va de même pour les services de communications interpersonnelles fondés sur la numérotation et qui n'exercent aucun contrôle effectif sur la transmission de signaux.

(51) Le marché intérieur dépend plus que jamais du fonctionnement d'internet. Les services de la quasi-totalité des entités essentielles et importantes dépendent de services fournis sur internet. Afin d'assurer la prestation harmonieuse des services fournis par les entités essentielles et importantes, il est important que les réseaux de communications électroniques publics, comme les dorsales internet ou les câbles de communication sous-marins, disposent de mesures de cybersécurité appropriées et signalent les incidents qui les concernent.

(52) […] **Le cas échéant**, les entités devraient informer les destinataires de leurs services […] des mesures **particulières** qu'ils peuvent prendre pour atténuer le risque qui […] résulte pour eux **d'une cybermenace importante**. **Les entités devraient, lorsque c'est approprié et en particulier dans les cas où la cybermenace importante peut se matérialiser, informer également de la menace elle-même les destinataires de leurs services, parallèlement aux autorités compétentes ou aux CSIRT.** L'obligation qui est faite aux entités d'informer les destinataires de ces menaces ne devrait pas les dispenser de l'obligation de prendre immédiatement, à leurs frais, les mesures appropriées pour prévenir ou remédier à toute cybermenace pour la sécurité et pour rétablir le niveau normal de sécurité du service. Informer les destinataires au sujet des **cyber**menaces […] devrait être gratuit.

(53) Plus particulièrement, il convient que les fournisseurs de réseaux de communications électroniques publics ou de services de communications électroniques accessibles au public informent les destinataires des services des cybermenaces particulières et importantes pour la sécurité et des mesures qu'ils peuvent prendre pour sécuriser leurs communications, par exemple en recourant à des types spécifiques de logiciels ou de techniques de chiffrement.

(54) Afin de préserver la sécurité des réseaux et services de communications électroniques, il convient d'encourager l'utilisation du chiffrement, notamment du chiffrement de bout en bout, voire si nécessaire de l'imposer, pour les fournisseurs de ces services et réseaux, conformément aux principes de sécurité et de respect de la vie privée par défaut et dès la conception aux fins de l'article 18. Il convient de concilier l'utilisation du chiffrement de bout en bout avec les pouvoirs dont disposent les États membres pour garantir la protection de leurs intérêts essentiels de sécurité et de la sécurité publique et pour permettre la détection d'infractions pénales et les enquêtes et poursuites en la matière, dans le respect du droit de l'Union. Les solutions pour un accès légal aux informations contenues dans les communications chiffrées de bout en bout devraient préserver l'efficacité du cryptage pour ce qui est de la protection de la vie privée et de la sécurité des communications, tout en apportant une réponse efficace à la criminalité.

(55) La présente directive établit une approche en deux étapes du signalement des incidents afin de trouver le juste équilibre entre, d'une part, le signalement rapide qui aide à atténuer la propagation potentielle des incidents et permet aux entités de chercher de l'aide et, d'autre part, le signalement approfondi qui permet de tirer des leçons précieuses des incidents individuels et d'améliorer au fil du temps la résilience des entreprises individuelles et de secteurs tout entiers face aux cybermenaces. Lorsque les entités prennent connaissance d'un incident, elles devraient être tenues de présenter une notification initiale dans les 24 heures, suivie d'un rapport final un mois après au plus tard. La notification initiale ne devrait inclure que les informations strictement nécessaires pour porter l'incident à la connaissance des autorités compétentes et permettre à l'entité de demander une assistance, le cas échéant. Cette notification, le cas échéant, devrait indiquer si l'incident semble être causé par des actions illégales ou malveillantes. Les États membres devraient veiller à ce que l'obligation de présenter cette notification initiale ne détourne pas les ressources de l'entité effectuant le signalement des activités liées à la gestion de l'incident, qui doivent être prioritaires. Afin d'éviter que les obligations de signalement des incidents détournent les ressources des activités de gestion des incidents ou compromettent de quelque manière que ce soit les efforts déployés par les entités à cet égard, les États membres devraient également prévoir que, dans des cas dûment justifiés et en accord avec les autorités compétentes ou avec le CSIRT, l'entité concernée peut ne pas respecter les délais de 24 heures pour la notification initiale et de un mois pour le rapport final.

(55 *bis*) Une approche proactive à l'égard des cybermenaces est un élément essentiel de la gestion des risques en matière de cybersécurité, qui devrait permettre aux autorités compétentes d'éviter efficacement que les cybermenaces ne se matérialisent en incidents réels susceptibles de causer des pertes matérielles ou immatérielles considérables. À cette fin, le signalement des cybermenaces importantes revêt une importance capitale.

(56) Les entités essentielles et importantes se retrouvent souvent dans une situation dans laquelle un incident en particulier, en raison de ses caractéristiques, doit être signalé à différentes autorités en raison d'obligations de notification incluses dans différents instruments juridiques. De tels cas créent des charges supplémentaires et peuvent également conduire à des incertitudes en ce qui concerne le format et les procédures de ces notifications. C'est pourquoi, afin de simplifier le signalement des incidents de sécurité, les États membres […] **pourraient** mettre en place un *point d'entrée unique* pour toutes les notifications requises en vertu de la présente directive et d'autres actes législatifs de l'Union, comme le règlement (UE) 2016/679 et la directive 2002/58/CE. L'ENISA, en collaboration avec le groupe de coopération, devrait mettre au point des formulaires de notification communs au moyen de lignes directrices qui permettraient de simplifier et de rationaliser les informations de signalement exigées par le droit de l'Union et de réduire les charges pesant sur les entreprises.

(57) Lorsqu'il y a lieu de suspecter qu'un incident est lié à des activités criminelles graves au regard du droit de l'Union ou du droit national, les États membres devraient encourager les entités essentielles et importantes, sur la base de leurs procédures pénales applicables conformément au droit de l'Union, à signaler aux autorités répressives compétentes tout incident de ce type. Le cas échéant, et sans préjudice des règles de protection des données à caractère personnel applicables à Europol, il est souhaitable que la coordination entre les autorités compétentes et les autorités répressives de différents États membres soit facilitée par le CE3 et l'ENISA.

(58) Dans de nombreux cas, des données à caractère personnel sont compromises à la suite d'incidents. Dans de telles circonstances, les autorités compétentes devraient coopérer et échanger des informations sur tous les aspects pertinents avec les autorités chargées de la protection des données et les autorités de contrôle conformément à la directive 2002/58/CE.

(59) Le maintien à jour des bases de données précises et complètes de noms de domaines et de données d'enregistrement (appelées "données WHOIS") ainsi que la fourniture d'un accès licite à ces données sont essentiels pour garantir la sécurité, la stabilité et la résilience du système de noms de domaines (DNS), lequel contribue en retour à assurer un niveau élevé commun de cybersécurité dans l'Union. Lorsque le traitement comprend des données à caractère personnel, ce traitement doit s'effectuer conformément au droit de l'Union en matière de protection des données.

(60) La disponibilité de ces données, et leur accessibilité, en temps opportun, pour les autorités publiques, y compris les autorités compétentes en vertu du droit de l'Union ou du droit national en matière de prévention d'infractions pénales, d'enquêtes et de poursuites en la matière, les CERT (ou CSIRT) et, en ce qui concerne les données de leurs clients, pour les fournisseurs de réseaux et de services de communications électroniques et les fournisseurs de technologies et de services de cybersécurité agissant pour le compte de ces clients, sont essentielles pour prévenir et à combattre l'utilisation abusive des noms de domaines, en particulier pour prévenir, détecter et répondre aux incidents de cybersécurité. Cet accès doit être conforme au droit de l'Union en matière de protection des données dans la mesure où il concerne des données à caractère personnel.

(61) Afin d'assurer la disponibilité de données exactes et complètes sur l'enregistrement des noms de domaines, les registres des noms de domaines de premier niveau ainsi que les entités qui fournissent des services d'enregistrement de noms de domaines pour le registre de noms de domaines de premier niveau (appelées "bureaux d'enregistrement") doivent collecter et garantir l'intégrité et la disponibilité des données relatives à l'enregistrement des noms de domaines. **En ce qui concerne les données d'enregistrement, les entités devraient notamment vérifier le nom et l'adresse électronique du titulaire du nom de domaine.** […] Les registres de noms domaines de premier niveau ainsi que les entités fournissant des services d'enregistrement de noms de domaines pour le registre de noms de domaines de premier niveau devraient établir des politiques et des procédures aux fins de collecter et maintenir des données d'enregistrement exactes et complètes, ainsi que pour prévenir et corriger les données d'enregistrement inexactes, conformément aux règles de l'Union en matière de protection des données.

(62) Les registres des noms de domaines de premier niveau ainsi que les entités leur fournissant des services d'enregistrement de noms de domaines devraient rendre publiques les données relatives à l'enregistrement de noms de domaines qui ne relèvent pas du champ d'application des règles de l'Union en matière de protection des données, telles que les données concernant les personnes morales[25]. Les registres des noms de domaines de premier niveau ainsi que les entités fournissant des services d'enregistrement de noms de domaines pour le registre de noms de domaines de premier niveau devraient également permettre aux demandeurs d'accès légitimes d'accéder légalement à des données spécifiques d'enregistrement de noms de domaines concernant des personnes physiques, conformément à la législation de l'Union sur la protection des données. Les États membres devraient veiller à ce que les registres des noms de domaines de premier niveau ainsi que les entités qui leur fournissent des services d'enregistrement de noms de domaines répondent dans les meilleurs délais aux demandes de divulgation de données d'enregistrement de noms de domaines émanant de demandeurs d'accès légitimes, **par exemple les autorités compétentes, en droit de l'Union ou en droit national, dans le domaine de la sécurité nationale et de la justice pénale, ou les CSIRT**. Les registres des noms de domaines de premier niveau ainsi que les entités qui leur fournissent des services d'enregistrement de noms de domaines devraient établir des politiques et des procédures entourant la publication et la divulgation des données d'enregistrement, y compris des accords de niveau de service régissant la gestion des demandes d'accès des demandeurs d'accès légitimes. La procédure d'accès peut également inclure l'utilisation d'une interface, d'un portail ou d'un autre outil technique afin de fournir un système efficace de demande et d'accès aux données d'enregistrement. **Les États membres devraient veiller à ce que tous les types d'accès aux données d'enregistrement de nom de domaine (à caractère personnel ou non) soient gratuits.** En vue de promouvoir des pratiques harmonisées dans l'ensemble du marché intérieur, la Commission peut adopter des lignes directrices eu égard à ces procédures sans préjudice des compétences du comité européen de la protection des données, **en conformité et complémentarité avec les normes internationales élaborées par la communauté multipartite**.

---

25 Le considérant (14) du règlement (UE) 2016/679 du Parlement européen et du Conseil indique que "[l]e présent règlement ne couvre pas le traitement des données à caractère personnel qui concernent les personnes morales, et en particulier des entreprises dotées de la personnalité juridique, y compris le nom, la forme juridique et les coordonnées de la personne morale".

(63) […] Les entités essentielles et importantes au sens de la présente directive devraient relever de la compétence de l'État membre dans lequel elles fournissent leurs services. **Les entités visées à l'annexe I, points 1 à 7 et 10, les prestataires de services de confiance et les fournisseurs de points d'échange internet visés à l'annexe I, point 8, et à l'annexe II, points 1 à 5, de la présente directive devraient relever de la compétence de l'État membre dans lequel ils sont établis.** Si l'entité fournit des services **ou a son établissement** dans plus d'un État membre, elle doit dès lors relever de la juridiction distincte et concurrente de chacun de ces États membres. Les autorités compétentes de ces États membres devraient coopérer, se prêter mutuellement assistance et, le cas échéant, mener des actions communes de surveillance. **Lorsque les États membres décident d'exercer leur compétence, ils devraient éviter que le même comportement soit sanctionné plus d'une fois pour violation des obligations prévues par la présente directive.**

(64) Afin de tenir compte de la nature transfrontalière des services et des opérations des fournisseurs de services DNS, des registres des noms de domaines de premier niveau, **des entités fournissant des services d'enregistrement de noms de domaine pour les domaines de premier niveau**, des fournisseurs de réseaux de diffusion de contenu, des fournisseurs de services d'informatique en nuage, des fournisseurs de services de centre de données et des fournisseurs de service numérique, un seul État membre devrait avoir compétence eu égard à ces entités. La compétence devrait être attribuée à l'État membre dans lequel l'entité concernée a son principal établissement dans l'Union. Le critère d'établissement aux fins de la présente directive suppose l'exercice effectif d'une activité au moyen d'une installation stable. La forme juridique retenue pour un tel dispositif, qu'il s'agisse d'une succursale ou d'une filiale ayant la personnalité juridique, n'est pas déterminante à cet égard.

Le respect de ce critère ne devrait pas dépendre de la localisation physique du réseau et des systèmes d'information dans un lieu donné; la présence et l'utilisation de tels systèmes ne constituent pas en soi l'établissement principal et ne sont donc pas des critères déterminants permettant de déterminer l'établissement principal. L'établissement principal devrait être le lieu où sont **principalement** prises les décisions relatives aux mesures de gestion des risques en matière de cybersécurité dans l'Union. Cela correspondra généralement au lieu d'administration centrale des entreprises dans l'Union. **Si le lieu où ces décisions sont principalement prises ne peut pas être déterminé ou** si ces décisions ne sont pas prises dans l'Union, l'établissement principal doit être considéré comme se trouvant dans les États membres où l'entité possède un établissement avec le plus grand nombre de salariés dans l'Union. Lorsque les services sont effectués par un groupe d'entreprises, l'établissement principal de l'entreprise qui exerce le contrôle devrait être considéré comme étant l'établissement principal du groupe d'entreprises.

(64 *bis*) Lorsqu'un service DNS récursif est fourni par un fournisseur de réseaux publics de communications électroniques ou de services de communications électroniques accessibles au public uniquement dans le cadre du service d'accès à l'internet, l'entité devrait être réputée relever de la compétence de tous les États membres dans lesquels ses services sont fournis.

(64 *bis bis*) Afin de garantir une vue d'ensemble claire des fournisseurs de services DNS, des registres de noms de domaine de premier niveau, des entités fournissant des services d'enregistrement des noms de domaine pour le registre de noms de domaine de premier niveau, des fournisseurs de réseaux de diffusion de contenu, des fournisseurs de services d'informatique en nuage, des fournisseurs de services de centre de données et des fournisseurs de services numériques offrant leurs services dans toute l'Union et relevant du champ d'application de la présente directive, l'ENISA devrait créer et tenir à jour un registre pour ces entités, sur la base des notifications reçues des États membres, le cas échéant par l'intermédiaire de leurs mécanismes nationaux d'autonotification. Afin de garantir l'exactitude et l'exhaustivité des informations qui devraient figurer dans ce registre, les États membres devraient soumettre à l'ENISA les informations disponibles dans leurs registres nationaux sur ces entités. L'ENISA et les États membres devraient prendre des mesures pour faciliter l'interopérabilité de ces registres, tout en assurant la protection des informations confidentielles ou classifiées.

(65) Dans les cas où un fournisseur de services DNS, un registre de noms de domaines de premier niveau, un fournisseur de réseau de diffusion de contenu, un fournisseur de services d'informatique en nuage, un fournisseur de services de centre de données ou un fournisseur de service numérique non établi dans l'Union propose des services à l'intérieur de l'Union, il devrait désigner un représentant. Afin de déterminer si une telle entité propose des services dans l'Union, il convient d'examiner s'il apparaît qu'elle envisage d'offrir des services à des personnes dans un ou plusieurs États membres. La seule accessibilité, dans l'Union, du site internet de l'entité ou d'un intermédiaire ou d'une adresse électronique et d'autres coordonnées ou encore l'utilisation d'une langue généralement utilisée dans le pays tiers où l'entité est établie ne suffisent pas pour établir une telle intention. Cependant, des facteurs tels que l'utilisation d'une langue ou d'une monnaie généralement utilisée dans un ou plusieurs États membres avec la possibilité de commander des services dans cette autre langue ou la mention de clients ou d'utilisateurs qui se trouvent dans l'Union peuvent indiquer que l'entité envisage d'offrir des services dans l'Union. Le représentant devrait agir pour le compte de l'entité et devrait pouvoir être contacté par les autorités compétentes ou les CSIRT. Le représentant devrait être expressément désigné par un mandat écrit de l'entité le chargeant d'agir en son nom pour remplir les obligations, y compris la notification des incidents, qui lui incombent en vertu de la présente directive.

(66) Lorsque des informations considérées comme classifiées en vertu du droit national ou du droit de l'Union sont échangées, communiquées ou partagées d'une autre manière en vertu des dispositions de la présente directive, les règles spécifiques correspondantes relatives au traitement des informations classifiées doivent être appliquées.

(67) Face à la complexité et la sophistication croissantes des cybermenaces, l'efficacité des mesures de détection et de prévention dépend dans une large mesure de l'échange régulier de renseignements sur les menaces et les vulnérabilités entre les entités. Le partage d'informations contribue à accroître la sensibilisation aux cybermenaces, laquelle renforce à son tour la capacité des entités à empêcher les menaces de se concrétiser en incidents réels et leur permet de mieux contenir les effets des incidents et de se rétablir plus efficacement. En l'absence d'orientations au niveau de l'Union, plusieurs facteurs semblent avoir entravé ce partage de renseignements, notamment l'incertitude quant à la compatibilité avec les règles en matière de concurrence et de responsabilité.

(68) Les entités devraient être encouragées à exploiter collectivement leurs connaissances individuelles et leur expérience pratique aux niveaux stratégique, tactique et opérationnel en vue d'améliorer leurs capacités à évaluer, surveiller, se défendre et répondre de manière adéquate aux cybermenaces. Il est donc nécessaire de permettre l'émergence, au niveau de l'Union, d'accords de partage volontaire d'informations. À cette fin, les États membres devraient activement soutenir et encourager également les entités concernées qui ne relèvent pas du champ d'application de la présente directive à participer à ces mécanismes d'échange d'informations. Ces mécanismes devraient être opérés dans le plein respect des règles de concurrence de l'Union ainsi que des règles du droit de l'Union en matière de protection des données.

(69) […] **D**ans la mesure strictement nécessaire et proportionnée aux fins de garantir la sécurité du réseau et des informations, **le traitement de données à caractère personnel** par des entités **essentielles et importantes** […] et des fournisseurs de technologies et de services de sécurité **pourrait être jugé nécessaire aux fins du respect d'une obligation légale ou** […] constituer un intérêt légitime du responsable du traitement concerné, tel que visé dans le règlement (UE) 2016/679. Cela […] **pourrait** comprendre des mesures liées à la prévention, à la détection, à l'analyse et à la réaction aux incidents, des mesures de sensibilisation à des cybermenaces spécifiques, l'échange d'informations dans le cadre de la correction des vulnérabilités et de la divulgation coordonnée, ainsi que l'échange volontaire d'informations sur ces incidents, les cybermenaces et les vulnérabilités, de même que les indicateurs de compromis, les tactiques, techniques et procédures, les alertes de cybersécurité et les outils de configuration. Ces mesures peuvent nécessiter le traitement […] **de différents** types de données à caractère personnel […]**, par exemple**: adresses IP, localisateurs de ressources uniformes (URL), noms de domaines et adresses électroniques. **Le traitement des données à caractère personnel par les autorités compétentes, les points de contact uniques et les CSIRT devrait être prévu par le droit national et considéré comme nécessaire au respect d'une obligation légale ou à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement, conformément à l'article 6, paragraphe 1, point c) ou e), du règlement (UE) 2016/679.**

(69 *bis*) Les législations des États membres peuvent établir des règles permettant aux autorités compétentes, aux points de contact uniques et aux CSIRT, dans la mesure où cela est strictement nécessaire et proportionné aux fins d'assurer la sécurité des réseaux et des systèmes d'information d'entités essentielles et importantes, de traiter des catégories particulières de données à caractère personnel conformément à l'article 9, paragraphe 1, du règlement (UE) 2016/679, notamment en prévoyant des mesures appropriées et spécifiques de protection des droits fondamentaux et des intérêts des personnes physiques, y compris des limitations techniques à la réutilisation de ces données et le recours aux mesures les plus avancées de protection de la sécurité et de la vie privée, par exemple la pseudonymisation ou le cryptage lorsque l'anonymisation peut avoir une incidence significative sur l'objectif poursuivi.

(70) Afin de renforcer les pouvoirs et actions de surveillance qui contribuent à assurer un respect effectif des règles, la présente directive devrait prévoir une liste minimale d'actions et de moyens de surveillance par lesquels les autorités compétentes peuvent contrôler les entités essentielles et importantes. En outre, la présente directive devrait établir une différenciation du régime de surveillance entre les entités essentielles et les entités importantes en vue de garantir un juste équilibre des obligations tant pour les entités que pour les autorités compétentes. Ainsi, les entités essentielles devraient être soumises à un régime de surveillance à part entière (ex ante et ex post), tandis que les entités importantes devraient pour leur part être soumises à un régime de surveillance léger, uniquement ex post. Pour ces dernières, cela signifie que les entités importantes ne […] **devraient** pas **être** tenues de documenter systématiquement le respect des exigences en matière de gestion des risques de cybersécurité, tandis que les autorités compétentes sont quant à elles invitées à mettre en œuvre une approche réactive de la surveillance ex post et, par conséquent, ne pas être assujetties à une obligation générale de surveillance de ces entités. **Pour les entités importantes, la surveillance ex post peut être déclenchée par des éléments ou toute indication ou information portés à la connaissance des autorités compétentes et considérés par ces autorités comme suggérant un manquement potentiel aux obligations prévues par la présente directive. Par exemple, ces éléments, indications ou informations pourraient être du type fourni aux autorités compétentes par d'autres autorités, entités, citoyens, médias ou autres sources, ou des informations publiquement disponibles, ou pourraient résulter d'autres activités menées par les autorités compétentes dans l'accomplissement de leurs tâches.**

(70 *bis*) Lorsqu'elles exercent une surveillance ex ante , les autorités compétentes devraient être en mesure de fixer les priorités en ce qui concerne le recours proportionné aux mesures et moyens de surveillance dont elles disposent. Cela signifie que les autorités compétentes peuvent fixer ces priorités sur la base de méthodes de surveillance qui devraient suivre une approche fondée sur les risques. Plus précisément, ces méthodes pourraient inclure des critères ou des valeurs de référence pour le classement des entités essentielles en catégories de risque, et les mesures et moyens de surveillance correspondants recommandés par catégorie de risque, tels que l'utilisation, la fréquence ou le type d'inspections sur place, d'audits de sécurité ciblés ou de scans de sécurité, le type d'informations à demander et le niveau de détail de ces informations. Ces méthodes de surveillance peuvent également être accompagnées de programmes de travail et faire l'objet d'une évaluation et d'un réexamen réguliers, y compris sur des aspects tels que l'affectation des ressources et les besoins de ressources.

(70 *bis bis*) En ce qui concerne les entités de l'administration publique, les pouvoirs de surveillance devraient être exercés conformément aux cadres et à l'ordre juridique nationaux. Les États membres devraient pouvoir décider d'imposer à ces entités des mesures de surveillance et d'exécution appropriées, proportionnées et efficaces.

(70 *bis bis bis*) Pour qu'il soit démontré que certaines mesures de gestion des risques en matière de cybersécurité sont respectées, les États membres pourraient exiger des entités essentielles et importantes qu'elles utilisent des services de confiance qualifiés ou des schémas d'identification électronique notifiés en vertu du règlement (UE) n° 910/2014.

(71) Afin de rendre l'application effective, il convient d'établir une liste minimale de sanctions administratives pour violation des obligations de gestion des risques et de notification en matière de cybersécurité prévues par la présente directive, en établissant un cadre clair et cohérent pour ces sanctions dans toute l'Union. Il convient de tenir dûment compte de la nature, de la gravité et de la durée de la violation, des dommages ou pertes réels causés ou des dommages ou pertes potentiels qui auraient pu être provoqués, du caractère intentionnel ou négligent de la violation, des mesures prises pour prévenir ou atténuer les dommages et/ou pertes subis, du degré de responsabilité ou de toute violation antérieure pertinente, du degré de coopération avec l'autorité compétente et de toute autre circonstance aggravante ou atténuante. L'imposition de sanctions y compris d'amendes administratives devrait faire l'objet de garanties procédurales appropriées conformément aux principes généraux du droit de l'Union et de la charte des droits fondamentaux de l'Union européenne, y compris le droit à une protection juridictionnelle effective et à une procédure régulière.

(71 *bis*) Les dispositions relatives à la responsabilité des personnes physiques assumant certaines responsabilités au sein d'une entité en cas de manquement à leur obligation d'assurer le respect des obligations prévues par la présente directive n'exigent pas des États membres qu'ils garantissent des poursuites pénales ou la responsabilité civile pour les dommages causés à des tiers par ce manquement.

(72) Afin de garantir une application efficace des obligations prévues par la présente directive, chaque autorité compétente devrait avoir le pouvoir d'imposer ou de demander l'imposition d'amendes administratives.

(73) Lorsque des amendes administratives sont imposées à une entreprise, ce terme doit, à cette fin, être compris comme une entreprise conformément aux articles 101 et 102 du traité sur le fonctionnement de l'Union européenne. Lorsque des amendes administratives sont imposées à des personnes qui ne sont pas une entreprise, l'autorité de contrôle devrait tenir compte, lorsqu'elle examine quel serait le montant approprié de l'amende, du niveau général des revenus dans l'État membre ainsi que de la situation économique de la personne en cause. Il devrait appartenir aux États membres de déterminer si et dans quelle mesure les autorités publiques devraient faire l'objet d'amendes administratives. L'imposition d'une amende administrative n'affecte pas l'exercice d'autres pouvoirs par les autorités compétentes ou l'imposition d'autres sanctions prévues dans les dispositions nationales transposant la présente directive.

(74) Les États membres […] **peuvent** déterminer le régime des sanctions pénales applicables en cas de violations des dispositions nationales transposant la présente directive. Toutefois, l'imposition de sanctions pénales en cas de violation de ces dispositions nationales et l'imposition de sanctions administratives connexes ne devraient pas entraîner la violation du principe ne bis in idem tel qu'il a été interprété par la Cour de justice.

(75) Lorsque la présente directive n'harmonise pas les sanctions administratives ou, si nécessaire dans d'autres circonstances, par exemple en cas de violation grave des obligations prévues par la présente directive, les États membres devraient mettre en œuvre un système qui prévoit des sanctions effectives, proportionnées et dissuasives. La nature de ces sanctions, pénales ou administratives devrait être déterminée par le droit des États membres.

(76) Afin de renforcer encore l'efficacité et le caractère dissuasif des sanctions applicables aux violations des obligations prévues en vertu de la présente directive, les autorités compétentes devraient être habilitées à imposer des sanctions consistant en la suspension d'une certification ou d'une autorisation concernant tout ou partie des services fournis par une entité essentielle et en l'interdiction temporaire de l'exercice de fonctions de direction par une personne physique. Compte tenu de leur gravité et de leur incidence sur les activités des entités et, en définitive, sur leurs consommateurs, ces sanctions ne devraient être appliquées que proportionnellement à la gravité de la violation et en tenant compte des circonstances spécifiques de chaque cas, notamment le caractère intentionnel ou négligent de la violation, les mesures prises pour prévenir ou atténuer les dommages et/ou les pertes subis. Ces sanctions ne devraient être appliquées qu'à titre d'ultima ratio, c'est-à-dire uniquement après que les autres mesures d'exécution pertinentes prévues par la présente directive ont été épuisées, et seulement pendant la période durant laquelle les entités auxquelles elles s'appliquent prennent les mesures nécessaires pour remédier aux manquements ou se conformer aux exigences de l'autorité compétente pour laquelle ces sanctions ont été appliquées. L'imposition de ces sanctions est soumise à des garanties procédurales appropriées conformément aux principes généraux du droit de l'Union et à la charte des droits fondamentaux de l'Union européenne, y compris le droit à une protection juridictionnelle effective, une procédure régulière, la présomption d'innocence et les droits de la défense.

(76 *bis*) Afin d'assurer une surveillance et une exécution efficaces, notamment dans les affaires revêtant une dimension transfrontière, les États membres qui ont reçu une demande d'assistance mutuelle devraient, en fonction de la portée de la demande, prendre des mesures de surveillance et d'exécution appropriées à l'égard de l'entité concernée qui fournit des services ou dont le réseau et le système d'information se trouvent sur leur territoire.

(77) La présente directive devrait établir des règles de coopération entre les autorités compétentes et les autorités de contrôle conformément au règlement (UE) 2016/679 pour traiter les violations relatives aux données à caractère personnel.

(78) La présente directive devrait viser à assurer un niveau de responsabilité important pour les mesures de gestion des risques en matière de cybersécurité et les obligations de notification au niveau des organisations. Pour ces raisons, les organes de direction des entités entrant dans le champ d'application de la présente directive devraient approuver les mesures relatives aux risques en matière de cybersécurité et superviser leur mise en œuvre.

(79) Un […] **système d'apprentissage** par les pairs devrait être mis en place **pour contribuer au renforcement de la confiance mutuelle et tirer des enseignements des bonnes pratiques et des expériences acquises, ce qui ouvrirait la possibilité d'échanges entre pairs, parmi les** experts désignés par les États membres, **en ce qui concerne** […] la mise en œuvre des politiques de cybersécurité […]. **Lors de la mise en œuvre du système d'apprentissage par les pairs, il convient de veiller tout particulièrement à ce qu'il n'impose pas de charge inutile ou disproportionnée aux autorités compétentes des États membres. La Commission devrait étudier toutes les possibilités afin de garantir potentiellement la couverture financière des coûts qui pourraient découler de l'organisation de missions d'apprentissage par les pairs. En outre, le système d'apprentissage par les pairs devrait tenir compte des résultats de mécanismes similaires, comme le système d'évaluation par les pairs du réseau des CSIRT, apporter une valeur ajoutée et éviter les doubles emplois. La mise en œuvre du système d'apprentissage par les pairs devrait être sans préjudice de la législation nationale ou de l'Union relative à la protection des informations confidentielles et classifiées. Avant le début des cycles d'apprentissage par les pairs, les États membres peuvent procéder à une autoévaluation des aspects pertinents. À la demande du groupe de coopération, l'ENISA peut, lorsque c'est nécessaire, fournir des orientations sur l'autoévaluation et les modèles pertinents. Les États membres pourraient décider de rendre leurs rapports accessibles au public.**

(80) […]

(81) Afin d'assurer des conditions uniformes de mise en œuvre des dispositions pertinentes de la présente directive concernant les modalités de procédure nécessaires au fonctionnement du groupe de coopération, les éléments techniques des mesures de gestion des risques ou le type d'informations, le format et la procédure en ce qui concerne la notification des incidents, **ainsi que les catégories d'entités dont il doit être exigé qu'elles recourent à certains produits, services et processus TIC certifiés,** il convient de conférer des compétences d'exécution à la Commission. Ces compétences devraient être exercées conformément au règlement (UE) n° 182/2011 du Parlement européen et du Conseil[26].

(82) La présente directive devrait être réexaminée périodiquement par la Commission, en consultation avec les parties intéressées, notamment en vue de déterminer s'il est nécessaire de la modifier pour tenir compte de l'évolution de la société, de la situation politique, des technologies ou de la situation des marchés.

[26] Règlement (UE) n° 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 (JO L 55 du 28.2.2011, p. 13).

(83) Étant donné que l'objectif de la présente directive, qui vise à atteindre un niveau élevé commun de cybersécurité dans l'Union, ne peut pas être atteint de manière suffisante par les États membres mais peut, en raison des effets de l'action, l'être mieux au niveau de l'Union, celle-ci peut prendre des mesures, conformément au principe de subsidiarité consacré à l'article 5 du traité sur l'Union européenne. Conformément au principe de proportionnalité tel qu'énoncé audit article, la présente directive n'excède pas ce qui est nécessaire pour atteindre cet objectif.

(84) La présente directive respecte les droits fondamentaux et observe les principes reconnus par la charte des droits fondamentaux de l'Union européenne et, en particulier, le droit au respect de la vie privée et des communications, le droit à la protection des données à caractère personnel, le droit à la liberté d'entreprise, le droit de propriété ainsi que le droit à un recours effectif et à un procès équitable. La présente directive devrait être mise en œuvre conformément à ces droits et principes,

ONT ADOPTÉ LA PRÉSENTE DIRECTIVE:

CHAPITRE I

Dispositions générales

Article premier

Objet

1. La présente directive établit des mesures visant à assurer un niveau commun élevé de cybersécurité dans l'Union **de manière à améliorer le fonctionnement du marché intérieur**.

2. À cette fin, la présente directive:

   a) fixe des obligations aux États membres en ce qui concerne l'adoption de stratégies nationales de cybersécurité, la désignation d'autorités nationales compétentes, de points de contact uniques et d'équipes de réponse aux incidents de sécurité informatique (CSIRT);

   b) définit les obligations en matière de gestion et de signalement des risques de cybersécurité pour les entités d'un type [...] **visé aux annexes I et II**[...];

   c) fixe **des règles et** des obligations pour le partage d'informations en matière de cybersécurité.

Article 2

Champ d'application

1. La présente directive s'applique aux entités publiques et privées [...] d'un type [...] **figurant sur les listes aux annexes I et II qui atteignent ou dépassent les seuils pour les moyennes entreprises** [...] au sens de la recommandation 2003/361/CE de la Commission[27]. **L'article 3, paragraphe 4, et l'article 6, paragraphe 2, deuxième et troisième alinéas, de l'annexe de ladite recommandation ne s'appliquent pas aux fins de la présente directive.**

2. [...]**Q**uelle que soit l[...]**a** taille **des entités visées au paragraphe 1**, la présente directive s'applique également **dans les cas suivants**: […]

   a) les services sont fournis par l'une des entités suivantes:

      i) **des fournisseurs de** réseaux de communications électroniques publics ou de services de communications électroniques accessibles au public visés à l'annexe I, point 8;

      ii) **des prestataires de services de confiance qualifiés visés à l'annexe I, point XX;**

      iii) **des prestataires de services de confiance non qualifiés visés à l'annexe I, point XX;**

      iv) des registres des noms de domaines de premier niveau [...] visés à l'annexe I, point 8;

   b) […]

[27] Recommandation 2003/361/CE de la Commission du 6 mai 2003 concernant la définition des micro, petites et moyennes entreprises (JO L 124 du 20.5.2003, p. 36).

c) l'entité est**, dans un État membre,** le seul prestataire [...] **d'un service qui est essentiel au maintien de fonctions sociétales ou économiques critiques**;

d) une éventuelle interruption du service fourni par l'entité pourrait avoir une incidence **significative** sur la sécurité publique, la sûreté publique ou la santé publique;

e) une éventuelle perturbation du service fourni par l'entité pourrait induire des risques systémiques **significatifs**, en particulier pour les secteurs où cette perturbation pourrait avoir une incidence transfrontalière;

f) [...];

g) l'entité est identifiée comme une entité critique conformément à la directive (UE) XXXX/XXXX du Parlement européen et du Conseil[28] [directive sur la résilience des entités critiques], **[**ou comme une entité équivalente à une entité critique conformément à l'article 7 de cette directive**]**.

2 *bis*. La présente directive s'applique également, quelle que soit leur taille, aux entités de l'administration publique des pouvoirs publics centraux reconnues comme telles dans un État membre en vertu du droit national et visées à l'annexe I, point 9. Les États membres peuvent établir que la présente directive s'applique également aux entités de l'administration publique aux niveaux régional et local.

28 [insérer le titre complet et la référence de la publication au JO lorsqu'elle est connue]

3. […]

La présente directive est sans préjudice de la responsabilité des États membres en matière de protection de la sécurité nationale ou de leur pouvoir de sauvegarder d'autres fonctions essentielles de l'État, y compris la garantie de l'intégrité territoriale de l'État et le maintien de l'ordre public.

3 *bis*. 1) La présente directive ne s'applique pas:

a) aux entités qui ne relèvent pas du champ d'application du droit de l'Union, et en tout état de cause elle ne s'applique à aucune entité dont les activités portent en premier lieu sur les domaines de la défense, de la sécurité nationale, de la sécurité publique ou de l'application de la loi, quelle que soit l'entité qui exerce ces activités et indépendamment du fait qu'il s'agisse d'une entité publique ou d'une entité privée;

b) aux entités qui exercent des activités dans les domaines de la justice, des parlements ou des banques centrales.[...]

2) Lorsque les activités portant sur ces domaines ne constituent qu'une partie des activités globales d'une entité de l'administration publique, ladite entité est entièrement exclue du champ d'application de la présente directive.

3 *bis bis*. La présente directive ne s'applique pas:

i) aux activités d'entités qui ne relèvent pas du champ d'application du droit de l'Union, et en tout état de cause elle ne s'applique à aucune activité relative à la défense ou à la sécurité nationale, quelle soit l'entité qui exerce ces activités et indépendamment du fait qu'il s'agisse d'une entité publique ou d'une entité privée;

ii) aux activités d'entités dans les domaines de la justice, des parlements, des banques centrales et de la sécurité publique, ce qui concerne aussi les entités de l'administration publique exerçant des activités répressives à des fins de prévention, d'enquête, de détection d'infraction et de poursuite en matière pénale, ou d'exécution de sanctions pénales.

3 *bis bis bis*. Les obligations fixées par la présente directive n'impliquent pas la fourniture d'informations dont la divulgation est contraire aux intérêts essentiels des États membres en matière de sécurité nationale, de sécurité publique ou de défense.

3 *bis bis bis bis*.La présente directive est sans préjudice du droit de l'Union concernant la protection des données à caractère personnel, en particulier du règlement (UE) 2016/679 et de la directive 2002/58/CE.

3 *ter*. La présente directive ne s'applique pas aux entités exemptées des dispositions du règlement (UE) XXXX/XXXX du Parlement européen et du Conseil [règlement sur la résilience opérationnelle numérique du secteur financier] conformément à l'article 2, paragraphe 4, du règlement sur la résilience opérationnelle numérique du secteur financier.

4. La présente directive est sans préjudice [...][29] [...]des directives 2011/93/UE[30] et 2013/40/UE[31] du Parlement européen et du Conseil.

5. Sans préjudice de l'article 346 du traité sur le fonctionnement de l'Union européenne, les informations considérées comme confidentielles en application de la réglementation nationale et de l'Union, telle que les règles applicables au secret des affaires, ne peuvent faire l'objet d'un échange avec la Commission et d'autres autorités concernées **conformément à la présente directive** que si cet échange est nécessaire à l'application de la présente directive. Les informations échangées se limitent au minimum nécessaire et sont proportionnées à l'objectif de cet échange. L'échange d'informations préserve la confidentialité des informations concernées et protège la sécurité et les intérêts commerciaux des entités essentielles ou importantes.

---

29 [...]

30 Directive 2011/93/UE du Parlement européen et du Conseil du 13 décembre 2011 relative à la lutte contre les abus sexuels et l'exploitation sexuelle des enfants, ainsi que la pédopornographie et remplaçant la décision-cadre 2004/68/JAI du Conseil (JO L 335 du 17.12.2011, p. 1).

31 Directive 2013/40/UE du Parlement européen et du Conseil du 12 août 2013 relative aux attaques contre les systèmes d'information et remplaçant la décision-cadre 2005/222/JAI du Conseil (JO L 218 du 14.8.2013, p. 8).

Article 2 bis

Entités essentielles et entités importantes

1. Parmi les entités auxquelles s'applique la présente directive, sont considérées comme essentielles:

i) les entités d'un type prévu aux points 1 à 8 *bis* et 10 de l'annexe I de la présente directive qui dépassent les seuils pour les moyennes entreprises au sens de la recommandation 2003/361/CE de la Commission;

ii) les moyennes entités visées à l'article 2, paragraphe 2, point a) i);

iii) les entités visées à l'article 2, paragraphe 2, points a) ii) et iv), de la présente directive, quelle que soit leur taille;

iv) les entités visées à l'article 2, paragraphe 2, point g), et à l'article 2, paragraphe 2 *bis*, de la présente directive, quelle que soit leur taille;

v) si c'est établi par les États membres, les entités que les États membres ont définies, avant l'entrée en vigueur de la présente directive, comme des opérateurs de services essentiels conformément à la directive (UE) 2016/1148 ou au droit national;

vi) les entités dépassant les seuils pour les moyennes entreprises au sens de la recommandation 2003/361/CE de la Commission du type prévu à l'annexe II que les États membres déterminent comme essentielles sur la base des critères visés à l'article 2, paragraphe 2, points c) à e);

vii) les moyennes entités au sens de la recommandation 2003/361/CE de la Commission que les États membres déterminent comme essentielles sur la base des critères visés à l'article 2, paragraphe 2, points c) à e);

viii) les micro ou petites entités au sens de la recommandation 2003/361/CE de la Commission prévue au paragraphe 2), point a) i), ou identifiées conformément au paragraphe 2), points c) à e), du présent article, que les États membres déterminent comme essentielles sur la base d'évaluations des risques nationales.

2. Parmi les entités auxquelles s'applique la présente directive, sont considérées comme importantes:

i) les entités d'un type prévu à l'annexe I de la présente directive qualifiables de moyennes entreprises au sens de la recommandation 2003/361/CE de la Commission et les entités du type prévu à l'annexe II qui atteignent ou dépassent les seuils des moyennes entreprises au sens de la recommandation 2003/361/CE de la Commission[32];

ii) les entités visées à l'article 2, paragraphe 2, point a) iii), de la présente directive, quelle que soit leur taille;

iii) les petites et micro entités visées à l'article 2, paragraphe 2, point a) i);

iv) les petites et micro entités que les États membres considèrent comme des entités importantes sur la base de l'article 2, paragraphe 2, points c) à e).

32 Recommandation 2003/361/CE de la Commission du 6 mai 2003 concernant la définition des micro, petites et moyennes entreprises (JO L 124 du 20.5.2003, p. 36).

Article 2 bis

Mécanismes de signalement

1. **Les États membre peuvent mettre en place des mécanismes nationaux d'autosignalement, selon lesquels toutes les entités relevant de la présente directive devraient communiquer, aux autorités compétentes en vertu de la présente directive ou aux organismes désignés à cet effet par les États membres, au minimum leur nom, leur adresse et leurs coordonnées, ainsi que le secteur dans lequel elles exercent leurs activités ou le type de service qu'elles fournissent, et, le cas échéant, une liste des États membres dans lesquels elles fournissent leurs services relevant de la présente directive.**

2. Les États membres [...] **communiquent à la Commission, en ce qui concerne les entités qu'ils ont identifiées au titre de l'article 2, paragraphe 2, points b) à e), au moins des informations pertinentes sur le nombre d'entités identifiées, le secteur auquel elles appartiennent ou le type de services définis aux annexes qu'elles fournissent, et la ou les dispositions précises de l'article 2, paragraphe 2, sur la base desquelles elles avaient été identifiées à la date du [12 mois après le délai de transposition de la présente directive].** Les États membres réexaminent [...] **ces informations** [...] régulièrement, puis au moins tous les deux ans, et, le cas échéant, [...]**les** mettent à jour.

Article 2 ter

Actes sectoriels de l'Union

1. Lorsque des [...] **actes juridiques sectoriels** de l'Union imposent à des entités essentielles ou importantes [...] d'adopter des mesures de gestion des risques en matière de cybersécurité [...] **ou** de notifier des incidents ou des cybermenaces [...] **importants**, et lorsque ces exigences sont au moins équivalentes dans leurs effets aux obligations prévues par la présente directive, les dispositions pertinentes de la présente directive, y compris [...]**les** disposition**s** relative**s** à la surveillance et à l'exécution prévue**s** au chapitre VI, ne sont pas applicables **auxdites entités**. **Lorsque des actes sectoriels de l'Union ne couvrent pas toutes les entités d'un secteur spécifique relevant du champ d'application de la présente directive, les dispositions pertinentes de la présente directive continuent de s'appliquer aux entités non couvertes par ces dispositions sectorielles.**

2. Les exigences visées au paragraphe 1 du présent article sont considérées comme équivalentes aux obligations prévues par la présente directive si l'acte sectoriel de l'Union concerné prévoit un accès immédiat, le cas échéant automatique et direct, aux signalements d'incidents par les autorités compétentes au titre de la présente directive ou par les CSIRT désignés, et si:

a) les mesures de gestion des risques en matière de cybersécurité sont au moins équivalentes dans leurs effets à celles prévues à l'article 18, paragraphes 1 et 2, de la présente directive; ou si

b) les exigences de signalement d'incidents importants sont au moins équivalentes dans leurs effets à celles prévues à l'article 20, paragraphes 1 à 6.

3. La Commission réexamine périodiquement l'application de l'exigence selon laquelle les dispositions sectorielles d'un acte juridique de l'Union devraient avoir un effet équivalent à celui des exigences prévues aux paragraphes 1 et 2 du présent article. La Commission consulte le groupe de coopération et l'ENISA lorsqu'elle prépare ces réexamens périodiques.

Article 3

Harmonisation minimale

Sans préjudice des autres obligations qui leur incombent en vertu du droit de l'Union, les États membres peuvent [...] adopter ou maintenir des dispositions assurant un niveau plus élevé de cybersécurité **dans les domaines couverts par la présente directive**.

Article 4

Définitions

Aux fins de la présente directive, on entend par:

1) "réseau et système d'information",

   a) un réseau de communications électroniques au sens de l'article 2, point 1), du règlement (UE) 2018/1972;

   b) tout dispositif ou tout ensemble de dispositifs interconnectés ou apparentés, dont un ou plusieurs éléments assurent, en exécution d'un programme, un traitement automatisé de données numériques;

   c) les données numériques stockées, traitées, récupérées ou transmises par les éléments visés aux points a) et b) en vue de leur fonctionnement, utilisation, protection et maintenance;

2) "sécurité des réseaux et des systèmes d'information", la capacité des réseaux et des systèmes d'information de résister, à un niveau de confiance donné, à **tout événement susceptible de compromettre** [...] la disponibilité, l'authenticité, l'intégrité ou la confidentialité de données stockées, transmises ou faisant l'objet d'un traitement, ou des services [...] que ces réseaux et systèmes d'information offrent ou rendent accessibles;

2 *bis*) "service de communications électroniques", tout service de communications électroniques au sens de l'article 2, point 4, de la directive (UE) 2018/1972;

3) "cybersécurité", la cybersécurité au sens de l'article 2, point 1, du règlement (UE) 2019/881 du Parlement européen et du Conseil[33];

4) "stratégie nationale [...] de cybersécurité", le cadre cohérent d'un État membre fournissant **une gouvernance en vue d'atteindre** des objectifs et des priorités stratégiques **dans le domaine de** [...] **la cybersécurité** [...] dans cet État membre;

5) "incident", tout événement compromettant la disponibilité, l'authenticité, l'intégrité ou la confidentialité des données stockées, transmises ou faisant l'objet d'un traitement ou des services [...] que ces réseaux et systèmes d'information offrent ou rendent accessibles;

5 *bis*) "incident majeur de cybersécurité", un incident ayant une incidence significative sur au moins deux États membres ou qui provoque des perturbations dépassant les capacités d'un État membre à y réagir;

---

33 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) (JO L 151 du 7.6.2019, p. 15).

6) "traitement des incidents", toutes les actions et procédures visant à détecter, analyser et contenir un incident et à y répondre;

6 *bis*) "risque", le potentiel de perte ou de perturbation causé par un incident, exprimé comme la combinaison de l'ampleur de cette perte ou de cette perturbation et de la probabilité que ledit incident se produise;

7) "cybermenace", une cybermenace au sens de l'article 2, point 8, du règlement (UE) 2019/881;

7 *bis*) **"cybermenace majeure", une cybermenace qui, compte tenu de ses caractéristiques techniques, peut être considérée comme susceptible d'avoir une incidence grave sur les réseaux et les systèmes d'information d'une entité ou de ses utilisateurs en causant des pertes matérielles ou immatérielles considérables;**

8) "vulnérabilité", une faiblesse, une susceptibilité ou la faille d'un actif informatique ou d'un système [...] qui peut être exploitée par une cybermenace;

8 *bis*) "incident évité", un événement qui aurait potentiellement pu causer des dommages aux réseaux et aux systèmes d'information d'une entité ou de ses utilisateurs, mais dont la réalisation totale a pu être empêchée;

9) "représentant", toute personne physique ou morale établie dans l'Union qui est expressément désignée pour agir pour le compte i) d'un fournisseur de services DNS, d'un registre de noms de domaines de premier niveau, d'un fournisseur d'informatique en nuage, d'un fournisseur de services de centre de données, d'un fournisseur de réseau de diffusion de contenu tel que désigné au point 8 de l'Annexe I ou ii) d'entités visées au point [...] **6** de l'annexe II non établies dans l'Union, qui peut être contactée par une autorité nationale compétente ou un CSIRT à la place de l'entité concernant les obligations incombant à ladite entité en vertu de la présente directive;

10) "norme", une norme au sens de l'article 2, point 1, du règlement (UE) 1025/2012 du Parlement européen et du Conseil[34];

11) "spécification technique", une spécification technique au sens de l'article 2, point 4, du règlement (UE) n° 1025/2012;

12) "point d'échange internet (IXP)" une structure de réseau qui permet l'interconnexion de plus de deux réseaux indépendants (systèmes autonomes), essentiellement aux fins de faciliter l'échange de trafic internet; un IXP n'assure l'interconnexion que pour des systèmes autonomes; un IXP n'exige pas que le trafic internet passant entre une paire quelconque de systèmes autonomes participants transite par un système autonome tiers, pas plus qu'il ne modifie ou n'altère par ailleurs un tel trafic;

13) "système de noms de domaines (DNS)", un système hiérarchique et distribué d'affectation de noms qui permet aux utilisateurs finaux d'accéder à des services et à des ressources sur l'internet;

14) "fournisseur de services DNS" une entité qui fournit des services de résolution de noms de domaines récursifs ou faisant autorité [...] **pour une utilisation par des tiers, à l'exception des serveurs racines de nom de domaine** [...];

---

34 Règlement (UE) n° 1025/2012 du Parlement européen et du Conseil du 25 octobre 2012 relatif à la normalisation européenne, modifiant les directives 89/686/CEE et 93/15/CEE du Conseil ainsi que les directives 94/9/CE, 94/25/CE, 95/16/CE, 97/23/CE, 2004/22/CE, 2007/23/CE, 2009/23/CE et 2009/105/CE du Parlement européen et du Conseil et abrogeant la décision 87/95/CEE du Conseil et la décision n° 1673/2006/CE du Parlement européen et du Conseil (JO L 316 du 14.11.2012, p. 12).

15) "registre de noms de domaines de premier niveau", une entité à laquelle un registre de noms de domaines de premier niveau spécifique a été délégué et qui est responsable de l'administration du registre de noms de domaines de premier niveau, y compris de l'enregistrement des noms de domaines sous le registre de noms de domaines de premier niveau et du fonctionnement technique du registre de noms de domaines de premier niveau, notamment l'exploitation de ses serveurs de noms, la maintenance de ses bases de données et la distribution des fichiers de zone du registre de noms de domaines de premier niveau sur les serveurs de noms, **tout en excluant les situations où les noms de domaine de premier niveau ne sont utilisés par un registre que pour son propre usage**;

15 *bis*) "entités fournissant des services d'enregistrement de noms de domaine pour les registres de noms de domaine de premier niveau", les registres de noms de domaine de premier niveau, les bureaux d'enregistrement des noms de domaine de premier niveau et les agents des bureaux d'enregistrement, tels que les revendeurs et les fournisseurs de services d'enregistrement fiduciaire;

16) "service numérique", un service au sens de l'article 1er, paragraphe 1, point b), de la directive (UE) 2015/1535 du Parlement européen et du Conseil[35];

16 *bis*) "service de confiance", un service de confiance au sens de l'article 3, point 16, du règlement (UE) n° 910/2014;

[35] Directive (UE) 2015/1535 du Parlement européen et du Conseil du 9 septembre 2015 prévoyant une procédure d'information dans le domaine des réglementations techniques et des règles relatives aux services de la société de l'information (JO L 241 du 17.9.2015, p. 1).

16 *ter*) "prestataire de services de confiance qualifié", un prestataire de services de confiance qualifié au sens de l'article 3, point 20, du règlement (UE) n° 910/2014;

17) "place de marché en ligne", un service numérique au sens de l'article 2, point n), de la directive 2005/29/CE du Parlement européen et du Conseil[36];

18) "moteur de recherche en ligne", un service numérique au sens de l'article 2, point 5, du règlement (UE) 2019/1150 du Parlement européen et du Conseil[37];

19) "service d'informatique en nuage", un service numérique qui permet l'administration à la demande et l'accès à distance à un ensemble modulable et variable de ressources informatiques [...] pouvant être partagées**, y compris lorsqu'elles sont réparties à différents endroits**;

20) "service de centre de données", un service qui englobe les structures, ou groupes de structures, dédiées à l'hébergement, l'interconnexion et l'exploitation centralisées des équipements de traitement de l'information et de réseau fournissant des services de stockage, de traitement et de transport des données, ainsi que l'ensemble des installations et infrastructures de distribution d'électricité et de contrôle environnemental;

---

36 Directive 2005/29/CE du Parlement européen et du Conseil du 11 mai 2005 relative aux pratiques commerciales déloyales des entreprises vis-à-vis des consommateurs dans le marché intérieur et modifiant la directive 84/450/CEE du Conseil et les directives 97/7/CE, 98/27/CE et 2002/65/CE du Parlement européen et du Conseil et le règlement (CE) n° 2006/2004 du Parlement européen et du Conseil (JO L 149 du 11.6.2005, p. 22).

37 Règlement (UE) 2019/1150 du Parlement européen et du Conseil du 20 juin 2019 promouvant l'équité et la transparence pour les entreprises utilisatrices de services d'intermédiation en ligne (JO L 186 du 11.7.2019, p. 57).

21) "réseau de diffusion de contenu", un réseau de serveurs géographiquement répartis visant à assurer la haute disponibilité, l'accessibilité ou la fourniture rapide de contenu et de services numériques aux utilisateurs d'internet pour le compte de fournisseurs de contenu et de services;

22) "plateforme de services de réseaux sociaux", une plateforme qui permet aux utilisateurs finaux de se connecter, de partager, de découvrir et de communiquer entre eux sur plusieurs terminaux, notamment par conversations en ligne, publications, vidéos et recommandations[...];

23) "entité de l'administration publique", une entité **reconnue comme telle dans un État membre conformément au droit national,** [...] qui satisfait aux critères suivants:

a) elle a été créée pour satisfaire des besoins d'intérêt général et n'a pas de caractère industriel ou commercial;

b) elle est dotée de la personnalité juridique **ou juridiquement habilitée à agir pour le compte d'une autre entité dotée de la personnalité juridique**;

c) elle est financée majoritairement par l'État, les collectivités régionales ou d'autres organismes de droit public; ou leur gestion est soumise à un contrôle de la part de ces autorités ou organes; ou leur organe d'administration, de direction ou de surveillance est composé de membres dont plus de la moitié sont désignés par l'État, les autorités régionales ou d'autres organismes de droit public;

d) elle a le pouvoir de signifier aux personnes physiques ou morales des décisions administratives ou réglementaires affectant leurs droits en matière de mouvements transfrontières des personnes, des biens, des services ou des capitaux.

24) "entité", toute personne physique ou morale constituée et reconnue comme telle en vertu du droit national de son lieu de constitution, et ayant, en son nom propre, la capacité d'être titulaire de droits et d'obligations;

25) "entité essentielle", toute entité d'un type [...] **prévu à l'annexe I et désignée comme "essentielle" conformément à l'article 2 *bis*, paragraphe 1**;

26) "entité importante", toute entité d'un type [...] **prévu aux annexes I et II et désignée comme "importante" conformément à l'article 2 *bis*, paragraphe 2**;

26 *bis*) "produit TIC", un produit TIC au sens de l'article 2, point 12, du règlement (UE) 2019/881;

26 *bis bis*) "service TIC", un service TIC au sens de l'article 2, point 13, du règlement (UE) 2019/881;

26 *bis ter*) "processus TIC", un processus TIC au sens de l'article 2, point 14, du règlement (UE) 2019/881;

26 *bis quater*) "fournisseur de services gérés", toute entité qui fournit des services, notamment de réseau, d'application, d'infrastructure et de sécurité, à travers des activités continues et régulières de gestion, de soutien et d'administration active dans les locaux des clients, dans le centre de données de leur fournisseur de services gérés (hébergement), ou dans un centre de données tiers.

26 *bis quinquies*) "fournisseur de services de sécurité gérés", toute entité qui assure de façon externalisée le suivi et la gestion des dispositifs et systèmes de sécurité. Les services communs comprennent les services gérés de pare-feu, de détection des intrusions, de réseau privé virtuel, d'examen de la vulnérabilité et d'antivirus.

Ils comprennent également le recours à des centres d'opération de sécurité à haute disponibilité (soit à partir de leurs propres installations, soit auprès d'autres fournisseurs de centres de données) pour fournir des services 24 heures sur 24 et 7 jours sur 7 conçus pour réduire le nombre d'agents de sécurité opérationnels qu'une entreprise a besoin de recruter, former et retenir pour maintenir une posture de sécurité acceptable.

CHAPITRE II

Cadres réglementaires coordonnés en matière de cybersécurité

Article 5

Stratégie nationale en matière de cybersécurité

1. Chaque État membre adopte une stratégie nationale en matière de cybersécurité qui définit les objectifs stratégiques et les mesures politiques et réglementaires appropriées, en vue de parvenir à un niveau élevé de cybersécurité et de le maintenir. La stratégie nationale en matière de cybersécurité comprend notamment les éléments suivants:

   a) [...]**les** objectifs et [...]**les** priorités de la stratégie des États membres en matière de cybersécurité;

   b) un cadre de gouvernance visant à atteindre ces objectifs et priorités, y compris les politiques visées au paragraphe 2 ainsi que les rôles et responsabilités des différents acteurs et autorités concernés par la mise en œuvre de la stratégie [...];

   c) [...] **des orientations** visant à déterminer les actifs pertinents et **à évaluer** les risques de cybersécurité dans cet État membre[...];

   d) un inventaire des mesures garantissant la préparation, la réaction et la récupération des services après incident, y compris la coopération entre les secteurs public et privé;

   e) […]

f) un cadre politique visant une coordination renforcée entre les autorités compétentes en vertu de la présente directive et de la directive (UE) XXXX/XXXX du Parlement européen et du Conseil[38] [directive sur la résilience des entités critiques] aux fins du partage d'informations sur les **risques en matière de sécurité,** [...] l**es menaces et les incidents dans les domaines cyber et non cyber,** et de l'exercice des tâches de contrôle**, en tant que de besoin**;

f *bis*) un cadre politique pour la coordination et la coopération entre les autorités compétentes en vertu de la présente directive et les autorités compétentes désignées en vertu de la législation sectorielle.

2. Dans le cadre de la stratégie nationale en matière de cybersécurité, les États membres adoptent notamment les politiques suivantes:

a) une politique traitant de la cybersécurité dans le cadre de la chaîne d'approvisionnement des produits et services TIC utilisés par des entités [...] pour la fourniture de leurs services;

b) **une politique** [...] concernant l'inclusion et la spécification d'exigences liées à la cybersécurité pour les produits et services TIC dans les marchés publics**, y compris la certification de cybersécurité**;

c) une politique **relative à la gestion des vulnérabilités comprenant la promotion et la facilitation de** [...] la divulgation coordonnée des vulnérabilités au sens de l'article 6**, paragraphe 1, sur une base volontaire**;

d) une politique liée au maintien de la disponibilité générale**,** [...] de l'intégrité **et de la confidentialité** du noyau public de l'internet ouvert;

e) une politique de promotion et de développement **de l'éducation et de la formation ainsi que** des compétences en matière de cybersécurité, de sensibilisation et d'initiatives de recherche et développement;

38 [*insérer le titre complet et la référence de la publication au JO lorsqu'elle est connue*]

f) une politique de soutien aux institutions universitaires et de recherche visant à développer des outils de cybersécurité et à sécuriser les infrastructures de réseau;

g) une politique, des procédures pertinentes et des outils de partage d'informations appropriés visant à soutenir le partage volontaire d'informations sur la cybersécurité entre les entreprises dans le respect du droit de l'Union;

h) une politique répondant aux besoins spécifiques des PME, en particulier de celles qui sont exclues du champ d'application de la présente directive, en matière d'orientation et de soutien visant à améliorer leur résilience aux **cyber**menaces[...].

3. Les États membres notifient leurs stratégies nationales en matière de cybersécurité à la Commission dans les trois mois suivant leur adoption. **Dans ce cadre,** les États membres peuvent exclure **des éléments de la stratégie se rapportant à** [...] la sécurité nationale.

4. Les États membres évaluent leurs stratégies nationales de cybersécurité au moins tous les [...] **cinq** ans sur la base d'indicateurs clés de performance et, le cas échéant, les modifient. L'Agence de l'Union européenne pour la cybersécurité (ENISA) aide les États membres, sur **leur** demande, à élaborer une stratégie nationale et des indicateurs clés de performance aux fins de l'évaluation de la stratégie.

Article 6

Divulgation coordonnée des vulnérabilités et registre européen des vulnérabilités

1. Chaque État membre désigne l'un de ses CSIRT visés à l'article 9 comme coordinateur aux fins de la divulgation coordonnée des vulnérabilités. Le CSIRT désigné doit agir comme intermédiaire de confiance, en facilitant, si nécessaire, les interactions entre l'entité effectuant le signalement**, le détenteur potentiel d'une vulnérabilité** et le fabricant ou le fournisseur de produits ou de services TIC. **Toute personne physique ou morale peut signaler au CSIRT désigné, éventuellement de manière anonyme, une vulnérabilité visée à l'article 4, paragraphe 8. Le CSIRT désigné veille à ce que le signalement soit suivi avec diligence et à ce que la confidentialité de l'identité de la personne qui signale la vulnérabilité soit assurée.** Lorsque la vulnérabilité signalée [...] **est potentiellement susceptible d'avoir un impact significatif sur des entités dans plusieurs États membres,** le CSIRT désigné de chaque État membre concerné coopère**, en tant que de besoin, avec d'autres CSIRT désignés au sein du** [...] réseau CSIRT.

2. L'ENISA élabore et tient à jour un registre européen des vulnérabilités**, en consultation avec le groupe de coopération.** À cette fin, l'ENISA établit et maintient les systèmes d'information, les politiques et les procédures appropriés en vue notamment de permettre aux entités importantes et essentielles et à leurs fournisseurs de réseaux et de systèmes d'information de divulguer et d'enregistrer**, sur une base volontaire,** les vulnérabilités **publiquement connues** présentes dans les produits TIC ou les services TIC, ainsi que de donner accès à toutes les parties intéressées aux informations sur les vulnérabilités contenues dans le registre. Le registre comprend notamment des informations décrivant la vulnérabilité, le produit TIC ou les services TIC affectés ainsi que la gravité de la vulnérabilité en termes de circonstances dans lesquelles elle peut être exploitée, la disponibilité des correctifs correspondants et, en l'absence de correctifs disponibles, des orientations **émises par les autorités nationales compétentes ou les CSIRT** adressées aux utilisateurs de produits et services vulnérables sur la manière dont les risques résultant des vulnérabilités divulguées peuvent être atténués. **L'ENISA veille à ce que le registre européen des vulnérabilités utilise des infrastructures de communication et d'information sûres et résilientes.**

Article 7

Cadres nationaux de gestion de crise dans le domaine de la cybersécurité

1. Chaque État membre désigne une ou plusieurs autorités compétentes qui sont chargées de la gestion des crises et incidents majeurs **de cybersécurité.** Les États membres veillent à ce que les autorités compétentes disposent de ressources suffisantes pour s'acquitter, de manière effective et efficace, des tâches qui leur sont dévolues. **Les États membres veillent à la cohérence avec les cadres existants pour la gestion générale des crises.**

2. Chaque État membre recense les capacités, les moyens et les procédures qui peuvent être déployés en cas de crise aux fins de la présente directive.

3. Chaque État membre adopte un plan national de réaction aux incidents et aux crises de cybersécurité dans lequel sont définis les objectifs et les modalités de gestion des incidents et crises de cybersécurité majeurs. Le plan doit, notamment, prévoir les éléments suivants:

   a) les objectifs des mesures et activités nationales de préparation;

   b) les tâches et responsabilités des autorités compétentes nationales;

   c) les procédures de gestion de crise**, y compris leur intégration dans le cadre national général de gestion des crises** et les canaux d'échange d'informations;

   d) les mesures de préparation, y compris des exercices réguliers et des activités de formation;

   e) les parties [...] publiques et privées et les infrastructures concernées;

   f) les procédures et arrangements nationaux entre les autorités et les organismes nationaux compétents visant à garantir la participation et le soutien effectifs de l'État membre à la gestion coordonnée des incidents et crises de cybersécurité majeurs au niveau de l'Union.

4. Les États membres [...] **informent l**a Commission **de** la désignation de leurs autorités compétentes visées au paragraphe 1 et soumettent **des informations pertinentes relatives aux exigences du paragraphe 3 du présent article quant à** leurs plans nationaux d'intervention en cas d'incident et de crise de cybersécurité [...] dans les trois mois suivant cette désignation et l'adoption de ces plans. Les États membres peuvent exclure certaines informations [...] lorsque et dans la mesure où cela est [...] nécessaire pour préserver leur sécurité nationale**, leur sécurité publique ou leur défense**.

Article 8

Autorités nationales compétentes et points de contact uniques

1. Chaque État membre désigne une ou plusieurs autorités compétentes chargées de la cybersécurité et des tâches de contrôle visées au chapitre VI de la présente directive. Les États membres peuvent désigner à cet effet une ou des autorités existantes.

2. Les autorités compétentes visées au paragraphe 1 contrôlent l'application de la présente directive au niveau national.

3. Chaque État membre désigne un point de contact national unique en matière de sécurité (ci-après dénommé "point de contact unique"). Lorsqu'un État membre désigne une seule autorité compétente, cette dernière fait aussi fonction de point de contact unique dudit État membre.

4. Chaque point de contact unique exerce une fonction de liaison visant à assurer la coopération transfrontalière des autorités de son État membre avec les autorités compétentes des autres États membres, ainsi que pour garantir la coopération intersectorielle avec les autres autorités nationales compétentes de son État membre.

5. Les États membres veillent à ce que les autorités compétentes visées au paragraphe 1 et les points de contact uniques disposent de ressources suffisantes pour pouvoir s'acquitter de leurs tâches de manière effective et efficace et atteindre ainsi les objectifs de la présente directive. Les États membres font en sorte que les représentants désignés pour siéger au sein du groupe de coopération visé à l'article 12 puissent coopérer de manière effective, efficace et sécurisée.

6. Chaque État membre notifie dans les meilleurs délais à la Commission la désignation de l'autorité compétente visée au paragraphe 1 et du point de contact unique visé au paragraphe 3, les tâches qui leur sont confiées et toute modification ultérieure dans ce cadre. Chaque État membre rend leur désignation publique. La Commission publie la liste des points de contact uniques désignés.

Article 9

Centres de réponse aux incidents de sécurité informatique (CSIRT)

1. Chaque État membre désigne un ou plusieurs CSIRT, se conformant aux exigences énumérées à l'article 10, paragraphe 1, couvrant au moins les secteurs, les sous-secteurs ou les entités visés aux annexes I et II, et chargés de la gestion des incidents selon un processus bien défini. Un CSIRT peut être établi au sein d'une autorité compétente visée à l'article 8.

2. Les États membres veillent à ce que chaque CSIRT dispose de ressources suffisantes pour pouvoir s'acquitter efficacement de ses tâches énumérées à l'article 10, paragraphe 2. **Dans l'exécution de ces tâches, les CSIRT peuvent donner la priorité à la fourniture de services particuliers à des entités sur la base d'une approche fondée sur les risques.**

3. Les États membres veillent à ce que chaque CSIRT dispose d'une infrastructure de communication et d'information adaptée, sécurisée et résiliente pour échanger des informations avec les entités essentielles et importantes et les autres parties intéressées concernées. À cette fin, les États membres veillent à ce que les CSIRT contribuent au déploiement d'outils sécurisés de partage d'informations.

4. Les CSIRT coopèrent et, le cas échéant, échangent des informations pertinentes conformément à l'article 26 avec des communautés sectorielles ou intersectorielles de confiance d'entités essentielles et importantes.

5. Les CSIRT participent aux **apprentissages** [...] par les pairs organisés conformément à l'article 16.

6. Les États membres veillent à ce que leurs CSIRT coopèrent de manière effective, efficace et sécurisée au sein du réseau des CSIRT visé à l'article 13.

7. Les États membres communiquent dans les meilleurs délais à la Commission les CSIRT désignés conformément au paragraphe 1, le coordinateur des CSIRT désigné conformément à l'article 6, paragraphe 1, et leurs tâches respectives prévues en ce qui concerne les entités visées aux annexes I et II.

8. Les États membres peuvent solliciter l'assistance de l'ENISA pour la mise en place des CSIRT nationaux.

Article 10

Obligations et tâches des CSIRT

1. Les CSIRT satisfont aux exigences suivantes:

   a) les CSIRT doivent veiller à un niveau élevé de disponibilité de leurs [...] **canaux** de communication en évitant les points uniques de défaillance et ils doivent disposer de plusieurs moyens pour être contactés et contacter autrui à tout moment. Les CSIRT doivent clairement spécifier les canaux de communication et les faire connaître aux partenaires et collaborateurs;

   b) les locaux des CSIRT et les systèmes d'information utilisés doivent se trouver sur des sites sécurisés;

c) les CSIRT sont dotés d'un système approprié de gestion et de routage des demandes afin, notamment, de faciliter les transferts effectifs et efficaces;

d) les CSIRT sont dotés des effectifs adéquats afin de pouvoir garantir une disponibilité permanente;

e) les CSIRT doivent être dotés de systèmes redondants et d'un espace de travail de secours pour assurer la continuité de leurs services;

f) les CSIRT ont la possibilité de participer aux réseaux de coopération internationale.

2. Les CSIRT assument les tâches suivantes:

a) la surveillance des cybermenaces, des vulnérabilités et des incidents au niveau national;

b) l'activation du mécanisme d'alerte précoce, la diffusion de messages d'alerte, les annonces et la diffusion d'informations sur les cybermenaces, les vulnérabilités et les incidents auprès des entités essentielles et importantes ainsi qu'auprès **des autorités compétentes et** des autres parties intéressées;

c) la réaction aux incidents;

d) la collecte et l'analyse des données de police scientifique, et l'analyse dynamique des risques et incidents et la conscience situationnelle en matière de cybersécurité;

e) la réalisation [...] d'un scannage proactif du réseau et des systèmes d'information [...] **pour détecter les vulnérabilités susceptibles d'avoir un impact significatif à condition que, en l'absence de consentement de l'entité en question, le réseau et les systèmes d'information n'aient pas subi d'intrusion ou que leur fonctionnement n'ait pas été négativement impacté;**

f) la participation au réseau des CSIRT ainsi que la fourniture d'une assistance mutuelle **en fonction de leurs capacités et de leurs compétences** aux autres membres du réseau à leur demande;

f *bis*) le cas échéant, ils agissent en tant que coordinateur aux fins du processus de divulgation coordonnée des vulnérabilités conformément à l'article 6, paragraphe 1, qui comprend notamment la facilitation de l'interaction entre les entités effectuant le signalement, le détenteur potentiel d'une vulnérabilité et le fabricant ou le fournisseur de produits TIC ou de services TIC lorsque cela est nécessaire, l'identification des entités concernées et le contact avec elles, le soutien aux entités effectuant le signalement, la négociation des délais de divulgation et la gestion des vulnérabilités qui touchent plusieurs organisations (divulgation multipartite coordonnée de vulnérabilité).

3. Les CSIRT établissent des relations de coopération avec les acteurs concernés du secteur privé, en vue de mieux atteindre les objectifs de la directive.

3 *bis*. Les CSIRT peuvent établir des relations de coopération avec les CSIRT nationaux de pays tiers. Dans le cadre de cette coopération, ils peuvent échanger des informations pertinentes, y compris des données à caractère personnel, dans le respect du droit de l'Union en matière de protection des données.

4. Afin de faciliter la coopération, les CSIRT encouragent l'adoption et l'utilisation de pratiques, de systèmes de classification et de taxonomies communs ou normalisés en ce qui concerne

a) les procédures de gestion des incidents;

b) la gestion des crises de cybersécurité;

c) la divulgation coordonnée des vulnérabilités.

Article 11

Coopération au niveau national

1. Lorsqu'ils sont distincts, les autorités compétentes visées à l'article 8, le point de contact unique et le(s) CSIRT d'un même État membre coopèrent les uns avec les autres aux fins du respect des obligations énoncées dans la présente directive.

2. Les États membres veillent à ce que leurs autorités compétentes ou leurs CSIRT reçoivent des signalements relatifs aux incidents, aux cybermenaces importantes et quasi-accidents, soumis en application de la présente directive. Lorsqu'un État membre décide que ses CSIRT ne reçoivent pas ces signalements, ils se voient accorder, dans la mesure nécessaire à l'accomplissement de leurs tâches, un accès aux données relatives aux incidents signalés par les entités essentielles ou importantes conformément à l'article 20.

3. Chaque État membre veille à ce que ses autorités compétentes ou CSIRT informent son point de contact unique des signalements d'incidents, de cybermenaces importantes et de quasi-accidents soumis en application de la présente directive.

4. Dans la mesure nécessaire pour s'acquitter efficacement des tâches et obligations prévues par la présente directive, les États membres assurent une coopération appropriée entre les autorités compétentes**, les CSIRT,** les points de contact uniques et les services répressifs, les autorités chargées de la protection des données et les autorités **compétentes désignées** [...] en vertu de la directive (UE) XXXX/XXXX [directive sur la résilience des entités critiques]**, les autorités compétentes au titre du règlement d'exécution 2019/1583 de la Commission, les autorités de régulation nationales désignées conformément à la directive (UE) 2018/1972, les autorités nationales désignées en vertu de l'article 17 du règlement (UE) n° 910/2014,** [...] les autorités financières nationales désignées conformément au règlement (UE) XXXX/XXXX du Parlement européen et du Conseil [le règlement sur la résilience opérationnelle numérique du secteur financier]**, ainsi que les autorités compétentes désignées par d'autres actes juridiques sectoriels de l'Union,** dans cet État membre.

5. Les États membres veillent à ce que leurs autorités compétentes **au titre de la présente directive et les autorités compétentes désignées en vertu de la directive (UE) XXXX/XXXX [directive sur la résilience des entités critiques échangent** [...] régulièrement des informations **sur l'identification des entités critiques, ainsi que des** [...] risques [...], **des** [...]menaces et [...]**des** incidents **en matière cyber et non cyber** affectant les entités essentielles identifiées comme critiques, **[**ou comme entités équivalentes aux entités critiques,**]** en vertu de la directive (UE) XXXX/XXXX [directive sur la résilience des entités critiques], ainsi [...] **que sur les** mesures prises [...] en réponse à ces risques et incidents. **Les États membres veillent également à ce que les autorités compétentes au titre de la présente directive [...] et les autorités compétentes désignées au titre du règlement XXXX/XXXX [règlement sur la résilience opérationnelle numérique du secteur financier], de la directive 2018/1972 et du règlement (UE) 910/2014 échangent régulièrement des informations pertinentes.**

En ce qui concerne les prestataires de services de confiance et [...]en particulier[...] lorsque ce rôle de surveillance au titre de la présente directive est confié à un autre organe que les organes de contrôle désignés en vertu du règlement (UE) n° 910/2014, les autorités nationales compétentes au titre de la présente directive coopèrent étroitement, en temps utile, en échangeant les informations pertinentes afin de garantir une surveillance efficace et le respect, par les prestataires de services de confiance, des exigences énoncées dans la présente directive et dans le règlement [XXXX/XXXX] **et, le cas échéant, l'autorité nationale compétente en vertu de la présente directive informe, dans les meilleurs délais, l'organe de contrôle établi en vertu du règlement eIDAS de toute menace ou incident majeur signalé dans le domaine du cyber ayant une incidence sur les services de confiance**

5 *bis*. Afin de simplifier le signalement des incidents, les États membres peuvent mettre en place un point d'entrée unique pour tous les signalements requis en vertu de la présente directive, ainsi que du règlement (UE) 2016/679 et de la directive 2002/58/CE, selon le cas. Les États membres peuvent utiliser le point d'entrée unique pour les signalements requis en vertu d'autres actes juridiques sectoriels de l'Union. Ce point d'entrée unique n'affecte pas l'application des dispositions du règlement (UE) 2016/679 et de la directive 2002/58/CE, en particulier celles relatives aux autorités de contrôle indépendantes.

CHAPITRE III

*Coopération **de l'UE***

Article 12

Groupe de coopération

1. Afin de soutenir et de faciliter la coopération stratégique et l'échange d'informations entre les États membres **et de** [...] **renforcer la confiance**, un groupe de coopération est créé.

2. Le groupe de coopération exécute ses tâches en s'appuyant sur les programmes de travail bisannuels visés au paragraphe 6.

3. Le groupe de coopération est composé de représentants des États membres, de la Commission et de l'ENISA. Le service européen pour l'action extérieure participe aux activités du groupe de coopération en qualité d'observateur. Les autorités européennes de surveillance (AES) **et les autorités compétentes désignées en vertu du règlement (UE) XXXX/XXXX [règlement sur la résilience opérationnelle numérique du secteur financier]** [...] peuvent participer aux activités du groupe de coopération**, conformément à l'article 42, paragraphe 1 du règlement (UE) XXXX/XXXX [règlement sur la résilience opérationnelle numérique du secteur financier].**

   Si besoin est, le groupe de coopération peut inviter des représentants des acteurs concernés à participer à ses travaux.

   Le secrétariat est assuré par la Commission.

4. Le groupe de coopération est chargé des tâches suivantes:

   a) la fourniture d'orientations aux autorités compétentes en rapport avec la transposition et la mise en œuvre de la présente directive;

   a *bis*) la fourniture d'orientations en ce qui concerne l'élaboration et la mise en œuvre des politiques de divulgation coordonnée des vulnérabilités, visées à l'article 5, paragraphe 2, point c), et à l'article 6, paragraphe 1;

b) l'échange des meilleures pratiques et d'informations relatives à la mise en œuvre de la présente directive, notamment en ce qui concerne les cybermenaces, les incidents, les vulnérabilités, les quasi-accidents, les initiatives de sensibilisation, les formations, les exercices et les compétences, le renforcement des capacités ainsi que les normes et les spécifications techniques;

c) l'échange de conseils et la coopération avec la Commission sur les initiatives politiques émergentes en matière de cybersécurité;

d) l'échange de conseils et la coopération avec la Commission sur les projets d'actes d'exécution [...] de la Commission adoptés en vertu de la présente directive;

e) l'échange de bonnes pratiques et d'informations avec les institutions, organes et organismes compétents de l'Union;

e *bis*) l'échange de vues sur la mise en œuvre de la législation sectorielle comportant des aspects liés à la cybersécurité;

f) la discussion portant sur les rapports relatifs [...] **aux apprentissages** par les pairs visés à l'article 16, paragraphe 7;

g) la discussion portant sur les [...] **expériences** des activités de contrôle conjoint dans les affaires transfrontières visées à l'article 34;

h) l'indication d'une orientation stratégique au réseau des CSIRT **et au réseau UE-CyCLONe** sur des questions nouvelles spécifiques;

h *bis*)l'échange de vues sur le suivi des mesures relatives aux incidents et crises majeurs de cybersécurité, sur la base des enseignements tirés du réseau des CSIRT et du réseau UE-CyCLONe;

i) la contribution aux capacités en matière de cybersécurité dans l'ensemble de l'Union via la facilitation de l'échange de fonctionnaires nationaux grâce à un programme de renforcement des capacités impliquant le personnel des autorités compétentes des États membres ou des CSIRT;

j) l'organisation régulière de réunions conjointes avec les parties privées intéressées de toute l'Union en vue de discuter des activités menées par le groupe et de recueillir des informations sur les nouveaux défis politiques;

k) la discussion portant sur les travaux entrepris en relation avec les exercices de cybersécurité, y compris les travaux effectués par l'ENISA;

k *bis*)l'établissement du mécanisme d'apprentissage par les pairs conformément à l'article 16 de la présente directive.

5. Le groupe de coopération peut demander au réseau **des** CSIRT d'élaborer un rapport technique sur des sujets choisis.

6. Au plus tard le ... [24 mois après la date d'entrée en vigueur de la présente directive] et ensuite tous les deux ans, le groupe de coopération établit un programme de travail concernant les actions à entreprendre pour mettre en œuvre ses objectifs et ses tâches. Le calendrier du premier programme adopté au titre de la présente directive est aligné sur le calendrier du dernier programme adopté au titre de la directive (UE) 2016/1148.

7. La Commission peut adopter des actes d'exécution fixant les modalités de procédure nécessaires au fonctionnement du groupe de coopération. Ces actes d'exécution sont adoptés en conformité avec la procédure d'examen visée à l'article 37, paragraphe 2.

8. Le groupe de coopération se réunit régulièrement et au moins une fois par an avec le groupe sur la résilience des entités critiques instauré en vertu de la directive (UE) XXXX/XXXX [directive sur la résilience des entités critiques] afin de promouvoir la coopération stratégique et **de faciliter** l'échange d'informations.

Article 13

Réseau des CSIRT

1. Afin de contribuer au renforcement de la confiance et de promouvoir une coopération opérationnelle rapide et effective entre les États membres, un réseau des CSIRT nationaux est établi.

2. Le réseau des CSIRT est composé de représentants des CSIRT des États membres **désignés conformément à l'article 9,** et du CERT-UE. La Commission participe au réseau des CSIRT en qualité d'observateur. L'ENISA assure le secrétariat et soutient activement la coopération entre les CSIRT.

3. Le réseau des CSIRT est chargé des tâches suivantes:

   a) l'échange d'informations sur les capacités des CSIRT;

   b) l'échange d'informations pertinentes sur les incidents, les quasi-accidents, les cybermenaces, les risques et les vulnérabilités;

b *bis*) l'échange d'informations en ce qui concerne les publications et les recommandations en matière de cybersécurité;

b *ter*) le partage de solutions techniques facilitant la gestion technique des incidents;

b *quater*) l'échange de bonnes pratiques, d'outils et de processus en ce qui concerne les missions des CSIRT;

c) à la demande d'un [...] **membre** du réseau **des** CSIRT potentiellement affecté par un incident, l'échange et la discussion portant sur les informations en rapport avec cet incident et les cybermenaces, risques et vulnérabilités connexes;

d) à la demande d'un [...] **membre** du réseau **des** CSIRT [...], la discussion et, si possible, la mise en œuvre d'une réponse coordonnée à un incident déterminé qui relève de la juridiction de cet État membre;

e) la fourniture aux États membres d'une assistance face aux incidents transfrontaliers en application de la présente directive;

f) la coopération**, l'échange de bonnes pratiques** et la fourniture d'une assistance aux CSIRT désignés visés à l'article 6 en ce qui concerne la gestion de la divulgation coordonnée [...] des vulnérabilités affectant plusieurs fabricants ou fournisseurs de produits TIC, de services TIC et processus TIC établis dans différents États membres;

g) la discussion et l'identification d'autres formes de coopération opérationnelle, notamment en rapport avec:

i) les catégories de cybermenaces et d'incidents;

ii) les alertes précoces;

iii) l'assistance mutuelle;

iv) les principes et modalités d'une coordination en réponse à des risques et incidents transfrontaliers;

v) la contribution au plan national de réaction aux incidents et aux crises de cybersécurité visé à l'article 7, paragraphe 3**, à la demande d'un État membre**;

h) l'information du groupe de coopération de ses activités et des autres formes de coopération opérationnelle débattues en application du point g), et lorsque cela s'avère nécessaire, la demande de fourniture d'orientations à cet égard;

i) l'examen des exercices de cybersécurité, y compris ceux organisés par l'ENISA;

j) à la demande d'un CSIRT donné, l'étude des capacités et de l'état de préparation dudit CSIRT;

k) la coopération et l'échange d'informations avec les centres d'opérations de sécurité (COS) régionaux et au niveau de l'Union afin d'améliorer la connaissance commune de la situation concernant les incidents et les menaces dans toute l'Union;

l) l'examen des rapports **relatifs aux apprentissages [**...] par les pairs visés à l'article 16, paragraphe 7;

m) la publication de lignes directrices afin de faciliter la convergence des pratiques opérationnelles en ce qui concerne l'application des dispositions du présent article relatives à la coopération opérationnelle.

4. Aux fins du réexamen visé à l'article 35 et d'ici le [24 mois après la date d'entrée en vigueur de la présente directive], puis tous les deux ans, le réseau des CSIRT évalue les progrès réalisés dans le cadre de la coopération opérationnelle et produit un rapport. Le rapport tire notamment des conclusions sur les résultats des [...] **apprentissages** par les pairs visés à l'article 16, effectuées en rapport avec les CSIRT nationaux, y compris des conclusions et des recommandations, conformément au présent article. Ce rapport est aussi transmis au groupe de coopération.

5. Le réseau des CSIRT adopte son propre règlement intérieur.

6. Le réseau des CSIRT coopère avec le réseau UE-CyCLONe sur la base des modalités procédurales convenues.

Article 14

Le réseau européen Cyber Crisis Liaison Organisation Network (UE-CyCLONe)

1. Afin de contribuer à la gestion coordonnée, au niveau opérationnel, des incidents et crises de cybersécurité majeurs, et de garantir l'échange régulier d'informations entre les États membres et les institutions, organes et agences de l'Union, le réseau européen pour la préparation et la gestion des crises cyber par les États membres (UE-CyCLONe – Cyber Crisis Liaison Organisation Network) est institué.

2. Le réseau UE-CyCLONe est composé des représentants [...] des autorités des États membres chargées de la gestion des **cyber**crises désignées conformément à l'article 7. **La Commission participe aux activités du réseau en qualité d'observateur.** L'ENISA assure le secrétariat du réseau et soutient l'échange sécurisé d'informations**, et fournit également les outils nécessaires pour soutenir la coopération entre États membres en garantissant un échange sécurisé d'informations.**

Si besoin est, le réseau UE-CyCLONe peut inviter des représentants des acteurs concernés à participer à ses travaux.

3. Le réseau UE-CyCLONe a pour mission:

a) de renforcer le niveau de préparation à la gestion des crises et incidents majeurs **en matière de cybersécurité**;

b) de développer une connaissance situationnelle partagée [...] **pour les incidents et crises de grande ampleur** en matière de cybersécurité;

b *bis*) d'évaluer les conséquences et l'impact des incidents de grande ampleur en matière de cybersécurité et de proposer d'éventuelles mesures d'atténuation;

c) de coordonner la gestion des crises et incidents de grande ampleur **en matière de cybersécurité** et de soutenir la prise de décision au niveau politique en ce qui concerne ces incidents et ces crises;

d) **à la demande d'un État membre,** d'examiner [...]**ses plans nationaux d'intervention en cas d'incident et de crise de cybersécurité** visés à l'article 7, paragraphe **3**[...];[…]

4. UE-CyCLONe adopte son règlement intérieur.

5. UE-CyCLONe rend régulièrement compte au groupe de coopération **de la gestion des incidents de cybersécurité majeurs et de la gestion de crise** [...], en mettant notamment l'accent sur leur incidence sur les entités essentielles et importantes.

6. UE-CyCLONe coopère avec le réseau des CSIRT sur la base des modalités procédurales convenues.

7. UE-CyCLONe soumet au Parlement européen et au Conseil un rapport évaluant ses travaux au plus tard le [24 mois après la date d'entrée en vigueur de la présente directive].

Article 14 bis

Coopération internationale

L'Union peut, conformément à l'article 218 du traité sur le fonctionnement de l'Union européenne et lorsque cela est pertinent, conclure, avec des pays tiers ou des organisations internationales, des accords internationaux qui permettent et organisent leur participation à certaines activités du groupe de coopération, du réseau des CSIRT et UE-CyCLONe, dans le respect de la législation de l'UE en matière de protection des données

Article 15

Rapport sur l'état de la cybersécurité dans l'Union

1. L'ENISA publie, en coopération avec la Commission **et le groupe de coopération**, un rapport bisannuel sur l'état de la cybersécurité dans l'Union. **En particulier, l**[...]e rapport comporte [...] [...]**l**es éléments suivants:

a *bis*) une évaluation des risques en matière de cybersécurité à l'échelle de l'Union, tenant compte du paysage des menaces;

a) [...] **une évaluation du** développement des capacités de cybersécurité dans les secteurs public et privé dans l'ensemble de l'Union;

b) […]

c) **une évaluation globale sur la base d'indicateurs quantitatifs et qualitatifs en matière** [...] de cybersécurité permettant [...] **une vue d'ensemble** du niveau de maturité des capacités de cybersécurité**, capacités sectorielles comprises.**

2. Le rapport comprend des recommandations politiques spécifiques visant à accroître le niveau de cybersécurité dans l'Union ainsi qu'un résumé des conclusions pour la période concernée des rapports de situation technique de l'Agence de l'UE sur la cybersécurité, publiés par l'ENISA conformément à l'article 7, paragraphe 6, du règlement (UE) 2019/881.

Article 16

Apprentissages par les pairs

1. **En vue de renforcer la confiance mutuelle, d'atteindre un niveau commun de cybersécurité élevé, ainsi que de renforcer les capacités et les politiques de cybersécurité des États membres nécessaire à la mise en œuvre effective de la présente directive, le groupe de coopération** [...] établit, **avec le soutien de la Commission et** après consultation de l'ENISA **ainsi que, le cas échéant, du réseau des CSIRT**, et au plus tard **24** [...] mois après l'entrée en vigueur de la présente directive, la méthodologie [...] **en vue** d'un système d'[...]**apprentissage** par les pairs [...] **objectif, non-discriminatoire et juste en ce qui concerne la mise en œuvre de la présente directive par les** États membres. **La participation à l'apprentissage par les pairs est facultative. Le système consiste en des exercices d'évaluation** [...] effectué[...]s par des experts [...] en cybersécurité provenant d'États membres [...] et porte [...] sur **un ou plusieurs des** [...] points suivants:

   i) [...] la mise en œuvre des exigences en matière de gestion des risques liés à la cybersécurité et des obligations de signalement visées aux articles 18 et 20;

   ii) [...] **les** capacités, y compris les ressources [...] disponibles, et [...] l'exercice des tâches des autorités nationales compétentes **visées à l'article 8 et de celles des CSIRT visées à l'article 9**;

[…]

i**ii**[...]) [...] **la mise en œuvre** de l'assistance mutuelle visée à l'article 34;

iv) [...] **la mise en œuvre** du cadre de partage des informations, visé à l'article 26 [...].

2. **Les critères sur la base desquels les États membres doivent désigner des experts susceptibles de participer aux exercices d'apprentissage par les pairs sont** [...] objectifs, non discriminatoires, équitables et transparents [...] **et sont inclus dans la méthodologie visée au paragraphe 1**. L'ENISA et la Commission [...] **peuvent désigner** des experts pour participer en tant qu'observateurs aux [...] **exercices d'apprentissage** par les pairs. […]

3. [...] .

3 *bis*. Avant le début des exercices d'apprentissage par les pairs, les États membres peuvent procéder à une autoévaluation des aspects couverts par l'exercice en question d'apprentissage par les pairs et soumettre cette autoévaluation aux experts désignés visés au paragraphe 2.

4. Les [...] **apprentissages** par les pairs [...] **peuvent comporter** des visites sur place physiques ou virtuelles et des échanges hors site. Compte tenu du principe de bonne coopération, les États membres [...] **prenant part à l'apprentissage par les pairs** fournissent aux experts désignés les informations demandées qui sont nécessaires à l'évaluation [...]**, sans préjudice des dispositions juridiques nationales ou de l'Union concernant la protection des informations confidentielles ou classifiées ou de la sauvegarde de fonctions essentielles de l'État, telles que la sécurité nationale.** Toute information obtenue durant le processus d'[...]**apprentissage** par les pairs n'est utilisée qu'à cet effet. Les experts participant à l'[...]**apprentissage** par les pairs ne divulguent à aucun tiers les informations sensibles ou confidentielles obtenues [...] **dans ce contexte**. **L'État membre participant à l'apprentissage par les pairs peut s'opposer à la désignation de certains experts pour des raisons dûment justifiées communiquées au groupe de coopération.**

5. Une fois **soumis à un exercice d'apprentissage par les pairs** [...], les mêmes aspects ne font pas l'objet [...] **de nouveaux exercices d'apprentissage** par les pairs **pour les États membres participants** [...] au cours des [...] **quatre** années suivant la conclusion [...] **dudit exercice d'apprentissage** par les pairs, sauf [...] **si l'État membre concerné le demande ou l'accepte à la suite d'une proposition** du groupe de coopération.

6. […]

7. Les experts participant aux [...] **exercices d'apprentissage** par les pairs rédigent des rapports sur les résultats et les conclusions des évaluations. **Les États membres sont autorisés à formuler des observations sur leurs projets de rapport respectifs, qui sont joints au rapport.** Les rapports **finaux** sont transmis au groupe de coopération[...]. **Les États membres peuvent décider de rendre leurs rapports respectifs accessibles au public.**

CHAPITRE IV

Obligations concernant la gestion des risques et le signalement en matière de cybersécurité

SECTION I

Gestion des risques et signalement en matière de cybersécurité

Article 17

Gouvernance

1. Les États membres veillent à ce que les organes de direction des entités essentielles et importantes approuvent les mesures de gestion des risques en matière de cybersécurité prises par ces entités afin de se conformer à l'article 18, supervisent sa mise en œuvre et […] **puissent être** tenus responsables du non-respect par ces entités des obligations découlant du présent article.

   L'application du présent paragraphe est sans préjudice des législations nationales des États membres en ce qui concerne les règles en matière de responsabilité dans les institutions publiques, ainsi que de responsabilité des agents de la fonction publique et des fonctionnaires élus et nommés.

2. Les États membres veillent à ce que les membres de l'organe de direction […] **soient tenus de suivre** régulièrement des formations […] afin d'acquérir des connaissances et des compétences suffisantes pour appréhender et évaluer les risques et les pratiques de gestion en matière de cybersécurité et leur incidence sur les activités de l'entité.

Article 18

Mesures de gestion des risques en matière de cybersécurité

1 ***bis***. **La présente directive applique une approche "tous risques" qui inclut la protection des réseaux et des systèmes d'information et de leur environnement physique contre tout événement susceptible de compromettre la disponibilité, l'authenticité, l'intégrité ou la confidentialité des données stockées, transmises ou faisant l'objet d'un traitement ou des services que ces réseaux et systèmes d'information offrent ou rendent accessibles.**

1. Les États membres veillent à ce que les entités essentielles et importantes prennent les mesures techniques et organisationnelles appropriées et proportionnées pour gérer les risques qui menacent la sécurité des réseaux […] et des systèmes d'information que ces entités utilisent dans le cadre de la fourniture de leurs services. Ces mesures garantissent, pour les réseaux et les systèmes d'information, un niveau de sécurité adapté au risque existant, compte tenu de l'état des connaissances **et des coûts de mise en œuvre**. **Lors de l'évaluation de la proportionnalité de ces mesures, il est dûment tenu compte du degré d'exposition de l'entité aux risques, de sa taille, de la probabilité d'occurrence d'incidents et de leur gravité. Compte tenu du niveau et du type de risque pour la société en cas d'incidents touchant des entités essentielles ou importantes, les mesures de gestion des risques en matière de cybersécurité imposées aux entités importantes peuvent être moins strictes que celles imposées aux entités essentielles.**

2. Les mesures visées au paragraphe 1 comprennent au minimum:

a) l'analyse des risques et les politiques de sécurité des systèmes d'information;

b) la gestion des incidents (prévention et détection des incidents, […] réaction aux incidents **et rétablissement après un incident**);

c) la continuité des activités et la gestion des crises;

d) la sécurité de la chaîne d'approvisionnement, y compris les aspects liés à la sécurité concernant les relations entre chaque entité et ses fournisseurs ou prestataires de services **directs** tels que les fournisseurs de services de stockage et de traitement des données ou de services de sécurité gérés;

e) la sécurité de l'acquisition, du développement et de la maintenance des réseaux et des systèmes d'information, y compris le traitement et la divulgation des vulnérabilités;

f) des politiques et des procédures […] pour évaluer l'efficacité des mesures de gestion des risques en matière de cybersécurité;

g) […] **une politique en matière d**'utilisation de la cryptographie et du cryptage**;**

g *bis*) la sécurité des ressources humaines, des politiques de contrôle d'accès et la gestion des actifs.

3. Les États membres veillent à ce que, lorsqu'elles envisagent de prendre les mesures appropriées visées au paragraphe 2, point d), les entités […] **soient tenues de prendre en** compte **l**es vulnérabilités propres à chaque fournisseur et prestataire de services **direct** et […] la qualité globale des produits et des pratiques de cybersécurité de leurs fournisseurs et prestataires de services, y compris de leurs procédures de développement sécurisé. **Les États membres veillent également à ce que, lorsqu'elles envisagent de prendre les mesures appropriées visées au paragraphe 2, point d), les entités soient tenues de prendre en compte les résultats des évaluations coordonnées des risques effectuées conformément à l'article 19, paragraphe 1.**

4. Les États membres veillent à ce que, lorsqu'une entité constate que ses services ou tâches respectifs ne sont pas conformes aux exigences énoncées au paragraphe 2, elle prenne dans les meilleurs délais toutes les mesures correctives nécessaires pour mettre le service concerné en conformité.

5. La Commission peut adopter des actes d'exécution afin d'établir les spécifications techniques et méthodologiques**, ainsi que les spécificités sectorielles, au besoin,** des éléments visés au paragraphe 2 **du présent article**. **Au plus tard le [18 mois après l'entrée en vigueur de la présente directive], la Commission adopte des actes d'exécution afin d'établir les spécifications techniques et méthodologiques pour les entités visées à l'article 24, paragraphe 1, et les prestataires de services de confiance visés à l'annexe I, point 8. Ces actes d'exécution sont adoptés en conformité avec la procédure d'examen visée à l'article 37, paragraphe 2.** Lorsqu'elle prépare ces actes **d'exécution**, la Commission […] **suit**, dans toute la mesure du possible, les normes internationales et européennes, ainsi que les spécifications techniques pertinentes **et échange des conseils avec le groupe de coopération et l'ENISA sur les projets d'actes d'exécution conformément à l'article 12, paragraphe 4, point d).**

6. […]

Article 19

Évaluations coordonnées au niveau de l'UE des risques liés aux chaînes d'approvisionnement critiques

1. Le groupe de coopération, en coopération avec la Commission et l'ENISA, peut procéder à des évaluations coordonnées des risques de sécurité inhérents à des chaînes d'approvisionnement de services, de systèmes ou de produits TIC critiques spécifiques, en tenant compte des facteurs de risque techniques et, le cas échéant, non techniques.

2. La Commission, après avoir consulté le groupe de coopération et l'ENISA, détermine les services, systèmes ou produits TIC critiques spécifiques qui peuvent faire l'objet de l'évaluation coordonnée des risques visée au paragraphe 1.

Article 20

Obligations concernant le signalement

1. Les États membres veillent à ce que les entités essentielles et importantes notifient dans les meilleurs délais aux autorités compétentes ou au CSIRT conformément aux paragraphes 3 et 4 tout incident ayant une incidence significative sur la fourniture de leurs services. Le cas échéant, ces entités notifient dans les meilleurs délais aux destinataires de leurs services […] **de tels** incidents susceptibles de nuire à la fourniture de ces services. Les États membres veillent à ce que ces entités signalent, entre autres, toute information permettant aux autorités compétentes ou au CSIRT de déterminer si l'incident a une incidence au niveau transfrontalier. **L'action de notification en elle-même n'accroît pas la responsabilité de l'entité qui en est à l'origine.**

2. […]

Le cas échéant, […] **les** entités **essentielles et importantes** notifient dans les meilleurs délais aux destinataires de leurs services qui sont potentiellement affectés par une cybermenace importante toutes les mesures ou corrections que ces destinataires peuvent appliquer en réponse à cette menace. Le cas échéant, les entités informent également leurs destinataires de la menace elle-même. […] **L'action de** notification **en elle-même** n'accroît pas la responsabilité de l'entité qui en est à l'origine.

3. Un incident est considéré comme "significatif" si:

   a) l'incident a causé ou est susceptible de causer une perturbation opérationnelle […] **grave des services** ou […] **de lourdes** pertes financières […] pour l'entité concernée;

   b) l'incident a affecté ou est susceptible d'affecter d'autres personnes physiques ou morales en causant des pertes matérielles ou non matérielles considérables.

4. Les États membres veillent à ce que, aux fins de la notification visée au paragraphe 1, les entités concernées soumettent aux autorités compétentes ou au CSIRT:

   a) sans retard injustifié et en tout cas dans les 24 heures après avoir eu connaissance de l'incident, une première notification **servant d'alerte précoce** qui, le cas échéant, indique si l'incident est vraisemblablement causé par une action illicite ou malveillante;

   b) à la demande d'une autorité compétente ou d'un CSIRT, un rapport intermédiaire sur les mises à jour pertinentes de la situation;

   c) un rapport **final** au plus tard un mois après […] **l'envoi de la première notification visée** au point a), comprenant au moins les éléments suivants:

      i) une description détaillée de l'incident, de sa gravité et de son incidence;

      ii) le type de menace ou la cause profonde qui a probablement déclenché l'incident;

      iii) les mesures d'atténuation appliquées et en cours.

   Les États membres prévoient que, dans des cas dûment justifiés et en accord avec les autorités compétentes ou le CSIRT, l'entité concernée peut déroger aux délais fixés aux points a) et c). **En particulier, une dérogation par rapport au délai visé au point c) peut se justifier dans les cas où l'incident est toujours en cours.**

5. Les autorités nationales compétentes ou le CSIRT fournissent, […] **dans les meilleurs délais après** la réception de la notification initiale visée au paragraphe 4, point a), une réponse à l'entité émettrice de la notification, y compris un retour d'information initial sur l'incident et, à la demande de l'entité, des orientations sur la mise en œuvre d'éventuelles mesures d'atténuation. Lorsque le CSIRT n'a pas reçu la notification visée au paragraphe 1, l'orientation est émise par l'autorité compétente en collaboration avec le CSIRT. Le CSIRT fournit un soutien technique supplémentaire si l'entité concernée le demande. Lorsqu'il y a lieu de suspecter que l'incident est de nature criminelle, les autorités nationales compétentes ou le CSIRT fournissent également des orientations sur les modalités de signalement de l'incident aux autorités répressives.

6. Lorsque c'est approprié, et notamment si l'incident visé au paragraphe 1 concerne deux États membres ou plus, l'autorité compétente, le CSIRT ou **le point de contact unique** informe les autres États membres touchés et l'ENISA de l'incident. **Ces informations comprennent au moins les éléments prévus au paragraphe 4.** Ce faisant, les autorités compétentes, les CSIRT et les points de contact uniques doivent, dans le respect du droit de l'Union ou de la législation nationale conforme au droit de l'Union, préserver la sécurité et les intérêts commerciaux de l'entité ainsi que la confidentialité des informations communiquées.

7. Lorsque la sensibilisation du public est nécessaire pour prévenir un incident ou pour faire face à un incident en cours, ou lorsque la divulgation de l'incident est par ailleurs dans l'intérêt public, l'autorité compétente ou le CSIRT et, le cas échéant, les autorités ou les CSIRT des autres États membres concernés peuvent, après avoir consulté l'entité concernée, informer le public de l'incident ou exiger de l'entité qu'elle le fasse.

8. À la demande de l'autorité compétente ou du CSIRT, le point de contact unique transmet les notifications reçues en vertu […] **du** paragraphe[…] 1 […] aux points de contact uniques des autres États membres touchés.

9. Le point de contact unique soumet […] **tous les six mois** à l'ENISA un rapport de synthèse comprenant des données anonymisées et agrégées sur les incidents, les cybermenaces majeures et les incidents évités notifiés conformément au[…] paragraphe[…] 1 […] et conformément à l'article 27. Afin de contribuer à la fourniture d'informations comparables, l'ENISA peut émettre des orientations techniques sur les paramètres des informations incluses dans le rapport de synthèse. **L'ENISA informe tous les six mois le groupe de coopération et le réseau des CSIRT de ses conclusions concernant les notifications reçues.**

10. Les autorités compétentes fournissent aux autorités compétentes désignées en vertu de la directive (UE) XXXX/XXXX [directive sur la résilience des entités critiques] des informations sur les incidents et les cybermenaces notifiés conformément aux paragraphes 1 et 2 par les entités essentielles identifiées comme des entités critiques**[**, ou comme des entités équivalentes aux entités critiques,**]** en vertu de la directive (UE) XXXX/XXXX [directive sur la résilience des entités critiques].

11. La Commission peut adopter des actes d'exécution précisant plus en détail le type d'informations, le format et la procédure d'une notification présentée en vertu des paragraphes 1 et 2. La Commission peut également adopter des actes d'exécution pour préciser plus en détail les cas dans lesquels un incident est considéré comme significatif au sens du paragraphe 3. Ces actes d'exécution sont adoptés en conformité avec la procédure d'examen visée à l'article 37, paragraphe 2.

Article 21

Recours aux schémas européens de certification de cybersécurité

1. Afin de démontrer la conformité à certaines exigences visées à l'article 18, **les États membres peuvent exiger que les entités utilisent des produits** […]**, services** […] **et processus TIC particuliers certifiés** dans le cadre de schémas européens de certification en matière de cybersécurité spécifiques adoptés conformément à l'article 49 du règlement (UE) 2019/881. Les produits, services et processus **TIC** soumis à la certification peuvent être développés par une entité essentielle ou importante ou achetés à des tiers.

2. La Commission […] **peut** adopter des actes […] **d'exécution** précisant quelles catégories d'entités essentielles **ou importantes** sont tenues **d'utiliser certains produits, services et processus TIC ou** d'obtenir un certificat […] dans le cadre de quels régimes européens de certification de cybersécurité […] **adoptés en vertu de l'article 49 du règlement (UE) 2019/881.**[…] **Ces actes d'exécution sont adoptés en conformité avec la procédure d'examen visée à l'article 37, paragraphe 2. Lorsqu'elle prépare ces actes d'exécution, conformément à l'article 56 du règlement (UE) 2019/881, la Commission:**

   i) tient compte de l'incidence des mesures, du point de vue des coûts, sur les fabricants ou fournisseurs de ces produits, services ou processus TIC et sur les utilisateurs, des avantages sociétaux ou économiques résultant du renforcement escompté du niveau de sécurité des produits, services ou processus TIC ciblés, ainsi que de la disponibilité de solutions de rechange sur le marché;

   ii) engage un processus de consultation ouvert, transparent et inclusif avec toutes les parties prenantes concernées et les États membres;

iii) prend en considération les délais de mise en œuvre ainsi que les mesures et périodes transitoires, en ce qui concerne, en particulier, l'incidence éventuelle des mesures sur les fabricants ou les fournisseurs de produits, services ou processus TIC, ou les utilisateurs de ceux-ci, en particulier les PME;

iv) tient compte de l'existence et de la mise en œuvre du droit des États membres concernés.

3. La Commission peut demander à l'ENISA de préparer un schéma candidat **ou de réexaminer un schéma européen de certification de cybersécurité existant** conformément à l'article 48, paragraphe 2, du règlement (UE) 2019/881 dans les cas où il n'existe pas de schéma européen de certification de cybersécurité approprié aux fins du paragraphe 2 **du présent article**.

Article 22

Normalisation

1. Afin de favoriser la convergence de la mise en œuvre de l'article 18, paragraphes 1 et 2, les États membres encouragent, sans imposer l'utilisation d'un type particulier de technologies ni créer de discrimination en faveur d'un tel type particulier de technologies, le recours à des normes et des spécifications européennes ou internationalement reconnues pour la sécurité des réseaux et des systèmes d'information.

2. L'ENISA, en collaboration avec les États membres, formule des avis et des lignes directrices concernant les domaines techniques qui doivent être pris en considération en lien avec le paragraphe 1, et concernant les normes existantes, y compris les normes nationales des États membres, qui permettraient de couvrir ces domaines.

Article 23

Bases de données des noms de domaines et des données d'enregistrement

1. Afin de contribuer à la sécurité, à la stabilité et à la résilience du DNS, les États membres veillent à ce que les registres des noms de domaines de premier niveau et les entités fournissant des services d'enregistrement de noms de domaines pour le registre de noms de domaines de premier niveau collectent et maintiennent les données d'enregistrement de noms de domaines exactes et complètes au sein d'une base de données dédiée avec la diligence requise, **conformément au** […] droit de l'Union en matière de protection des données à caractère personnel.

2. Les États membres veillent à ce que les bases de données relatives à l'enregistrement des noms de domaines visées au paragraphe 1 contiennent des informations pertinentes pour identifier et contacter les titulaires des noms de domaines et les points de contact qui gèrent les noms de domaines dans les registres des noms de domaines de premier niveau**, notamment au moins les éléments suivants:**

   a) le nom de domaine;

   b) la date d'enregistrement;

   c) les données relatives au titulaire, y compris:

      i) pour les personnes physiques: le nom, le prénom et l'adresse électronique;

      ii) pour les personnes morales: le nom et l'adresse électronique.

3. Les États membres veillent à ce que les registres des noms de domaines de premier niveau et les entités fournissant des services d'enregistrement de noms de domaines pour le registre de noms de domaines de premier niveau aient mis en place des politiques et des procédures visant à garantir que les bases de données contiennent des informations exactes et complètes. Les États membres veillent à ce que ces politiques et procédures soient mises à la disposition du public.

4. Les États membres veillent à ce que les registres des noms de domaines de premier niveau et les entités fournissant des services d'enregistrement de noms de domaines pour le registre de noms de domaines de premier niveau publient, dans les meilleurs délais après l'enregistrement d'un nom de domaine, des données d'enregistrement de domaine qui ne sont pas des données personnelles.

5. Les États membres veillent à ce que les registres des noms de domaines de premier niveau et les entités fournissant des services d'enregistrement de noms de domaines pour le registre de noms de domaines de premier niveau donnent accès aux données spécifiques d'enregistrement de noms de domaines sur demande légitime et dûment justifiée des demandeurs d'accès légitimes, dans le respect du droit de l'Union en matière de protection des données. Les États membres veillent à ce que les registres des noms de domaines de premier niveau et les entités fournissant des services d'enregistrement de noms de domaines pour le registre de noms de domaines de premier niveau répondent dans les meilleurs délais **et dans tous les cas dans un délai de 72 heures** à toutes les demandes d'accès. Les États membres veillent à ce que les politiques et procédures de divulgation de ces données soient rendues publiques.

Partie II

Compétence et enregistrement

Article 24

Compétence et territorialité

1 *bis*. Les entités au sens de la présente directive sont réputées relever de la compétence de l'État membre dans lequel elles fournissent leurs services. Les entités visées à l'annexe I, points 1 à 7 et 10, les prestataires de services de confiance et les fournisseurs de points d'échange internet visés à l'annexe I, point 8, et les entités visées à l'annexe II, points 1 à 5, sont réputés relever de la juridiction de l'État membre sur le territoire duquel ils sont établis.

1. Les fournisseurs de services DNS, les registres des noms de domaines de premier niveau **et les entités fournissant des services d'enregistrement de noms de domaine pour les registres de noms de domaines de premier niveau**, les fournisseurs de services d'informatique en nuage, les fournisseurs de services de centres de données**,** […] les fournisseurs de réseaux de diffusion de contenu**, les fournisseurs de services gérés et les fournisseurs de services de sécurité gérés** visés à l'annexe I, point**s** 8 **et 8 *bis***, ainsi que les fournisseurs de services numériques visés à l'annexe II, point 6, sont réputés relever de la juridiction de l'État membre dans lequel ils ont leur établissement principal dans l'Union.

2. Aux fins de la présente directive, les entités visées au paragraphe 1 sont réputées avoir leur établissement principal dans l'Union dans l'État membre où sont **principalement** prises les décisions relatives aux mesures de gestion des risques en matière de cybersécurité. Si **le lieu où ces décisions sont principalement prises ne peut pas être déterminé ou** si ces décisions ne sont pas prises dans un quelconque établissement de l'Union, l'établissement principal est considéré comme se trouvant dans l'État membre où l'entité possède l'établissement comptant le plus grand nombre de salariés dans l'Union. **Lorsque les services sont fournis par un groupe d'entreprises, l'établissement principal est considéré comme étant l'établissement principal du groupe d'entreprises.**

3. Si une entité visée au paragraphe 1 n'est pas établie dans l'Union, mais offre des services dans l'Union, elle désigne un représentant dans l'Union. Le représentant est établi dans l'un des États membres dans lesquels les services sont fournis. Ladite entité est considérée comme relevant de la compétence de l'État membre dans lequel le représentant est établi. En l'absence d'un représentant désigné au sein de l'Union en vertu du présent article, tout État membre dans lequel l'entité fournit des services peut intenter une action en justice contre l'entité pour non-respect des obligations découlant de la présente directive.

4. La désignation d'un représentant par une entité visée au paragraphe 1 est sans préjudice d'actions en justice qui pourraient être intentées contre l'entité elle-même.

4 *bis*. Les États membres qui ont reçu une demande d'assistance mutuelle en lien avec les entités visées au paragraphe 1 peuvent, dans les limites de la demande, prendre des mesures de surveillance et d'exécution appropriées à l'égard de l'entité concernée qui fournit des services ou qui dispose du réseau et du système d'information sur leur territoire.

Article 25

Registre pour certaines entités d'infrastructure numérique et certains fournisseurs de services numériques

1. […] **Les États membres veillent à ce que l**[…]es entités **visées à l'article 24, paragraphe 1, dont l'établissement principal se trouve sur leur territoire ou, si elles ne sont pas établies dans l'Union, dont le représentant désigné dans l'Union est établi sur leur territoire, soient tenues de** […] soumettre les informations suivantes **aux autorités compétentes** […] au plus tard [12 mois après l'entrée en vigueur de la directive]:

a) le nom de l'entité;

a *bis*) le type d'entité défini aux annexes I et II;

b) l'adresse de son établissement principal et de ses autres établissements légaux dans l'Union ou, si elle n'est pas établie dans l'Union, de son représentant désigné conformément à l'article 24, paragraphe 3;

c) les coordonnées actualisées, y compris les adresses de courrier électronique et les numéros de téléphone des entités **et de leurs représentants;**

d) les États membres dans lesquels l'entité fournit les services.

Le cas échéant, ces informations sont transmises par l'intermédiaire […] du mécanisme[…] national d'autonotification visé[…] à l'article 2 *bis*.

2. **Les États membres veillent à ce que l**[…]es entités visées au paragraphe 1 notifient […] **également** toute modification des informations qu'elles ont communiquées en vertu du paragraphe 1 dans les meilleurs délais et, en tout état de cause, dans un délai de trois mois à compter de la date à laquelle la modification a pris effet.

3. […] **Les points de contact uniques des États membres** transmettent **les informations visées aux paragraphes 1 et 2** […] à […] **l'ENISA**. […]

3 *bis*. Sur la base des informations reçues conformément au paragraphe 3, l'ENISA crée et tient à jour un registre des entités visées au paragraphe 1. À la demande des États membres, l'ENISA permet aux autorités compétentes concernées d'accéder au registre, tout en assurant les garanties nécessaires pour protéger la confidentialité des informations, le cas échéant.

4. […]

CHAPITRE V

Partage d'informations

Article 26

Dispositions relatives à l'échange d'informations en matière de cybersécurité

1. […] **Les** États membres veillent à ce que les entités essentielles et importantes puissent échanger entre elles**, à titre volontaire,** des informations pertinentes en matière de cybersécurité, y compris des informations relatives aux cybermenaces, **aux incidents évités,** aux vulnérabilités, aux indicateurs de compromission, aux tactiques, techniques et procédures, aux alertes de cybersécurité et aux outils de configuration, lorsque ce partage d'informations:

   a) vise à prévenir, détecter, répondre ou atténuer les incidents;

b) renforce le niveau de cybersécurité, notamment en sensibilisant aux cybermenaces, en limitant ou en empêchant leur "capacité de se propager", en soutenant une série de capacités de défense, en remédiant aux vulnérabilités et en les révélant, en mettant en œuvre des techniques de détection des menaces, des stratégies d'atténuation ou des étapes de réaction et de rétablissement.

2. Les États membres veillent à ce que l'échange d'informations ait lieu au sein de communautés […] d'entités essentielles et importantes. Cet échange est mis en œuvre au moyen d'accords de partage d'informations, compte tenu de la nature potentiellement sensible des informations partagées […].

3. Les États membres […] **peuvent établir** des règles précisant la procédure, les éléments opérationnels (y compris l'utilisation de plateformes TIC dédiées), le contenu et les conditions des accords de partage d'informations visés au paragraphe 2. Ces règles […] **peuvent** également **fixer** les détails de la participation des autorités publiques à ces accords, ainsi que les éléments opérationnels, y compris l'utilisation de plateformes informatiques dédiées. Les États membres offrent un soutien à l'application de ces accords conformément à leurs politiques visées à l'article 5, paragraphe 2, point g).

4. Les entités essentielles et importantes notifient aux autorités compétentes leur participation aux mécanismes de partage d'informations visés au paragraphe 2, lorsqu'elles commencent à participer à de tels mécanismes ou, le cas échéant, lorsqu'elles se retirent de ces mécanismes, une fois que le retrait prend effet.

5. […] **L**'ENISA soutient la mise en place des mécanismes de partage d'informations en matière de cybersécurité visés au paragraphe 2 par la fourniture de bonnes pratiques et d'orientations.

Article 27

Signalement volontaire d'informations pertinentes

1. Sans préjudice de l'article 20, les États membres veillent à ce que les entités essentielles et importantes puissent signaler, à titre volontaire, aux autorités compétentes ou aux CSIRT tout incident, cybermenace ou incident évité.

2. Sans préjudice de l'article 3, les États membres veillent à ce que les entités qui ne relèvent pas du champ d'application de la présente directive puissent, à titre volontaire, transmettre des signalements relatifs aux incidents importants, aux cybermenaces ou aux incidents évités. Lorsqu'ils traitent des signalements, les États membres agissent conformément à la procédure énoncée à l'article 20. Les États membres peuvent traiter les signalements obligatoires en leur donnant la priorité par rapport aux signalements volontaires. **Sans préjudice de la détection d'infractions pénales et des enquêtes et poursuites en la matière, un** […] signalement volontaire n'a pas pour effet d'imposer à l'entité qui est à l'origine du signalement des obligations supplémentaires auxquelles elle n'aurait pas été soumise si elle n'avait pas transmis ledit signalement.

3. Les signalements volontaires ne sont traités que lorsque leur traitement ne fait pas peser de charge disproportionnée ou inutile sur les États membres concernés.

CHAPITRE VI

Surveillance et exécution

Article 28

Aspects généraux concernant la surveillance et l'exécution

1. Les États membres veillent à ce que les autorités compétentes procèdent à une surveillance efficace et prennent les mesures nécessaires pour assurer le respect de la présente directive[…] et notamment des obligations énoncées aux articles 18**,** […] 20 **et 23**. **Les États membres peuvent autoriser les autorités compétentes à hiérarchiser la surveillance selon une approche fondée sur les risques.**

2. Pour traiter des incidents […] **de cybersécurité**, les autorités compétentes coopèrent étroitement avec les autorités chargées de la protection des données, **les autorités compétentes désignées en vertu de la directive (UE) XXXX/XXXX [directive sur la résilience des entités critiques], les organe de contrôle désignés en vertu du règlement (UE) 910/2014 et les autres autorités compétentes désignées en vertu d'actes juridiques sectoriels de l'Union**. […]

3. Sans préjudice des cadres législatifs et institutionnels nationaux, les États membres veillent à ce que, dans le cadre de la surveillance du respect de la présente directive par les entités de l'administration publique et de l'application d'éventuelles sanctions en cas de non-respect, les autorités compétentes disposent des pouvoirs appropriés pour mener à bien ces tâches en jouissant d'une indépendance opérationnelle vis-à-vis des entités surveillées. Les États membres peuvent décider d'imposer des mesures de surveillance et d'exécution appropriées, proportionnées et efficaces à l'égard de ces entités, conformément aux cadres et aux ordres juridiques nationaux.

Article 29

Surveillance et exécution pour les entités essentielles

1. Les États membres veillent à ce que les mesures de surveillance ou d'exécution imposées aux entités essentielles au titre des obligations énoncées dans la présente directive soient effectives, proportionnées et dissuasives, compte tenu des circonstances de chaque cas.

2. Les États membres veillent à ce que les autorités compétentes, lorsqu'elles accomplissent leurs missions de surveillance à l'égard d'entités essentielles, **suivent une approche fondée sur les risques et** aient le pouvoir de soumettre ces entités **au minimum** à:

   a) des inspections sur place et une surveillance à distance, y compris des contrôles aléatoires;

   b) des audits **de sécurité** réguliers;

   c) des audits de sécurité ciblés fondés sur des évaluations des risques ou sur des informations disponibles ayant trait aux risques;

   d) des scans de sécurité fondés sur des critères d'évaluation des risques objectifs, non discriminatoires, équitables et transparents**, lorsque cela est nécessaire pour des raisons techniques, avec la coopération de l'entité concernée**;

   e) des demandes d'informations nécessaires à l'évaluation des mesures de cybersécurité adoptées par l'entité, notamment les politiques de cybersécurité consignées par écrit […];

   f) des demandes d'accès à des données, à des documents ou à toutes informations nécessaires à l'accomplissement de leurs missions de surveillance;

   g) des demandes de preuves de la mise en œuvre de politiques de cybersécurité, telles que les résultats des audits de sécurité effectués par un auditeur qualifié et les éléments de preuve sous-jacents correspondants.

2 *bis*. Lorsqu'elles accomplissent leurs missions de surveillance prévues au paragraphe 2, les autorités compétentes peuvent mettre au point des méthodes de surveillance permettant de hiérarchiser ces tâches selon une approche fondée sur les risques.

3. Lorsqu'elles exercent leurs pouvoirs en vertu du paragraphe 2, points e) à g), les autorités compétentes mentionnent la finalité de la demande et précisent quelles sont les informations exigées.

4. Les États membres veillent à ce que les autorités compétentes, lorsqu'elles exercent leurs pouvoirs d'exécution à l'égard d'entités essentielles, aient **au minimum** le pouvoir:

a) d'émettre des avertissements concernant le non-respect par les entités des obligations énoncées dans la présente directive;

b) d'émettre des instructions contraignantes ou une injonction exigeant de ces entités qu'elles remédient aux insuffisances constatées ou aux violations des obligations énoncées dans la présente directive;

c) d'ordonner à ces entités de mettre un terme à un comportement qui ne respecte pas les obligations énoncées dans la présente directive et de ne pas le réitérer;

d) d'ordonner à ces entités de mettre leurs mesures de gestion des risques et/ou leurs obligations de signalement en conformité avec les obligations énoncées aux articles 18 et 20 de manière spécifique et dans un délai déterminé;

e) d'ordonner à ces entités d'informer la ou les personnes physiques ou morales à qui elles fournissent des services ou des activités susceptibles d'être affectées par une cybermenace importante de **la nature de la menace, ainsi que de** toutes mesures préventives ou réparatrices que ces personnes physiques ou morales pourraient prendre en réponse à cette menace;

f) d'ordonner à ces entités de mettre en œuvre les recommandations formulées à la suite d'un audit de sécurité dans un délai raisonnable;

g) […]

h) d'ordonner à ces entités de rendre publics les aspects de non-respect des obligations énoncées dans la présente directive de manière spécifique**, pour autant qu'une telle divulgation publique n'entraîne pas une exposition dommageable de l'entité concernée**;

i) […]

j) d'imposer ou de demander aux juridictions ou organes compétents d'imposer, conformément à la législation nationale, une amende administrative en vertu de l'article 31 en plus ou en lieu et place des mesures visées aux points a) à i) du présent paragraphe, en fonction des circonstances propres à chaque cas.

5. Lorsque les mesures d'exécution adoptées en vertu du paragraphe 4, points a) à d) et point f), se révèlent inefficaces, les États membres veillent à ce que les autorités compétentes aient le pouvoir de fixer un délai dans lequel l'entité essentielle est invitée à prendre les mesures nécessaires pour remédier aux insuffisances ou satisfaire aux exigences de ces autorités. Si la mesure demandée n'est pas prise dans le délai imparti, les États membres veillent à ce que les autorités compétentes aient le pouvoir:

a) de suspendre ou de demander **aux juridictions ou** aux organismes de certification ou d'autorisation**, conformément à la législation nationale,** de suspendre une certification ou une autorisation concernant tout ou partie des services ou activités fournis par une entité essentielle;

b) d'imposer ou de demander aux juridictions ou organes compétents d'imposer, conformément à la législation nationale, une interdiction temporaire interdisant à toute personne exerçant des responsabilités dirigeantes à un niveau de directeur général ou de représentant légal dans cette entité essentielle, ainsi qu'à toute autre personne physique tenue pour responsable de la violation, d'exercer des responsabilités dirigeantes dans cette entité.

Ces sanctions sont appliquées jusqu'à ce que l'entité prenne les mesures nécessaires pour remédier aux insuffisances ou se conformer aux exigences de l'autorité compétente à l'origine de l'application de ces sanctions.

Les sanctions prévues au présent paragraphe ne s'appliquent pas aux entités de l'administration publique relevant de la présente directive.

6. Les États membres veillent à ce que toute personne physique responsable d'une entité essentielle ou agissant en qualité de représentant d'une entité essentielle sur la base du pouvoir de la représenter, de prendre des décisions en son nom ou d'exercer son contrôle ait le pouvoir de veiller au respect, par l'entité, des obligations énoncées dans la présente directive. Les États membres veillent à ce que ces personnes physiques puissent être tenues responsables des manquements à leur devoir de veiller au respect des obligations énoncées dans la présente directive. **En ce qui concerne les entités de l'administration publique, cette disposition est sans préjudice des législations des États membres en ce qui concerne la responsabilité des agents de la fonction publique et des fonctionnaires élus et nommés.**

7. Lorsqu'elles prennent des mesures d'exécution ou appliquent des sanctions en vertu des paragraphes 4 et 5, les autorités compétentes respectent les droits de la défense et tiennent compte des circonstances propres à chaque cas et, au minimum, tiennent dûment compte:

   a) de la gravité de la violation et de l'importance des dispositions enfreintes. Parmi les violations devant être considérées comme graves, figurent: les violations répétées, le fait de ne pas notifier des incidents ayant des effets perturbateurs importants ou de ne pas y remédier, le fait de ne pas remédier aux insuffisances à la suite d'instructions contraignantes des autorités compétentes, le fait d'entraver des audits ou des activités de contrôle ordonnées par les autorités compétentes à la suite de la constatation d'une violation, la fourniture d'informations fausses ou manifestement inexactes relatives aux exigences en matière de gestion des risques ou aux obligations de signalement énoncées aux articles 18 et 20;

b) de la durée de la violation, y compris du caractère répété des violations;

c) des dommages effectifs causés, des pertes subies, des dommages potentiels ou des pertes qui auraient pu être engendrées, dans la mesure où il est possible de les déterminer. Lors de l'évaluation de cet aspect, il est tenu compte, entre autres, des pertes financières ou économiques effectives ou potentielles, des incidences sur d'autres services, du nombre d'utilisateurs touchés ou potentiellement touchés;

d) du fait que la violation a été commise délibérément ou par négligence;

e) des mesures prises par l'entité pour prévenir ou atténuer les dommages et/ou les pertes;

f) de l'application de codes de conduite approuvés ou de mécanismes de certification approuvés;

g) du degré de coopération de la ou des personnes physiques ou morales tenues pour responsables avec les autorités compétentes.

8. Les autorités compétentes exposent en détail les motifs de leurs décisions d'exécution. Avant de prendre de telles décisions, les autorités compétentes informent les entités concernées de leurs conclusions préliminaires et laissent à ces entités un délai raisonnable pour communiquer leurs observations**, sauf en cas de danger imminent**.

9. Les États membres veillent à ce que leurs autorités compétentes **au titre de la présente directive** informent les autorités compétentes concernées **au sein du même** […] État membre […] désignées conformément à la directive (UE) XXXX/XXXX [directive relative à la résilience des entités critiques] lorsqu'ils exercent leurs pouvoirs de surveillance et d'exécution dans le but de garantir qu'une entité définie comme critique **[**ou une entité équivalente à une entité critique**]** en vertu de la directive (UE) XXXX/XXXX [directive relative à la résilience des entités critiques] respecte ses obligations au titre de la présente directive. **Le cas échéant,** […] les autorités compétentes au titre de la directive (UE) XXXX/XXXX [directive relative à la résilience des entités critiques][…] **peuvent demander** aux autorités compétentes **au titre de la présente directive** […] **d'**exercer leurs pouvoirs de surveillance et d'exécution **en ce qui concerne** une identité essentielle **au titre de la présente directive qui est également définie** comme critique **[**ou équivalente**] au titre de la directive (UE) XXXX/XXXX [directive relative à la résilience des entités critiques].**

10. Les États membres veillent à ce que leurs autorités compétentes au titre de la présente directive informent le forum de supervision conformément à l'article 29, paragraphe 1, du règlement (UE) XXXX/XXXX [DORA] lorsqu'elles exercent leurs pouvoirs de surveillance et d'exécution dans le but de garantir qu'une entité essentielle désignée comme tiers prestataire critique de services informatiques au titre de l'article 28 du règlement (UE) XXXX/XXXX [DORA] respecte ses obligations au titre de la présente directive.

10 *bis*. Les États membres veillent à ce que leurs autorités compétentes au titre de la présente directive informent les autorités compétentes concernées désignées conformément au règlement (UE) n° 910/2014 lorsqu'elles exercent leurs pouvoirs de surveillance et d'exécution dans le but de garantir qu'une entité désignée comme prestataire de services de confiance au titre du règlement (UE) n° 910/2014 respecte ses obligations au titre de la présente directive.

Article 30

Surveillance et exécution pour les entités importantes

1. Lorsque, selon les éléments de preuve ou les indications **ou informations** communiquées, une entité importante ne respecte**rait** pas les obligations énoncées dans la présente directive, et notamment aux articles 18 et 20, les États membres veillent à ce que les autorités compétentes prennent des mesures, le cas échéant, dans le cadre de mesures de contrôle ex post.

2. Les États membres veillent à ce que les autorités compétentes, lorsqu'elles accomplissent leurs missions de surveillance à l'égard d'entités importantes, **suivent une approche fondée sur les risques et** aient le pouvoir de soumettre ces entités **au minimum** à:

   a) des inspections sur place et une surveillance à distance ex post;

   b) des audits de sécurité ciblés fondés sur des évaluations des risques ou sur des informations disponibles ayant trait aux risques;

   c) des scans de sécurité fondés sur des critères d'évaluation des risques objectifs, **non discriminatoires,** équitables et transparents**, lorsque cela est nécessaire pour des raisons techniques, avec la coopération de l'entité concernée**;

   d) des demandes de toutes informations nécessaires à l'évaluation ex post des mesures de cybersécurité […];

   e) des demandes d'accès à des données, à des documents et/ou à des informations nécessaires à l'accomplissement de leurs missions de surveillance;

   e *bis*) des demandes de preuves de la mise en œuvre de politiques de cybersécurité, telles que les résultats des audits de sécurité effectués par un auditeur qualifié et les éléments de preuve sous-jacents correspondants.

2 *bis*. Lorsqu'elles accomplissent leurs missions de surveillance prévues au paragraphe 2, les autorités compétentes peuvent mettre au point des méthodes de surveillance permettant de hiérarchiser ces tâches selon une approche fondée sur les risques.

3. Lorsqu'elles exercent leurs pouvoirs en vertu du paragraphe 2, points d) […] **à e *bis*)**, les autorités compétentes mentionnent la finalité de la demande et précisent quelles sont les informations exigées.

4. Les États membres veillent à ce que les autorités compétentes, lorsqu'elles exercent leurs pouvoirs d'exécution à l'égard d'entités importantes, aient **au minimum** le pouvoir:

a) d'émettre des avertissements concernant le non-respect par les entités des obligations énoncées dans la présente directive;

b) d'émettre des instructions contraignantes ou une injonction exigeant de ces entités qu'elles remédient aux insuffisances constatées ou aux violations des obligations énoncées dans la présente directive;

c) d'ordonner à ces entités de mettre un terme à un comportement qui ne respecte pas les obligations énoncées dans la présente directive et de ne pas le réitérer;

d) d'ordonner à ces entités de mettre leurs mesures de gestion des risques ou leurs obligations de signalement en conformité avec les obligations énoncées aux articles 18 et 20 de manière spécifique et dans un délai déterminé;

e) d'ordonner à ces entités d'informer la ou les personnes physiques ou morales à qui elles fournissent des services ou des activités susceptibles d'être affectées par une cybermenace importante de **la nature de la menace, ainsi que de** toutes mesures préventives ou réparatrices que ces personnes physiques ou morales pourraient prendre en réponse à cette menace;

f) d'ordonner à ces entités de mettre en œuvre les recommandations formulées à la suite d'un audit de sécurité dans un délai raisonnable;

g) d'ordonner à ces entités de rendre publics les aspects de non-respect de leurs obligations énoncées dans la présente directive de manière spécifique**, pour autant qu'une telle divulgation publique n'entraîne pas une exposition dommageable de l'entité concernée**;

h) […]

i) d'imposer ou de demander aux juridictions ou organes compétents d'imposer, conformément à la législation nationale, une amende administrative en vertu de l'article 31 en plus ou en lieu et place des mesures visées aux points a) à h) du présent paragraphe, en fonction des circonstances propres à chaque cas.

5. L'article 29, paragraphes 6 à 8, s'applique également aux mesures de surveillance et d'exécution prévues au présent article pour les entités importantes […].

Article 31

Conditions générales pour imposer des amendes administratives à des entités essentielles et importantes

1. Les États membres veillent à ce que les amendes administratives imposées aux entités essentielles et importantes en vertu du présent article pour des violations des obligations énoncées dans la présente directive soient, dans chaque cas d'espèce, effectives, proportionnées et dissuasives.

2. En fonction des circonstances propres à chaque cas, les amendes administratives sont imposées en complément ou à la place des mesures visées à l'article 29, paragraphe 4, points a) à i), à l'article 29, paragraphe 5, et à l'article 30, paragraphe 4, points a) à h).

3. Pour décider s'il y a lieu d'imposer une amende administrative et pour décider de son montant, dans chaque cas d'espèce, il est dûment tenu compte, au minimum, des éléments prévus à l'article 29, paragraphe 7.

4. Les États membres veillent à ce que les violations **par les entités essentielles** des obligations énoncées à l'article 18 ou à l'article 20, conformément aux paragraphes 2 et 3 du présent article, soient soumises à des amendes administratives d'un montant maximum s'élevant à au moins **4** […] 000 000 EUR ou**, dans le cas d'une personne morale,** […] à 2 % du chiffre d'affaires annuel mondial total de l'exercice précédent de l'entreprise à laquelle l'entité essentielle […] appartient, le montant le plus élevé étant retenu.

4 *bis*. Les États membres veillent à ce que les violations par les entités importantes des obligations énoncées à l'article 18 ou à l'article 20, conformément aux paragraphes 2 et 3 du présent article, soient soumises à des amendes administratives d'un montant maximum s'élevant à au moins 2 000 000 EUR ou, dans le cas d'une personne morale, à 1 % du chiffre d'affaires annuel mondial total de l'exercice précédent de l'entreprise à laquelle l'entité importante appartient, le montant le plus élevé étant retenu.

5. Les États membres peuvent prévoir le pouvoir d'imposer des astreintes pour contraindre une entité essentielle ou importante à mettre un terme à une violation conformément à une décision préalable de l'autorité compétente.

6. Sans préjudice des pouvoirs dont les autorités de contrôle disposent en vertu des articles 29 et 30, chaque État membre peut établir les règles déterminant si et dans quelle mesure des amendes administratives peuvent être imposées à des entités de l'administration publique au sens de l'article 4, paragraphe 23, sous réserve des obligations prévues dans la présente directive.

6 *bis*. Si le système juridique d'un État membre ne prévoit pas d'amendes administratives, les États membres veillent à ce que le présent article puisse être appliqué de telle sorte que l'amende soit déterminée par l'autorité de contrôle compétente et imposée par les juridictions nationales compétentes, tout en veillant à ce que ces voies de droit soit effectives et aient un effet équivalent aux amendes administratives imposées par les autorités de contrôle. En tout état de cause, les amendes imposées sont effectives, proportionnées et dissuasives. Les États membres concernés notifient à la Commission les dispositions légales qu'ils adoptent en vertu du présent paragraphe au plus tard le […] et, sans tarder, toute disposition légale modificative ultérieure ou toute modification ultérieure les concernant.

Article 32

Infractions donnant lieu à une violation de données à caractère personnel

1. Lorsque**, dans le cadre de la surveillance ou de l'exécution,** les autorités compétentes […] **prennent connaissance du fait que** l'infraction commise par une entité essentielle ou importante à l'égard des obligations énoncées aux articles 18 et 20 **de la présente directive peut** donne**r** lieu à une violation de données à caractère personnel au sens de l'article 4, paragraphe 12, du règlement (UE) 2016/679, devant être notifiée en vertu de l'article 33 dudit règlement, elles en informent**, dans les meilleurs délais,** les autorités de contrôle compétentes en vertu des articles 55 et 56 dudit règlement […].

2. Lorsque les autorités de contrôle compétentes conformément aux articles 55 et 56 du règlement (UE) 2016/679 décident d'exercer leurs pouvoirs en vertu de l'article 58, **paragraphe 2,** point i), dudit règlement et d'imposer une amende administrative, les autorités compétentes **visées à l'article 8 de la présente directive** n'imposent pas d'amende administrative pour […] **une** violation **constituée par le même acte** […] de l'article 31 de la présente directive. Les autorités compétentes peuvent toutefois appliquer les mesures d'exécution ou exercer les pouvoirs de sanction prévus à l'article 29, paragraphe 4, points a) à i), à l'article 29, paragraphe 5, et à l'article 30, paragraphe 4, points a) à h), de la présente directive.

3. Lorsque l'autorité de contrôle compétente en vertu du règlement (UE) 2016/679 est établie dans un autre État membre que l'autorité compétente, l'autorité compétente informe l'autorité de contrôle établie dans le même État membre.

Article 33

Sanctions

1. Les États membres fixent des règles relatives aux sanctions applicables en cas d'infraction aux dispositions nationales adoptées en vertu de la présente directive et prennent toutes les mesures nécessaires pour que ces règles soient appliquées. Les sanctions prévues sont effectives, proportionnées et dissuasives.

2. Les États membres informent la Commission, au plus tard [deux] ans après la date d'entrée en vigueur de la présente directive, des règles et mesures adoptées à cet égard, ainsi que, sans retard indu, de toute modification qui y serait apportée ultérieurement.

Article 34

Assistance mutuelle

1. Si une entité essentielle ou importante fournit des services dans plusieurs États membres, ou […] **fournit des services** dans un **ou plusieurs** État**s** membre**s** alors que ses réseaux et systèmes d'information sont situés dans un ou plusieurs autres États membres, […] **les** autorité**s** compétente**s** de**s** […] États membres **concernés** coopèrent et se prêtent mutuellement assistance si nécessaire. Cette coopération suppose, au minimum:

a) que les autorités compétentes appliquant des mesures de surveillance ou d'exécution dans un État membre informent et consultent, par l'intermédiaire du point de contact unique, les autorités compétentes des autres États membres concernés en ce qui concerne les mesures de surveillance et d'exécution prises […];

b) qu'une autorité compétente puisse demander à une autre autorité compétente de prendre les mesures de surveillance ou d'exécution […];

c) qu'une autorité compétente, dès réception d'une demande justifiée d'une autre autorité compétente, fournisse à l'autre autorité compétente une assistance **proportionnée en fonction des ressources dont elle-même dispose** afin que les mesures de surveillance ou d'exécution […] puissent être mises en œuvre de manière efficace, efficiente et cohérente. Cette assistance mutuelle peut porter sur des demandes d'informations et des mesures de contrôle, y compris des demandes de procéder à des inspections sur place, à une surveillance à distance ou à des audits de sécurité ciblés. Une autorité compétente à laquelle une demande d'assistance est adressée ne peut refuser cette demande que si, après un échange avec les autres autorités concernées […], il est établi que l'autorité n'est pas compétente pour fournir l'assistance demandée **ou ne dispose pas des ressources nécessaires,** ou que l'assistance demandée n'est pas proportionnée aux missions de surveillance **exercées par** l'autorité compétente […]**, ou que la demande concerne des informations ou implique l'exercice d'activités qui sont en contradiction avec la sécurité nationale, la sécurité publique ou la défense de cet État membre**.

2. Le cas échéant et d'un commun accord, les autorités compétentes de différents États membres peuvent mener à bien des actions communes de surveillance […].

CHAPITRE VII

Dispositions transitoires et finales

Article 35

Révision

La Commission réexamine périodiquement le fonctionnement de la présente directive et en rend compte au Parlement européen et au Conseil. Le compte rendu évalue notamment la pertinence des secteurs, des sous-secteurs, de la taille et du type des entités visées aux annexes I et II pour le fonctionnement de l'économie et de la société en ce qui concerne la cybersécurité. […] **Aux** fin**s de ce réexamen** […], la Commission tient compte des rapports […] du réseau des CSIRT sur l'expérience acquise au niveau […] opérationnel. Le premier rapport est présenté au plus tard le [54 mois après la date d'entrée en vigueur de la présente directive].

Article 36

[…]

[…]

[…]

Article 37

Procédure de comité

1. La Commission est assistée par un comité. Ledit comité est un comité au sens du règlement (UE) n° 182/2011.

2. Lorsqu'il est fait référence au présent paragraphe, l'article 5 du règlement (UE) n° 182/2011 s'applique.

3. Lorsque l'avis du comité doit être obtenu par procédure écrite, ladite procédure est close sans résultat lorsque, dans le délai prévu pour émettre un avis, le président du comité le décide ou un membre du comité le demande.

Article 38

Transposition

1. […] **A**u plus tard le **[24** mois après l'entrée en vigueur de la présente directive**]**, **les États membres adoptent et publient** les dispositions législatives, réglementaires et administratives nécessaires pour se conformer à la présente directive. Ils en informent immédiatement la Commission. Ils appliquent ces dispositions à partir du [un jour après la date visée au premier alinéa].

2. Lorsque les États membres adoptent ces dispositions, celles-ci contiennent une référence à la présente directive ou sont accompagnées d'une telle référence lors de leur publication officielle. Les modalités de cette référence sont arrêtées par les États membres.

Article 39

Modification du règlement (UE) n° 910/2014

Dans le règlement (UE) n° 910/2014, l'article 19 […] est supprimé **avec effet au [date limite de transposition de la directive]**.

Article 40

Modification de la directive (UE) 2018/1972

Dans la directive (UE) 2018/1972, les articles 40 et 41 […] sont supprimés **avec effet au [date limite de transposition de la directive]**.

Article 41

Abrogation

La directive (UE) 2016/1148 est abrogée avec effet au [date limite de transposition de la directive].

Les références à la directive (UE) 2016/1148 s'entendent comme faites à la présente directive et sont à lire selon le tableau de correspondance figurant à l'annexe II[…].

Article 42

Entrée en vigueur

La présente directive entre en vigueur le vingtième jour suivant celui de sa publication au *Journal officiel de l'Union européenne*.

Article 43

Destinataires

Les États membres sont destinataires de la présente directive.

Fait à Bruxelles, le

Par le Parlement européen	*Par le Conseil*
Le président	*Le président*

ANNEXE I

SECTEURS, SOUS-SECTEURS ET TYPES D'ENTITES

Secteur	Sous-secteur	Type d'entité
1. Énergie	a) Électricité	— Entreprises d'électricité au sens de l'article 2, point 57), de la directive (UE) 2019/944, qui remplissent la fonction de "fourniture" au sens de l'article 2, point 12), de ladite directive([39])
		— Gestionnaires de réseau de distribution au sens de l'article 2, point 29), de la directive (UE) 2019/944
		— Gestionnaires de réseau de transport au sens de l'article 2, point 35), de la directive (UE) 2019/944
		— Producteurs au sens de l'article 2, point 38), de la directive (UE) 2019/944
		— Opérateurs désignés du marché de l'électricité au sens de l'article 2, point 8), du règlement (UE) 2019/943([40])
		— Acteurs du marché de l'électricité au sens de l'article 2, point 25), du règlement (UE) 2019/943 fournissant des services d'agrégation, de participation active de la demande ou de stockage d'énergie au sens de l'article 2, points 18), 20) et 59), de la

[39] Directive (UE) 2019/944 du Parlement européen et du Conseil du 5 juin 2019 concernant des règles communes pour le marché intérieur de l'électricité et modifiant la directive 2012/27/UE (JO L 158 du 14.6.2019, p. 125).

[40] Règlement (UE) 2019/943 du Parlement européen et du Conseil sur le marché intérieur de l'électricité (JO L 158 du 14.6.2019, p. 54).

		directive (UE) 2019/944
	b) Réseaux de chaleur et de froid	— Réseaux de chaleur et de froid au sens de l'article 2, point 19), de la directive (UE) 2018/2001([41]) relative à la promotion de l'utilisation de l'énergie produite à partir de sources renouvelables
	c) Pétrole	— Exploitants d'oléoducs
		— Exploitants d'installations de production, de raffinage, de traitement, de stockage et de transport de pétrole
		— Entités centrales de stockage de pétrole au sens de l'article 2, point f), de la directive 2009/119/CE du Conseil([42])
	d) Gaz	— Entreprises de fourniture au sens de l'article 2, point 8), de la directive (UE) 2009/73/CE([43])
		— Gestionnaires de réseau de distribution au sens de l'article 2, point 6), de la directive 2009/73/CE
		— Gestionnaires de réseau de transport au sens de l'article 2, point 4), de la directive 2009/73/CE
		— Gestionnaires d'installation de stockage au sens de l'article 2, point 10), de la

41 Directive (UE) 2018/2001 du Parlement européen et du Conseil du 11 décembre 2018 relative à la promotion de l'utilisation de l'énergie produite à partir de sources renouvelables (JO L 328 du 21.12.2018, p. 82).

42 Directive 2009/119/CE du Conseil du 14 septembre 2009 faisant obligation aux États membres de maintenir un niveau minimal de stocks de pétrole brut et/ou de produits pétroliers (JO L 265 du 9.10.2009, p. 9).

43 Directive 2009/73/CE du Parlement européen et du Conseil du 13 juillet 2009 concernant des règles communes pour le marché intérieur du gaz naturel et abrogeant la directive 2003/55/CE (JO L 211 du 14.8.2009, p. 94).

		directive 2009/73/CE
		— Gestionnaires d'installation de GNL au sens de l'article 2, point 12), de la directive 2009/73/CE
		— Entreprises de gaz naturel au sens de l'article 2, point 1), de la directive 2009/73/CE
		— Exploitants d'installations de raffinage et de traitement de gaz naturel
	e) Hydrogène	Exploitants de systèmes de production, de stockage et de transmission d'hydrogène
2. Transports	a) Transports aériens	— Transporteurs aériens au sens de l'article 3, point 4), du règlement (CE) n° 300/2008([44]) **utilisés à des fins commerciales**
		— Entités gestionnaires d'aéroports au sens de l'article 2, point 2), de la directive 2009/12/CE([45]), aéroports au sens de l'article 2, point 1), de ladite directive, y compris les aéroports du réseau central énumérés à l'annexe II, section 2, du règlement (UE) n° 1315/2013([46]), et entités exploitant les installations annexes se trouvant dans les aéroports
		— Services du contrôle de la circulation aérienne au sens de

[44] Règlement (CE) n° 300/2008 du Parlement européen et du Conseil du 11 mars 2008 relatif à l'instauration de règles communes dans le domaine de la sûreté de l'aviation civile et abrogeant le règlement (CE) n° 2320/2002 (JO L 97 du 9.4.2008, p. 72).

[45] Directive 2009/12/CE du Parlement européen et du Conseil du 11 mars 2009 sur les redevances aéroportuaires (JO L 70 du 14.3.2009, p. 11).

[46] Règlement (CE) n° 1315/2013 du Parlement européen et du Conseil du 11 décembre 2013 sur les orientations de l'Union pour le développement du réseau transeuropéen de transport et abrogeant la décision n° 661/2010/UE (JO L 348 du 20.12.2013, p. 1).

		l'article 2, point 1), du règlement (CE) n° 549/2004([47])
	b) Transports ferroviaires	— Gestionnaires des infrastructures au sens de l'article 3, point 2), de la directive 2012/34/UE([48])
		— Entreprises ferroviaires au sens de l'article 3, point 1), de la directive 2012/34/UE, y compris les exploitants d'installations de services au sens de l'article 3, point 12), de la directive 2012/34/UE
	c) Transports par eau	— Sociétés de transport terrestre, maritime et côtier de passagers et de fret au sens de l'annexe I du règlement (CE) n° 725/2004([49]), à l'exclusion des navires exploités à titre individuel par ces sociétés
		— Entités gestionnaires des ports au sens de l'article 3, point 1), de la directive 2005/65/CE([50]), y compris les installations portuaires au sens de l'article 2, point 11), du règlement (CE) n° 725/2004, ainsi que les entités exploitant des infrastructures et des équipements à l'intérieur des ports

47 Règlement (CE) n° 549/2004 du Parlement européen et du Conseil du 10 mars 2004 fixant le cadre pour la réalisation du ciel unique européen ("règlement-cadre") (JO L 96 du 31.3.2004, p. 1).

48 Directive 2012/34/UE du Parlement européen et du Conseil du 21 novembre 2012 établissant un espace ferroviaire unique européen (JO L 343 du 14.12.2012, p. 32).

49 Règlement (CE) n° 725/2004 du Parlement européen et du Conseil du 31 mars 2004 relatif à l'amélioration de la sûreté des navires et des installations portuaires (JO L 129 du 29.4.2004, p. 6).

50 Directive 2005/65/CE du Parlement européen et du Conseil du 26 octobre 2005 relative à l'amélioration de la sûreté des ports (JO L 310 du 25.11.2005, p. 28).

		— Exploitants de services de trafic maritime au sens de l'article 3, point o), de la directive 2002/59/CE([51])
	d) Transports routiers	— Autorités routières au sens de l'article 2, point 12), du règlement délégué (UE) 2015/962 de la Commission([52]) chargées du contrôle de gestion du trafic**, à l'exclusion des entités publiques pour lesquelles la gestion du trafic ou l'utilisation des systèmes de transport intelligents ne constituent qu'une partie non essentielle de leur activité générale**
		— Exploitants de systèmes de transport intelligents au sens de l'article 4, point 1), de la directive 2010/40/UE([53])
3. Secteur bancaire		— Établissements de crédit au sens de l'article 4, point 1), du règlement (UE) n° 575/2013([54]) **[, à l'exception de ceux visés à l'article 2, paragraphe 5, point 8), de la directive 2013/36/UE qui sont exemptés conformément à l'article 2, paragraphe 4, du règlement XX [DORA]]**

[51] Directive 2002/59/CE du Parlement européen et du Conseil du 27 juin 2002 relative à la mise en place d'un système communautaire de suivi du trafic des navires et d'information, et abrogeant la directive 93/75/CEE du Conseil (JO L 208 du 5.8.2002, p. 10).

[52] Règlement délégué (UE) 2015/962 de la Commission du 18 décembre 2014 complétant la directive 2010/40/UE du Parlement européen et du Conseil en ce qui concerne la mise à disposition, dans l'ensemble de l'Union, de services d'informations en temps réel sur la circulation (JO L 157 du 23.6.2015, p. 21).

[53] Directive 2010/40/UE du Parlement européen et du Conseil du 7 juillet 2010 concernant le cadre pour le déploiement de systèmes de transport intelligents dans le domaine du transport routier et d'interfaces avec d'autres modes de transport (JO L 207 du 6.8.2010, p. 1).

[54] Règlement (UE) n° 575/2013 du Parlement européen et du Conseil du 26 juin 2013 concernant les exigences prudentielles applicables aux établissements de crédit et aux entreprises d'investissement et modifiant le règlement (UE) n° 648/2012 (JO L 176 du 27.6.2013, p. 1).

4. Infrastructures des marchés financiers		— Exploitants de plateformes de négociation au sens de l'article 4, point 24), de la directive 2014/65/UE([55])
		— Contreparties centrales au sens de l'article 2, point 1), du règlement (UE) n° 648/2012([56])
5. Santé		— Prestataires de soins de santé au sens de l'article 3, point g), de la directive 2011/24/UE([57])
		— Laboratoires de référence de l'Union européenne visés à l'article 15 du règlement XXXX/XXXX relatif aux menaces transfrontières graves sur la santé([58])
		— Entités exerçant des activités de recherche et de développement dans le domaine des médicaments au sens de l'article 1, point 2, de la directive 2001/83/CE([59]) — Entités fabriquant des produits pharmaceutiques de base et des préparations pharmaceutiques au sens de la NACE Rév. 2, section C, division 21 — Entités fabriquant des dispositifs médicaux considérés comme critiques en cas d'urgence de santé

[55] Directive 2014/65/UE du Parlement européen et du Conseil du 15 mai 2014 concernant les marchés d'instruments financiers et modifiant la directive 2002/92/CE et la directive 2011/61/UE (JO L 173 du 12.6.2014, p. 349).

[56] Règlement (UE) n° 648/2012 du Parlement européen et du Conseil du 4 juillet 2012 sur les produits dérivés de gré à gré, les contreparties centrales et les référentiels centraux (JO L 201 du 27.7.2012, p. 1).

[57] Directive 2011/24/UE du Parlement européen et du Conseil du 9 mars 2011 relative à l'application des droits des patients en matière de soins de santé transfrontaliers (JO L 88 du 4.4.2011, p. 45).

[58] [Règlement du Parlement européen et du Conseil relatif aux menaces transfrontières graves sur la santé et abrogeant la décision n° 1082/2013/UE, référence à mettre à jour une fois que la proposition COM (2020) 727 final sera adoptée].

[59] Directive 2001/83/CE du Parlement européen et du Conseil du 6 novembre 2001 instituant un code communautaire relatif aux médicaments à usage humain (JO L 311 du 28.11.2001, p. 67).

		publique ("liste des dispositifs médicaux critiques en cas d'urgence de santé publique") au sens de l'article 20 du règlement XXXX([60])
6. Eau potable		Fournisseurs et distributeurs d'eaux destinées à la consommation humaine au sens de l'article 2, point 1) a), de la directive 98/83/CE du Conseil([61]), à l'exclusion des distributeurs pour lesquels la distribution d'eaux destinées à la consommation humaine ne constitue qu'une partie **non essentielle** de leur activité générale de distribution d'autres produits et biens […]
7. Eaux usées		Entreprises collectant, éliminant ou traitant les eaux urbaines, ménagères et industrielles usées au sens de l'article 2, points 1) à 3), de la directive 91/271/CEE du Conseil([62]), **à l'exclusion des entreprises pour lesquelles la collecte, l'élimination ou le traitement des eaux urbaines, ménagères et industrielles usées ne constituent qu'une partie non essentielle de leur activité générale** […]
8. Infrastructure numérique		— Fournisseurs de points d'échange internet
		— Fournisseurs de services DNS, **à l'exclusion des opérateurs de serveurs racines de noms de domaines**
		— Registres de noms de domaines de premier niveau
		— Fournisseurs de services d'informatique en nuage

[60] [Règlement du Parlement européen et du Conseil relatif à un rôle renforcé de l'Agence européenne des médicaments dans la préparation aux crises et la gestion de celles-ci en ce qui concerne les médicaments et les dispositifs médicaux, référence à mettre à jour une fois que la proposition COM(2020) 725 final sera adoptée].

[61] Directive 98/83/CE du Conseil du 3 novembre 1998 relative à la qualité des eaux destinées à la consommation humaine (JO L 330 du 5.12.1998, p. 32).

[62] Directive 91/271/CEE du Conseil du 21 mai 1991 relative au traitement des eaux urbaines résiduaires (JO L 135 du 30.5.1991, p. 40).

		— Fournisseurs de services de centres de données
		— Fournisseurs de réseaux de diffusion de contenu
		— Prestataires de services de confiance au sens de l'article 3, point 19), du règlement (UE) n° 910/2014([63])
		— Fournisseurs de réseaux de communications électroniques publics au sens de l'article 2, point 8), de la directive (UE) 2018/1972([64]) ou fournisseurs de services de communications électroniques au sens de l'article 2, point 4), de la directive (UE) 2018/1972 lorsque leurs services sont accessibles au public
8 *bis*. Gestion des services informatiques **(B2B)**		**— Fournisseurs de services gérés** **— Fournisseurs de services de sécurité gérés**
9. **Entités de l'a**dministration publique		— Entités de l'administration publique des pouvoirs publics centraux **définies comme telles par un État membre conformément au droit national** — […][65][…] — […]

[63] Règlement (UE) n° 910/2014 du Parlement européen et du Conseil du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/CE (JO L 257 du 28.8.2014, p. 73).

[64] Directive (UE) 2018/1972 du Parlement européen et du Conseil du 11 décembre 2018 établissant le code des communications électroniques européen (JO L 321 du 17.12.2018, p. 36).

[65] […]

10. Espace		— Exploitants d'infrastructures terrestres, détenues, gérées et exploitées par des États membres ou par des parties privées, qui soutiennent la fourniture de services spatiaux, à l'exclusion des fournisseurs de réseaux de communications électroniques publics au sens de l'article 2, point 8), de la directive 2018/1972/UE

ANNEXE II

SECTEURS, SOUS-SECTEURS ET TYPES D'ENTITES

Secteur	Sous-secteur	Type d'entité
1. Services postaux et de courrier		Prestataires de services postaux au sens de l'article 2, point 1), de la directive 97/67/CE([66])**, y compris les** […] prestataires de services de courrier
2. Gestion des déchets		Entreprises exécutant des opérations de gestion des déchets au sens de l'article 3, point 9), de la directive 2008/98/CE([67]), à l'exclusion des entreprises pour qui la gestion des déchets n'est pas la principale activité économique

[66] Directive 97/67/CE du Parlement européen et du Conseil du 15 décembre 1997 concernant des règles communes pour le développement du marché intérieur des services postaux de la Communauté et l'amélioration de la qualité du service (JO L 15 du 21.1.1998, p. 14)**, telle que modifiée par la directive 2008/6/CE du Parlement européen et du Conseil du 20 février 2008 modifiant la directive 97/67/CE en ce qui concerne l'achèvement du marché intérieur des services postaux de la Communauté (JO L 52 du 27.2.2008, p. 3)**.

[67] Directive 2008/98/CE du Parlement européen et du Conseil du 19 novembre 2008 relative aux déchets et abrogeant certaines directives (JO L 312 du 22.11.2008, p. 3).

3. Fabrication, production et distribution de produits chimiques		Entreprises procédant à la fabrication […] et à la distribution de substances et […] **de mélanges** au sens de l'article 3, points […]9 et 14, du règlement (CE) n° 1907/2006([68]) **et entreprises procédant à la production d'articles à partir de substances ou de mélanges au sens de l'article 3, point 3, dudit règlement**
4. Production, transformation et distribution des denrées alimentaires		Entreprises du secteur alimentaire au sens de l'article 3, point 2), du règlement (CE) n° 178/2002([69]) **qui exercent des activités de distribution en gros ainsi que de production et de transformation industrielles**
5. Fabrication	a) Fabrication de dispositifs médicaux et de dispositifs médicaux de diagnostic in vitro	Entités fabriquant des dispositifs médicaux au sens de l'article 2, point 1), du règlement (UE) 2017/745([70]) et entités fabriquant des dispositifs médicaux de diagnostic in vitro au sens de l'article 2, point 2), du règlement (UE) 2017/746([71]), à l'exception des entités fabriquant des dispositifs médicaux mentionnés

[68] Règlement (CE) n° 1907/2006 du Parlement européen et du Conseil du 18 décembre 2006 concernant l'enregistrement, l'évaluation et l'autorisation des substances chimiques, ainsi que les restrictions applicables à ces substances (REACH), instituant une agence européenne des produits chimiques, modifiant la directive 1999/45/CE et abrogeant le règlement (CEE) n° 793/93 du Conseil et le règlement (CE) n° 1488/94 de la Commission ainsi que la directive 76/769/CEE du Conseil et les directives 91/155/CEE, 93/67/CEE, 93/105/CE et 2000/21/CE de la Commission (JO L 396 du 30.12.2006, p. 1).

[69] Règlement (CE) n° 178/2002 du Parlement européen et du Conseil du 28 janvier 2002 établissant les principes généraux et les prescriptions générales de la législation alimentaire, instituant l'Autorité européenne de sécurité des aliments et fixant des procédures relatives à la sécurité des denrées alimentaires (JO L 31 du 1.2.2002, p. 1).

[70] Règlement (UE) 2017/745 du Parlement européen et du Conseil du 5 avril 2017 relatif aux dispositifs médicaux, modifiant la directive 2001/83/CE, le règlement (CE) n° 178/2002 et le règlement (CE) n° 1223/2009 et abrogeant les directives 90/385/CEE et 93/42/CEE du Conseil (JO L 117 du 5.5.2017, p. 1).

[71] Règlement (UE) 2017/746 du Parlement européen et du Conseil du 5 avril 2017 relatif aux dispositifs médicaux de diagnostic in vitro et abrogeant la directive 98/79/CE et la décision 2010/227/UE de la Commission (JO L 117 du 5.5.2017, p. 176).

		à l'annexe 1, point 5
	b) Fabrication de produits informatiques, électroniques et optiques	Entreprises exerçant l'une des activités économiques visées dans la NACE Rév. 2, section C, division 26
	c) Fabrication d'équipements électriques	Entreprises exerçant l'une des activités économiques visées dans la NACE Rév. 2, section C, division 27
	d) Fabrication de machines et équipements n.c.a.	Entreprises exerçant l'une des activités économiques visées dans la NACE Rév. 2, section C, division 28
	e) Construction de véhicules automobiles, remorques et semi-remorques	Entreprises exerçant l'une des activités économiques visées dans la NACE Rév. 2, section C, division 29
	f) Fabrication d'autres matériels de transport	Entreprises exerçant l'une des activités économiques visées dans la NACE Rév. 2, section C, division 30
6. Fournisseurs numériques		— Fournisseurs de places de marché en ligne
		— Fournisseurs de moteurs de recherche en ligne
		— Fournisseurs de plateformes de réseaux sociaux