Parlement européen
2019-2024

Commission des libertés civiles, de la justice et des affaires intérieures

2020/0359(COD)

15.10.2021

AVIS

de la commission des libertés civiles, de la justice et des affaires intérieures

à l'intention de la commission de l'industrie, de la recherche et de l'énergie

sur la proposition de directive du Parlement européen et du Conseil concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union, abrogeant la directive (UE) 2016/1148
(COM(2020)0823 – C9-0422/2020 – 2020/0359(COD))

Rapporteur pour avis(*):Lukas Mandl

(*) Commission associée – Article 57 du règlement intérieur

PA_Legam

JUSTIFICATION SUCCINCTE

La proposition de directive du Parlement européen et du Conseil concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union, abrogeant la directive (UE) 2016/1148 (directive SRI 2)[1] fait partie d'un ensemble plus large d'initiatives à l'échelle de l'Union ayant pour objectif d'accroître la résilience des entités publiques et privées face aux menaces. La proposition vise à remédier aux lacunes de la législation existante et à permettre aux entités relevant de son champ d'application de mieux répondre aux nouveaux défis recensés par la Commission dans son analyse d'impact, laquelle comprenait une vaste consultation des parties intéressées. Parmi ces défis figurent en particulier l'utilisation croissante de supports et formats numériques dans le marché intérieur et l'évolution du paysage des menaces qui pèsent sur la cybersécurité.

La base juridique de la proposition est l'article 114 du traité FUE (marché intérieur). Du point de vue de la commission LIBE, il importe toutefois de souligner que les mesures que la directive SRI 2 impose aux réseaux et systèmes d'information ne servent pas seulement à assurer le bon fonctionnement du marché intérieur. La directive devrait également contribuer à la sécurité de l'Union dans son ensemble, notamment en évitant des divergences entre les États membres en matière de vulnérabilité aux risques liés à la cybersécurité.

À cette fin, il est essentiel d'éliminer les divergences existant entre les États membres en raison d'interprétations différentes du droit par les États membres. Pour cette raison, le rapporteur se félicite de la condition uniforme établie par le règlement pour déterminer les entités relevant du champ d'application de la directive. Des suggestions supplémentaires sont formulées pour éviter des divergences dans la mise en œuvre, notamment obliger la Commission à publier des lignes directrices relatives à la mise en œuvre de la lex specialis et des critères applicables aux PME (ce qui devrait également servir la clarté juridique et permettre d'éviter les charges inutiles) et exiger du groupe de coopération qu'il précise davantage les facteurs non techniques à prendre en compte dans les évaluations des risques liés aux chaînes d'approvisionnement. Il est en outre souligné que la coopération entre les autorités compétentes doit avoir lieu tant au sein des États membres qu'entre eux, et ce en temps réel.

Le projet de rapport intègre par ailleurs un certain nombre de **recommandations formulées par le CEPD** dans son avis sur la stratégie en matière de cybersécurité et la directive SRI 2.0[2]. Plus important encore, il est précisé tant dans les considérants que dans le dispositif du texte que tout traitement de données à caractère personnel au titre de la directive SRI 2 est sans préjudice du règlement (UE) 2016/679 (RGPD)[3] et de la directive 2002/58/CE[4] (vie

[1] 2020/0359(COD).

[2] Avis 5/2021: https://edps.europa.eu/system/files/2021-05/21-03-11_edps_nis2-opinion_fr_0.pdf.

[3] 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).

[4] 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

privée et communications électroniques). Le terme «sécurité des réseaux et des systèmes d'information» (ne couvre que la protection de la technologie) ayant une portée plus étroite que celle de la «cybersécurité» (couvre également les activités visant à protéger les utilisateurs), le premier terme n'est utilisé que lorsque le contexte est purement technique. En ce qui concerne les noms de domaine et les données d'enregistrement, des précisions sont proposées en ce qui concerne 1) la base juridique de la publication d'«informations pertinentes» aux fins de l'identification et des contacts, 2) les catégories de données d'enregistrement de domaine faisant l'objet d'une publication (sur la base d'une recommandation de l'ICANN) et 3) les entités susceptibles d'être des «demandeurs d'accès légitimes». Il est également précisé dans le texte juridique que la proposition n'a pas d'effet sur l'attribution de compétences et les compétences des autorités de contrôle de la protection des données en vertu du RGPD. Enfin, une base juridique plus complète est prévue pour la coopération et l'échange d'informations pertinentes entre les autorités compétentes au titre de la proposition et les autres autorités de contrôle concernées, notamment les autorités de contrôle au titre du RGPD.

D'autres modifications apportées par le rapporteur de la commission LIBE à la proposition de la Commission ont trait aux points suivants:

- Aux fins de la cohérence entre la directive SRI 2 et la proposition de directive sur la résilience des entités critiques (ICE)[5], le libellé de certaines dispositions a été aligné sur celui de la proposition de directive sur les ICE. Conformément à une modification similaire envisagée pour la directive sur les ICE, qui devrait couvrir les mêmes secteurs que la directive SRI 2, il est proposé d'ajouter «production, transformation et distribution des denrées alimentaires» au champ d'application.
- En ce qui concerne les données à caractère personnel, il est précisé que le scannage des réseaux et systèmes d'information par les CSIRT devrait être conforme non seulement au règlement (UE) 2016/679 (RGPD)[6], mais aussi à la directive 2002/58/CE[7] (vie privée et communications électroniques). Les transferts internationaux de données à caractère personnel au titre de la directive à l'examen devraient être conformes au chapitre V du RGPD.
- Le groupe de coopération devrait se réunir deux fois par an au lieu d'une fois pour faire le point sur les dernières évolutions en matière de cybersécurité. Le CEPD devrait prendre part aux réunions du groupe de coopération en qualité d'observateur.
- L'ENISA devrait publier un rapport annuel plutôt que bisannuel sur l'état de la

---

des communications électroniques (directive vie privée et communications électroniques), JO L 201 du 31.7.2002, p. 37.

[5] 2020/0365(COD).

[6] 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).

[7] 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.

cybersécurité dans l'Union. Il convient par ailleurs de prendre en compte dans le rapport les répercussions des incidents de cybersécurité sur la protection des données à caractère personnel dans l'Union.

- Le délai de notification des incidents est aligné sur le délai de notification des violations prévu par le RGPD, à savoir 72 heures.
- Si la notification des incidents réels de cybersécurité par des entités essentielles et importantes devrait en effet être obligatoire, la notification des cybermenaces devrait être volontaire afin de limiter la charge administrative et d'éviter des signalements excessifs. Pour être considéré comme significatif, un incident devrait avoir causé un dommage réel et touché d'autres personnes physiques et morales, et pas seulement «être susceptible» de produire de tels effets.
- Les circonstances à prendre en compte pour décider d'une sanction à la suite d'une violation des règles de cybersécurité sont alignées sur le RGPD. Étant donné que cela irait à l'encontre de la pratique actuelle en matière de responsabilité dans le droit de l'Union, il ne devrait pas être possible d'interdire temporairement à des personnes physiques d'exercer des fonctions de direction.
- Afin d'éviter des atteintes à la réputation, les entités ne devraient pas être tenues de rendre publics les aspects du non-respect des exigences de la directive à l'examen ou l'identité des personnes physiques ou morales responsables de l'infraction.

AMENDEMENTS

La commission des libertés civiles, de la justice et des affaires intérieures invite la commission de l'industrie, de la recherche et de l'énergie, compétente au fond, à prendre en considération les amendements suivants:

Amendement 1

Proposition de directive
Considérant 1

Texte proposé par la Commission	*Amendement*
(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.	(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 ***à la sécurité de l'Union et*** au fonctionnement efficace de ***son économie*** et de ***sa*** société.

[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).

[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).

Amendement 2

Proposition de directive
Considérant 2

Texte proposé par la Commission	*Amendement*
(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 cybersécurité, 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.	(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 cybersécurité, 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 et du réseau des centres de réponse aux incidents de sécurité informatique (ci-après le «réseau des CSIRT»). 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. ***En outre, l'expansion des activités en ligne dans le contexte de la pandémie de COVID-19 a mis en évidence***

	l'importance de la cybersécurité, qui est essentielle pour que les citoyens de l'UE puissent faire confiance à l'innovation et à la connectivité, ainsi que l'importance de l'éducation et de la formation à grande échelle dans ce domaine. La Commission devrait donc soutenir les États membres dans la conception de programmes éducatifs sur la cybersécurité afin de permettre aux entités importantes et essentielles de recruter des experts en cybersécurité qui leur permettent de se conformer aux obligations découlant de la présente directive.
[12] Article 11 de la directive (UE) 2016/1148.	[12] Article 11 de la directive (UE) 2016/1148.
[13] Article 12 de la directive (UE) 2016/1148.	[13] Article 12 de la directive (UE) 2016/1148.

Amendement 3

Proposition de directive
Considérant 3

Texte proposé par la Commission	*Amendement*
(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	(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.

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***, au fonctionnement de notre démocratie et aux valeurs et libertés sur lesquelles notre société repose***. La préparation à la cybersécurité et l'effectivité de la cybersécurité sont dès lors plus importantes que jamais ***à la sécurité de l'Union et au*** bon fonctionnement du marché intérieur***, compte tenu de la transformation numérique des activités quotidiennes dans l'ensemble de l'Union. Cela nécessite une coopération plus étroite entre les autorités au sein des États membres et entre ceux-ci, ainsi qu'entre les autorités nationales et les organes compétents de l'Union.***

Amendement 4

Proposition de directive
Considérant 5

Texte proposé par la Commission	*Amendement*
(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 normes 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	(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 normes différentes. ***En fin de compte, ces divergences peuvent aggraver la vulnérabilité de certains États membres aux menaces en matière de cybersécurité, ce qui peut avoir des retombées dans l'ensemble de l'Union, tant au regard du marché intérieur que de la sécurité en général.*** La présente directive a pour objectif de supprimer ces divergences importantes entre les États membres, notamment en définissant des règles minimales concernant le fonctionnement

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.	d'un cadre réglementaire coordonné, en établissant des mécanismes permettant une coopération efficace ***et en temps réel*** entre les autorités compétentes ***au sein d'un même*** État membre ***et entre les autorités compétentes des différents États membres***, 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.

Amendement 5

Proposition de directive
Considérant 6

Texte proposé par la Commission	*Amendement*
(6) La présente directive ne modifie pas la possibilité donnée à chaque État membre d'adopter les mesures nécessaires pour garantir la protection des intérêts essentiels de sa sécurité, assurer l'action publique et la sécurité publique et permettre la détection d'infractions pénales et les enquêtes et poursuites en la matière, dans le respect du droit de l'Union. Conformément à l'article 346 du TFUE, aucun État membre n'est tenu de fournir des renseignements dont la divulgation serait contraire aux intérêts essentiels de sa sécurité intérieure. À cet égard, les règles nationales et 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) La présente directive ne modifie pas la possibilité donnée à chaque État membre d'adopter les mesures nécessaires pour garantir la protection des intérêts essentiels de sa sécurité ***nationale***, assurer l'action publique et la sécurité publique et permettre ***la prévention et*** la détection d'infractions pénales et les enquêtes et poursuites en la matière, dans le respect du droit de l'Union. Conformément à l'article 346 du TFUE, aucun État membre n'est tenu de fournir des renseignements dont la divulgation serait contraire aux intérêts essentiels de sa sécurité intérieure. À cet égard, les règles nationales et 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.
[14] Le protocole «Traffic Light Protocol» permet à une personne partageant des	[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).

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).

Amendement 6

Proposition de directive
Considérant 8

Texte proposé par la Commission	*Amendement*
(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 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. Les États membres ne devraient pas être tenus de dresser la liste des entités qui remplissent ce critère d'application générale portant sur la taille.	(8) ***Pour ce qui est de la responsabilité des États membres,*** 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»)***, ce qui a entraîné des*** divergences importantes entre les États membres à cet égard***. Sans préjudice*** des ***exceptions spécifiques prévues par la présente directive***, il convient d'établir un critère uniforme déterminant les entités qui relèvent du champ d'application de la présente directive ***afin d'éliminer ces divergences et de garantir la sécurité juridique concernant les exigences de gestion des risques et les obligations de signalement pour toutes les entités concernées***. 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. Les États membres ne devraient pas être tenus de dresser la liste des entités qui remplissent ce critère d'application générale portant sur la taille.

[15] Recommandation 2003/361/CE de la

[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).

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

Amendement 7

Proposition de directive
Considérant 8 bis (nouveau)

Texte proposé par la Commission	*Amendement*
	(8 bis) Compte tenu des différences entre les cadres nationaux de l'administration publique, les États membres conservent leur capacité décisionnelle en ce qui concerne la désignation des entités relevant du champ d'application de la présente directive.

Amendement 8

Proposition de directive
Considérant 9

Texte proposé par la Commission	*Amendement*
(9) ***Toutefois, 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.	(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 ***sur la base d'une évaluation des risques, notamment les entités définies comme des entités critiques ou des entités équivalentes à des entités critiques au sens de la directive (UE) XXX/XXX du Parlement européen et du Conseil[1 bis],*** 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.
	1 bis Directive (UE) [XXX/XXX] du Parlement européen et du Conseil du

XXX sur la résilience des entités critiques (JO...).

Amendement 9

Proposition de directive
Considérant 10

Texte proposé par la Commission	*Amendement*
(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.	(10) La Commission, en coopération avec le groupe de coopération, ***devrait*** publier des lignes directrices concernant la mise en œuvre des critères applicables aux ***microentités*** et aux ***entités*** de petite taille.

Amendement 10

Proposition de directive
Considérant 12

Texte proposé par la Commission	*Amendement*
(12) La législation et les instruments sectoriels peuvent contribuer à garantir des niveaux élevés de cybersécurité tout en tenant pleinement compte du caractère spécifique et complexe de ces secteurs. Lorsqu'un acte juridique sectoriel de l'Union impose aux entités essentielles ou importantes d'adopter des mesures de gestion des risques en matière de cybersécurité ou de notifier des incidents ou des cybermenaces importantes et que cette obligation produit un effet au moins équivalent à celui des obligations prévues par la présente directive, il convient d'appliquer ces dispositions sectorielles, y compris en matière de surveillance et d'application. La Commission ***peut*** publier des lignes directrices relatives à la mise en œuvre de la lex specialis. La présente directive n'empêche pas l'adoption d'actes sectoriels de l'Union supplémentaires prévoyant des mesures de gestion des risques en matière de cybersécurité et la	(12) La législation et les instruments sectoriels peuvent contribuer à garantir des niveaux élevés de cybersécurité tout en tenant pleinement compte du caractère spécifique et complexe de ces secteurs. Lorsqu'un acte juridique sectoriel de l'Union impose aux entités essentielles ou importantes d'adopter des mesures de gestion des risques en matière de cybersécurité ou de notifier des incidents ou des cybermenaces importantes et que cette obligation produit un effet au moins équivalent à celui des obligations prévues par la présente directive, il convient d'appliquer ces dispositions sectorielles, y compris en matière de surveillance et d'application. La Commission ***devrait*** publier des lignes directrices relatives à la mise en œuvre de la lex specialis. La présente directive n'empêche pas l'adoption d'actes sectoriels de l'Union supplémentaires prévoyant des mesures de gestion des risques en matière de

notification des incidents. La présente directive 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.

cybersécurité et la notification des incidents. La présente directive 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.

Amendement 11

Proposition de directive
Considérant 14

Texte proposé par la Commission	*Amendement*
(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[17] 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 en vertu des deux directives devraient coopérer et échanger des informations, notamment en ce qui concerne le recensement des entités critiques, les cybermenaces, les risques en matière de cybersécurité, les incidents affectant les entités critiques ainsi que les mesures de cybersécurité adoptées par les entités critiques. Sur demande des autorités compétentes au titre de la directive (UE) XXX/XXX, les autorités	(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[17] et la présente directive***, lorsque cela est possible et approprié***. 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 ***les autorités compétentes au sein d'un même État membre et entre les autorités compétentes de différents États membres*** 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 ***informatiques*** et aux cybermenaces ainsi que de l'exercice des tâches de surveillance. Les autorités en vertu des deux directives devraient coopérer et échanger des informations ***au sein d'un même État membre et entre États membres***, notamment en ce qui concerne le recensement des entités critiques, les cybermenaces, les risques en matière de cybersécurité, les incidents

compétentes au titre de la présente directive devraient être autorisées à ***exercer leurs pouvoirs de surveillance et d'exécution sur une entité essentielle définie*** comme ***critique***. Les deux autorités devraient coopérer et échanger des informations à cette fin.

affectant les entités critiques ainsi que les mesures de cybersécurité adoptées par les ***autorités compétentes au titre de la présente directive pertinentes pour les*** entités critiques. Sur demande des autorités compétentes au titre de la directive (UE) XXX/XXX, les autorités compétentes au titre de la présente directive devraient être autorisées à ***évaluer la cybersécurité des entités essentielles définies*** comme ***critiques***. Les deux autorités devraient coopérer et échanger des informations ***en temps réel*** à cette fin.

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

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

Amendement 12

Proposition de directive
Considérant 18

Texte proposé par la Commission

Amendement

(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 centres 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

(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 ***cybersécurité***, la présente directive devrait également couvrir les fournisseurs de services de centres 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

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.

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.

Amendement 13

Proposition de directive
Considérant 20

Texte proposé par la Commission	*Amendement*
(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) 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 ***production, transformation et distribution des denrées alimentaires, 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. ***Les attaques intensifiées menées contre les systèmes d'information durant*** la pandémie de COVID-19 ***ont*** mis en évidence la vulnérabilité de nos sociétés de plus en plus interdépendantes face à des

risques peu probables. ***Par conséquent, des investissements supplémentaires dans la cybersécurité sont nécessaires.***

Amendement 14

Proposition de directive
Considérant 20 bis (nouveau)

Texte proposé par la Commission	*Amendement*
	(20 bis) Il est essentiel de renforcer la cybersensibilisation et la cyberrésilience dans toutes les entités critiques et importantes, y compris les entités de l'administration publique.

Amendement 15

Proposition de directive
Considérant 21

Texte proposé par la Commission	*Amendement*
(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.	(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 ***et veiller à ce que celle-ci dispose des ressources suffisantes pour s'acquitter de ses tâches de manière effective et efficace***.

Amendement 16

Proposition de directive
Considérant 22

Texte proposé par la Commission	*Amendement*
(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.	(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 ***cybersécurité*** et de la coopération transfrontalière au niveau de l'Union.

Amendement 17

Proposition de directive
Considérant 23

Texte proposé par la Commission	*Amendement*
(23) Les autorités compétentes ou les CSIRT devraient recevoir les notifications d'incidents provenant des entités de manière efficace et efficiente. Les points de contact uniques devraient être chargés de transmettre les notifications d'incidents aux points de contact uniques ***des*** autres États membres ***touchés***. Au niveau des autorités des États membres, afin de garantir l'existence d'un seul point d'entrée dans chaque État membre, les points de contact uniques devraient également être les destinataires des informations pertinentes portant sur les incidents concernant les entités du secteur financier fournies par les autorités compétentes au titre du règlement XXXX/XXXX, qu'ils devraient pouvoir transmettre, le cas échéant, aux autorités nationales compétentes ou aux CSIRT en vertu de la présente directive.	(23) Les autorités compétentes ou les CSIRT devraient recevoir les notifications d'incidents provenant des entités de manière efficace et efficiente. Les points de contact uniques devraient être chargés de transmettre ***en temps réel*** les notifications d'incidents aux points de contact uniques ***de tous les*** autres États membres. Au niveau des autorités des États membres, afin de garantir l'existence d'un seul point d'entrée dans chaque État membre, les points de contact uniques devraient également être les destinataires des informations pertinentes portant sur les incidents concernant les entités du secteur financier fournies par les autorités compétentes au titre du règlement XXXX/XXXX, qu'ils devraient pouvoir transmettre, le cas échéant, aux autorités nationales compétentes ou aux CSIRT en vertu de la présente directive.

Amendement 18

Proposition de directive
Considérant 25

Texte proposé par la Commission	*Amendement*
(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. 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.	(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]***et*** à ***la directive 2002/58/CE***, au nom et sur demande d'une entité en vertu de la présente directive, ***un examen de sécurité*** des systèmes d'information ***et de la zone de couverture*** utilisés pour la fourniture de leurs services***, afin d'identifier, de réduire ou de prévenir des menaces spécifiques***. 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. ***En outre, les risques en matière de cybersécurité ne devraient jamais servir de prétexte à des violations des droits fondamentaux.***
[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).	[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).

Amendement 19

Proposition de directive
Considérant 27

Texte proposé par la Commission	*Amendement*
(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.	(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 ***ou présentant de graves risques pour la sécurité publique dans plusieurs États membres ou dans l'Union dans son ensemble***. 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. ***Les États membres doivent surveiller l'application des règles de l'UE, s'entraider en cas de problème transfrontalier, établir un dialogue plus structuré avec le secteur privé et collaborer face aux risques pour la sécurité et aux menaces liées aux nouvelles technologies, comme ils l'ont fait pour la 5G.***
[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).	[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).

Amendement 20

Proposition de directive
Considérant 33

Texte proposé par la Commission	*Amendement*
(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.	(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 ***et sectorielles***, évaluer les effets produits par les éléments livrables du groupe de coopération sur les approches nationales ***et sectorielles***, 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.

Amendement 21

Proposition de directive
Considérant 34

Texte proposé par la Commission	*Amendement*
(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.	(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 ***inviter*** les organes et agences ***concernés*** de l'Union participant à la politique de cybersécurité, ***notamment Europol***, 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.

Amendement 22

Proposition de directive
Considérant 36

Texte proposé par la Commission	*Amendement*
(36) L'Union devrait, 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 et du réseau des CSIRT. ***De tels accords devraient assurer*** un ***niveau suffisant de protection des données***.	(36) L'Union devrait, 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 et du réseau des CSIRT. ***Lorsque des données à caractère personnel sont transférées à*** un ***pays tiers ou à une organisation internationale, il convient d'appliquer le chapitre V du règlement (UE) 2016/679***.

Amendement 23

Proposition de directive
Considérant 37

Texte proposé par la Commission	*Amendement*
(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 d'organisations de liaison en cas de crises de cybersécurité (UE - CyCLONe), le réseau des CSIRT et le groupe de coopération. EU-CyCLONe et le réseau des CSIRT devraient coopérer sur la base de modalités de procédure définissant les conditions de cette coopération. 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	(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 d'organisations de liaison en cas de crises de cybersécurité (UE - CyCLONe), le réseau des CSIRT et le groupe de coopération. EU-CyCLONe et le réseau des CSIRT devraient coopérer sur la base de modalités de procédure définissant les conditions de cette coopération. 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 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.

pertinents et les modèles de partage d'informations, ainsi que les moyens de communication. Pour la gestion des crises au niveau 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 ***concerne deux États membres ou plus et s'il est suspecté qu'elle est de nature criminelle, le déclenchement du protocole de réaction d'urgence des services répressifs de l'Union devrait être envisagé. 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.

Amendement 24

Proposition de directive
Considérant 45

Texte proposé par la Commission	*Amendement*
(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	(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.	toutes les mesures de cybersécurité appropriées lorsqu'elles ont recours à des services de transformation et d'analyse des données fournis par des tiers ***et signaler toute cyberattaque éventuelle identifiée***.

Amendement 25

Proposition de directive
Considérant 46 bis (nouveau)

Texte proposé par la Commission	*Amendement*
	(46 bis) Il convient de tenir particulièrement compte du fait que les services, systèmes ou produits TIC soumis à des exigences spécifiques dans le pays d'origine pourraient représenter un obstacle à la conformité avec le droit de l'Union en matière de protection de la vie privée et des données à caractère personnel. Le cas échéant, le comité européen de la protection des données devrait être consulté dans le cadre de ces évaluations des risques. Les logiciels libres et open source ainsi que les matériels open source pourraient apporter des avantages considérables en matière de cybersécurité, notamment en ce qui concerne la transparence et la nature vérifiable des caractéristiques. Dans la mesure où cela pourrait contribuer à aborder et à atténuer les risques liés aux chaînes d'approvisionnement, leur utilisation devrait être privilégiée dans la mesure du possible, conformément à l'avis 5/2021 du CEPD[1 bis].
	[1 bis] ***Avis 5/2021 du Contrôleur européen de la protection des données concernant les stratégies de cybersécurité et la directive SRI 2.0 du 11 mars 2021***.

Amendement 26

Proposition de directive
Considérant 47

Texte proposé par la Commission	*Amendement*
(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.	(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 que le groupe de coopération devrait détailler davantage***, ***qui comprennent*** 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.

Amendement 27

Proposition de directive
Considérant 48 bis (nouveau)

Texte proposé par la Commission	*Amendement*
	(48 bis) Les petites et moyennes entreprises, souvent, ne disposent ni de l'échelle ni des ressources nécessaires pour répondre à une gamme de besoins élargie et croissante en matière de cybersécurité dans un monde interconnecté où le travail à distance ne cesse de croître. Les États membres devraient par conséquent aborder l'orientation et le soutien à apporter aux petites et moyennes entreprises dans le cadre de leurs stratégies nationales de cybersécurité.

Amendement 28

Proposition de directive
Considérant 50

Texte proposé par la Commission	*Amendement*
(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	(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 ***cybersécurité*** 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.

contrôle effectif sur la transmission de signaux.

Amendement 29

Proposition de directive
Considérant 52

Texte proposé par la Commission	*Amendement*
(52) Lorsque cela est approprié, les entités devraient informer les destinataires de leurs services des menaces importantes et considérables, ainsi que des mesures qu'ils peuvent prendre pour atténuer le risque qui en résulte pour eux. 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 menaces pour la sécurité devrait être gratuit.	(52) Lorsque cela est approprié, les entités devraient ***pouvoir*** informer les destinataires de leurs services des menaces importantes et considérables, ainsi que des mesures qu'ils peuvent prendre pour atténuer le risque qui en résulte pour eux. 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 menaces pour la sécurité devrait être gratuit.

Amendement 30

Proposition de directive
Considérant 53

Texte proposé par la Commission	*Amendement*
(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***.	(53) Plus particulièrement, il convient que les fournisseurs de réseaux de communications électroniques publics ou de services de communications électroniques accessibles au public ***mettent en œuvre des mesures de sécurité dès la conception et par défaut, et soient en mesure d'informer*** les destinataires des services des cybermenaces particulières et importantes pour la sécurité et des mesures ***supplémentaires*** qu'ils peuvent prendre pour sécuriser leurs ***appareils et*** communications, par exemple en recourant à des types spécifiques de logiciels ou de

techniques de ***cryptage. Afin d'accroître la sécurité des logiciels et des matériels, il convient d'encourager les fournisseurs à recourir aux matériels open source et ouverts.***

Amendement 31

Proposition de directive
Considérant 54

Texte proposé par la Commission	*Amendement*
(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***.	(54) Afin de préserver la sécurité des réseaux et services de communications électroniques ***ainsi que les droits fondamentaux à la protection des données et au respect de la vie privée***, 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 ***la responsabilité des*** États membres ***de*** garantir la protection de leurs intérêts essentiels de sécurité et de la sécurité publique et ***de*** permettre la ***prévention et la*** détection d'infractions pénales et les enquêtes et poursuites en la matière, dans le respect du droit ***national et*** 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***. Aucune disposition du présent règlement ne saurait être interprétée comme constituant un effort visant à affaiblir le du chiffrement bout en bout, que ce soit par l'intermédiaire d'«accès dérobés» ou d'autres solutions, étant donné que les lacunes en matière de chiffrement peuvent être exploitées à des***

fins malveillantes. Toute mesure visant à affaiblir le chiffrement ou à contourner l'architecture de la ***technologie peut présenter des risques importants pour les capacités de protection efficaces qui sont en jeu. Le décryptage non autorisé ou la surveillance des communications électroniques en dehors d'autorités légales doivent être interdits pour garantir l'efficacité de la technologie et de son utilisation plus large. Il importe que les États membres s'attaquent aux problèmes rencontrés par les autorités judiciaires et les experts qui recherchent les vulnérabilités. Dans certains États membres, les entités et les personnes physiques qui recherchent les vulnérabilités sont soumises à la responsabilité pénale et civile. Les États membres sont donc encouragés à établir des lignes directrices relatives à l'absence de poursuites et l'absence de responsabilité en matière de recherche sur la sécurité de l'information.***

Amendement 32

Proposition de directive
Considérant 56

Texte proposé par la Commission	*Amendement*
(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 devraient mettre en place un point d'entrée unique ***pour toutes les notifications requises*** en	(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 devraient mettre en place un point d'entrée unique ***requis*** en vertu de la présente directive et

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.

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 ***et le comité européen de la protection des données***, 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.

Amendement 33

Proposition de directive
Considérant 57

Texte proposé par la Commission	*Amendement*
(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.	(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 ***Centre européen de lutte contre la cybercriminalité (***CE3***) d'Europol*** et l'ENISA.

Amendement 34

Proposition de directive
Considérant 58

Texte proposé par la Commission	*Amendement*
(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.	(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 ***au règlement (UE) 2016/679 et*** à la directive 2002/58/CE.

Amendement 35

Proposition de directive
Considérant 59

Texte proposé par la Commission	*Amendement*
(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.	(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 ***applicable*** en matière de protection des données.

Amendement 36

Proposition de directive
Considérant 62

Texte proposé par la Commission	*Amendement*
(62) ***Les*** registres des noms de domaines de premier niveau ainsi que les entités leur	(62) ***Pour se conformer à une obligation légale en vertu de l'article 6,***

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***. 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. 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

paragraphe 1, point c), et de l'article 6, paragraphe 3, du règlement (UE) 2016/679, 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 ***certaines*** données relatives à l'enregistrement de noms de domaines ***spécifiées dans le droit de l'État membre auquel ils sont soumis, telles que le nom de domaine et le nom de la personne morale***. 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***, notamment aux autorités compétentes au titre de la présente directive ou aux autorités*** de ***contrôle au titre du règlement (UE) 2016/679***conformément à ***leurs compétences, d'accéder légalement à des données spécifiques d'enregistrement de noms de domaines***. 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 ***légales et dûment justifiées émanant des autorités publiques, y compris les autorités compétentes au titre de la présente directive, 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, ou les autorités*** de ***contrôle au titre du règlement (UE) 2016/679, en vue de la divulgation de données d'enregistrement de noms de domaines***. 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

européen de la protection 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. 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.

_____ _____

[25] RÈGLEMENT (UE) 2016/679 DU PARLEMENT EUROPÉEN ET DU CONSEIL, considérant 14, aux termes duquel «Le 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».

Amendement 37

Proposition de directive
Considérant 63

Texte proposé par la Commission	*Amendement*
(63) ***Toutes*** les entités essentielles et importantes au sens de la présente directive devraient relever de la juridiction de l'État membre dans lequel elles fournissent leurs services. Si l'entité fournit des services 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	(63) ***Aux fins de la présente directive, toutes*** les entités essentielles et importantes au sens de la présente directive devraient relever de la juridiction de l'État membre dans lequel elles fournissent leurs services. Si l'entité fournit des services 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 ***se mettre d'accord sur les classifications constitutives,*** coopérer ***dans toute la mesure du possible***, se prêter

surveillance.	mutuellement assistance ***en temps réel*** et, le cas échéant, mener des actions communes de surveillance.

Amendement 38

Proposition de directive
Considérant 64

Texte proposé par la Commission	*Amendement*
(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 fournisseurs de réseaux de diffusion de contenu, des fournisseurs de services d'informatique en nuage, des fournisseurs de services de centres 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 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 ces décisions ne sont pas	(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 fournisseurs de réseaux de diffusion de contenu, des fournisseurs de services d'informatique en nuage, des fournisseurs de services de centres de données et des fournisseurs de service numérique, un seul État membre devrait avoir compétence eu égard à ces entités. ***Aux fins de la présente directive,*** 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 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

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.

dans l'Union. 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.

Amendement 39

Proposition de directive
Considérant 69

Texte proposé par la Commission	*Amendement*
(69) Le traitement de données à caractère personnel, dans la mesure strictement nécessaire et proportionnée aux fins de garantir la sécurité du réseau et des informations par des entités, des autorités publiques, des CERT, des CSIRT et des fournisseurs de technologies et de services de sécurité devrait constituer un intérêt légitime du responsable du traitement concerné, tel que visé ***dans le*** règlement (UE) 2016/679. Cela devrait 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 ***des types*** de données à caractère personnel ***suivants:*** Adresses IP, localisateurs de ressources uniformes (URL), noms de domaines et	(69) Le traitement de données à caractère personnel, dans la mesure strictement nécessaire et proportionnée aux fins de garantir la sécurité du réseau et des informations par des entités, des autorités publiques, des CERT, des CSIRT et des fournisseurs de technologies et de services de sécurité ***est nécessaire au respect des obligations légales qui leur incombent en vertu du droit national transposant la présente directive et est donc couvert par l'article 6, paragraphe 1, point c), et l'article 6, paragraphe 3, du règlement (UE) 2016/679. En outre, ce traitement*** devrait constituer un intérêt légitime du responsable du traitement concerné, tel que visé ***à l'article 6, paragraphe 1, point f), du*** règlement (UE)2016/679. Cela devrait 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

adresses électroniques.	de compromis, les tactiques, techniques et procédures, les alertes de cybersécurité et les outils de configuration. ***Dans de nombreux cas, des données à caractère personnel sont compromises à la suite d'incidents de cybersécurité, c'est pourquoi les autorités compétentes et les autorités chargées de la protection des données dans les États membres de l'UE devraient coopérer et échanger des informations sur tous les aspects pertinents pour traiter n'importe quel cas de violation de la sécurité des données à caractère personnel.*** Ces mesures peuvent nécessiter le traitement ***de certaines catégories*** de données à caractère personnel***, notamment les*** adresses IP, ***les*** localisateurs de ressources uniformes (URL), ***les*** noms de domaines et ***les*** adresses électroniques.

Amendement 40

Proposition de directive
Considérant 71

Texte proposé par la Commission	*Amendement*
(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	(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 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***, de toute infraction antérieure pertinente, de la manière dont l'infraction a été portée à la connaissance de l'autorité compétente***, du caractère intentionnel ou négligent de la violation, des mesures prises pour prévenir ou atténuer les dommages et/ou pertes subis, du degré de

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.

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.

Amendement 41

Proposition de directive
Considérant 74

Texte proposé par la Commission	*Amendement*
(74) Les États membres devraient pouvoir 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.	(74) Les États membres devraient pouvoir déterminer le régime des sanctions pénales applicables en cas de violations des dispositions nationales transposant la présente directive. ***Ces sanctions pénales peuvent aussi permettre la saisie des profits réalisés en violation du présent règlement.*** 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.

Amendement 42

Proposition de directive
Considérant 76

Texte proposé par la Commission	*Amendement*
(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,	(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.	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. 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 ***l'accès*** à ***des voies de recours juridictionnel effectives***, une procédure régulière, la présomption d'innocence et les droits de la défense.

Amendement 43

Proposition de directive
Considérant 77

Texte proposé par la Commission	*Amendement*
(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.	(77) La présente directive devrait établir des règles de coopération entre les autorités compétentes ***au titre de la présente directive*** et les autorités de contrôle ***au titre du*** règlement (UE) 2016/679 pour traiter les violations relatives aux données à caractère personnel.

Amendement 44

Proposition de directive
Considérant 79

Texte proposé par la Commission	*Amendement*
(79) Un mécanisme d'évaluation par les pairs devrait être mis en place, permettant l'évaluation par des experts désignés par les États membres de la mise en œuvre des politiques de cybersécurité, y compris le niveau des capacités et des ressources disponibles des États membres.	(79) Un mécanisme d'évaluation par les pairs devrait être mis en place, permettant l'évaluation par des experts désignés par les États membres de la mise en œuvre des politiques de cybersécurité, y compris le niveau des capacités et des ressources disponibles des États membres. ***L'UE devrait faciliter une réponse coordonnée aux incidents et aux crises de cybersécurité de grande ampleur, tout en apportant une aide à la reprise aux victimes de telles cyberattaques.***

Amendement 45

Proposition de directive
Considérant 82 bis (nouveau)

Texte proposé par la Commission	*Amendement*
	(82 bis) La présente directive ne s'applique pas aux institutions, organes et organismes de l'Union. Toutefois, les organes de l'Union devraient être considérés comme des entités essentielles ou importantes dans le cadre de la présente directive. Afin d'atteindre un niveau uniforme de protection grâce à des

règles cohérentes et homogènes, la Commission devrait publier une proposition législative visant à inclure les institutions, organes et organismes de l'Union dans le cadre de cybersécurité à l'échelle de l'UE au plus tard le 31 décembre 2022.

Amendement 46

Proposition de directive
Considérant 84

Texte proposé par la Commission	*Amendement*
(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,	(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, ***et dans le respect intégral de la législation existante de l'Union régissant ces questions. Tout traitement de données à caractère personnel en vertu de la présente directive est soumis au règlement (UE) 2016/679 et à la directive 2002/58/CE, dans leur champ d'application respectif, y compris les tâches et les pouvoirs des autorités de contrôle compétentes pour surveiller le respect de ces instruments juridiques.***

Amendement 47

Proposition de directive
Article 2 – paragraphe 1

Texte proposé par la Commission	*Amendement*
1. La présente directive s'applique	1. La présente directive s'applique

aux entités publiques et privées d'un type appelé «entités essentielles» à l'annexe I et «entités importantes» à l'annexe II. La présente directive ne s'applique pas aux entités qui peuvent être qualifiées de microentreprises et de petites entreprises au sens de la recommandation 2003/361/CE de la Commission[28].	aux entités publiques et privées d'un type appelé «entités essentielles» à l'annexe I et «entités importantes» à l'annexe II. La présente directive ne s'applique pas aux entités qui peuvent être qualifiées de microentreprises et de petites entreprises au sens de la recommandation 2003/361/CE de la Commission[28]. ***L'article 3, paragraphe 4, de l'annexe de la recommandation 2003/361/CE de la Commission n'est pas applicable.***
[28] 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).	[28] 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).

Amendement 48

Proposition de directive
Article 2 – paragraphe 2 – partie introductive

Texte proposé par la Commission	*Amendement*
2. Toutefois, quelle que soit leur taille, la présente directive s'applique également aux entités visées aux annexes I et II, dans les cas suivants:	2. Toutefois, quelle que soit leur taille, ***et sur la base d'une évaluation des risques réalisée conformément à l'article 18,*** la présente directive s'applique également aux entités visées aux annexes I et II, dans les cas suivants:

Amendement 49

Proposition de directive
Article 2 – paragraphe 2 – point c

Texte proposé par la Commission	*Amendement*
c) l'entité est le seul prestataire de services ***dans un État membre***;	c) l'entité est le seul prestataire de services ***au niveau national ou régional***;

Amendement 50

Proposition de directive
Article 2 – paragraphe 2 – point d

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

Amendement 51

Proposition de directive
Article 2 – paragraphe 2 – point e

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

Amendement 52

Proposition de directive
Article 2 – paragraphe 4 bis (nouveau)

Texte proposé par la Commission	*Amendement*
	4 bis. Tout traitement de données à caractère personnel en vertu de la présente directive est conforme au règlement (UE) 2016/679 et à la directive 2002/58/CE et est limité à ce qui est strictement nécessaire et proportionné aux fins de la présente directive.

Amendement 53

Proposition de directive
Article 2 – paragraphe 5

Texte proposé par la Commission	*Amendement*
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,	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 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.	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 que si cet échange est nécessaire à l'application de la présente directive. Les informations échangées se limitent au minimum nécessaire 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.

Amendement 54

Proposition de directive
Article 2 – paragraphe 6 bis (nouveau)

Texte proposé par la Commission	*Amendement*
	6 bis. Au plus tard le 31 décembre 2021, la Commission publie une proposition législative visant à inclure les institutions, organes et organismes de l'Union dans le cadre global de l'Union en matière de cybersécurité, dans le but de parvenir à un niveau de protection uniforme à l'aide de règles cohérentes et homogènes.

Amendement 55

Proposition de directive
Article 4 – alinéa 1 – point 1 – sous-point b

Texte proposé par la Commission	*Amendement*
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;	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***, et qui sont intégrés dans le système informatique et utilisés pour la fourniture des services auxquels ils sont destinés***;

Amendement 56

Proposition de directive
Article 4 – alinéa 1 – point 4

Texte proposé par la Commission	*Amendement*
4) «stratégie nationale en matière de cybersécurité», le cadre cohérent d'un État membre fournissant des objectifs et des priorités stratégiques en matière de ***sécurité des réseaux et des systèmes d'information*** dans cet État membre;	4) «stratégie nationale en matière de cybersécurité», le cadre cohérent d'un État membre fournissant des objectifs et des priorités stratégiques en matière de ***cybersécurité*** dans cet État membre;

Amendement 57

Proposition de directive
Article 4 – alinéa 1 – point 12

Texte proposé par la Commission	*Amendement*
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;	***supprimé***

Amendement 58

Proposition de directive
Article 4 – alinéa 1 – point 22

Texte proposé par la Commission	*Amendement*
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,	***supprimé***

publications, vidéos et recommandations);

Amendement 59

Proposition de directive
Article 4 – alinéa 1 – point 24

Texte proposé par la Commission	*Amendement*
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;	24) «entité», toute personne physique ou ***toute personne*** 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;

Amendement 60

Proposition de directive
Article 5 – paragraphe 1 – point a

Texte proposé par la Commission	*Amendement*
a) une définition des objectifs et des priorités de la stratégie des États membres en matière de cybersécurité;	a) une définition des objectifs et des priorités de la stratégie des États membres en matière de cybersécurité***, tenant compte du niveau général de sensibilisation des citoyens à la cybersécurité ainsi que du niveau général de sécurité des appareils connectés des consommateurs***;

Amendement 61

Proposition de directive
Article 5 – paragraphe 1 – point f

Texte proposé par la Commission	*Amendement*
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	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 incidents et les cybermenaces et de l'exercice des tâches de contrôle.	critiques]***, dans et entre les États membres,*** aux fins du partage d'informations sur les incidents et les cybermenaces et de l'exercice des tâches de contrôle.
[38] [insérer le titre complet et la référence de la publication au JO lorsqu'ils seront connus]	[38] [insérer le titre complet et la référence de la publication au JO lorsqu'ils seront connus]

Amendement 62

Proposition de directive
Article 5 – paragraphe 2 – point b

Texte proposé par la Commission	*Amendement*
b) des lignes directrices concernant l'inclusion et la spécification d'exigences liées à la cybersécurité pour les produits et services TIC dans les marchés publics;	b) des lignes directrices concernant l'inclusion et la spécification d'exigences liées à la cybersécurité pour les produits et services TIC dans les marchés publics***, y compris, mais sans s'y limiter, les exigences en matière de cryptage et la promotion de l'utilisation de produits de cybersécurité open source***;

Amendement 63

Proposition de directive
Article 5 – paragraphe 2 – point d bis (nouveau)

Texte proposé par la Commission	*Amendement*
	d bis) une politique visant à soutenir l'utilisation de données ouvertes et open source dans le cadre de la sécurité par la transparence;

Amendement 64

Proposition de directive
Article 5 – paragraphe 2 – point d ter (nouveau)

Texte proposé par la Commission	*Amendement*
	d ter) une politique visant à promouvoir la protection et la sécurité des données à caractère personnel des utilisateurs des

services en ligne;

Amendement 65

Proposition de directive
Article 5 – paragraphe 2 – point e

Texte proposé par la Commission	*Amendement*
e) une politique de promotion et de développement des compétences en matière de cybersécurité, de sensibilisation et d'initiatives de recherche et développement;	e) une politique de promotion et de développement des compétences en matière de cybersécurité, de sensibilisation et d'initiatives de recherche et développement***, y compris l'élaboration de programmes de formation sur la cybersécurité afin de fournir aux entités des spécialistes et des techniciens***;

Amendement 66

Proposition de directive
Article 5 – paragraphe 2 – point f

Texte proposé par la Commission	*Amendement*
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***;	f) une politique de soutien aux institutions universitaires et de recherche ***qui contribuent*** à ***la stratégie nationale de cybersécurité en élaborant et en déployant*** des outils de cybersécurité et ***des infrastructures de réseau sécurisées qui contribuent*** à ***la stratégie nationale de cybersécurité, y compris des politiques spécifiques traitant des questions liées à la représentation et à l'équilibre entre les hommes et*** les ***femmes dans ce secteur***;

Amendement 67

Proposition de directive
Article 5 – paragraphe 2 – point h

Texte proposé par la Commission	*Amendement*
h) une politique répondant aux besoins	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 menaces de cybersécurité.	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 menaces de cybersécurité ***et leur capacité à réagir aux incidents de cybersécurité***.

Amendement 68

Proposition de directive
Article 6 – paragraphe 2

Texte proposé par la Commission	*Amendement*
2. L'ENISA élabore et tient à jour un registre européen des vulnérabilités. 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 les vulnérabilités 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 adressées aux utilisateurs de produits et services vulnérables sur la manière dont les risques résultant des vulnérabilités divulguées peuvent être atténués.	2. L'ENISA élabore et tient à jour un registre européen des vulnérabilités. 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 les vulnérabilités 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 adressées aux utilisateurs de produits et services vulnérables sur la manière dont les risques résultant des vulnérabilités divulguées peuvent être atténués. ***Afin de garantir la sécurité et l'accessibilité des informations contenues dans le registre, l'ENISA applique les mesures de sécurité les plus récentes et met les informations à disposition dans des formats lisibles par machine au moyen d'interfaces***

correspondantes.

Amendement 69

Proposition de directive
Article 7 – paragraphe 3 – point a

Texte proposé par la Commission	*Amendement*
a) les objectifs des mesures et activités nationales de préparation;	a) les objectifs des mesures et activités nationales ***et, le cas échéant, régionales et transfrontalières*** de préparation;

Amendement 70

Proposition de directive
Article 10 – paragraphe 2 – point e

Texte proposé par la Commission	*Amendement*
e) la réalisation, à la demande d'une entité, d'un ***scannage proactif du réseau et*** des systèmes d'information utilisés pour la fourniture de leurs services;	e) la réalisation, à la demande d'une entité, d'un ***examen de sécurité*** des systèmes d'information ***et de la zone de couverture*** utilisés pour la fourniture de leurs services ***afin d'identifier, de réduire ou de prévenir des menaces spécifiques; le traitement des données à caractère personnel dans le cadre de ce scannage est limité à ce qui est strictement nécessaire et, dans tous les cas, aux adresses IP et aux URL;***

Amendement 71

Proposition de directive
Article 11 – paragraphe 4

Texte proposé par la Commission	*Amendement*
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 et les points de contact	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 et les points de contact

uniques et les services répressifs, les autorités chargées de la protection des données et les autorités responsables des infrastructures critiques en vertu de la directive (UE) XXXX/XXXX [directive sur la résilience des entités critiques] et les autorités financières nationales désignées conformément au règlement (UE) XXXX/XXXX du Parlement européen et du Conseil[39] [le règlement sur la résilience opérationnelle numérique du secteur financier] dans cet État membre.	uniques et les services répressifs, les autorités chargées de la protection des données et les autorités responsables des infrastructures critiques en vertu de la directive (UE) XXXX/XXXX [directive sur la résilience des entités critiques] et les autorités financières nationales désignées conformément au règlement (UE) XXXX/XXXX du Parlement européen et du Conseil[39] [le règlement sur la résilience opérationnelle numérique du secteur financier] dans cet État membre***, conformément à leurs compétences respectives***.
[39] [insérer le titre complet et la référence de la publication au JO lorsqu'ils seront connus]	[39] [insérer le titre complet et la référence de la publication au JO lorsqu'ils seront connus]

Amendement 72

Proposition de directive
Article 11 – paragraphe 5

Texte proposé par la Commission	*Amendement*
5. Les États membres veillent à ce que leurs autorités compétentes fournissent régulièrement des informations aux autorités compétentes désignées en vertu de la directive (UE) XXXX/XXXX [directive sur la résilience des entités critiques] eu égard aux risques en matière de cybersécurité, aux cybermenaces et aux incidents 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 qu'eu égard aux mesures prises par les autorités compétentes en réponse à ces risques et incidents.	5. Les États membres veillent à ce que leurs autorités compétentes fournissent régulièrement***, en temps utile,*** des informations aux autorités compétentes désignées en vertu de la directive (UE) XXXX/XXXX [directive sur la résilience des entités critiques] eu égard aux risques en matière de cybersécurité, aux cybermenaces et aux incidents 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 qu'eu égard aux mesures prises par les autorités compétentes en réponse à ces risques et incidents.

Amendement 73

Proposition de directive
Article 12 – paragraphe 3 – partie introductive

Texte proposé par la Commission	*Amendement*
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), conformément à l'article 17, paragraphe 5, point c), du règlement (UE) XXXX/XXXX [le règlement sur la résilience opérationnelle numérique du secteur financier], peuvent participer aux activités du groupe de coopération.	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***, le Centre européen de lutte contre la cybercriminalité à Europol et le comité européen de la protection des données participent*** aux activités du groupe de coopération en qualité ***d'observateurs***. Les autorités européennes de surveillance (AES), conformément à l'article 17, paragraphe 5, point c), du règlement (UE) XXXX/XXXX [le règlement sur la résilience opérationnelle numérique du secteur financier], peuvent participer aux activités du groupe de coopération.

Amendement 74

Proposition de directive
Article 12 – paragraphe 3 – alinéa 1

Texte proposé par la Commission	*Amendement*
Si besoin est, le groupe de coopération ***peut inviter*** des représentants des acteurs concernés à participer à ses travaux.	***Lorsque cela*** est ***nécessaire à l'accomplissement de ses tâches***, le groupe de coopération ***invite*** des représentants des acteurs concernés à participer à ses travaux ***et le Parlement européen à participer en qualité d'observateur***.

Amendement 75

Proposition de directive
Article 12 – paragraphe 8

Texte proposé par la Commission	*Amendement*
8. Le groupe de coopération se réunit	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 l'échange d'informations.	régulièrement et au moins ***deux*** 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 ***faciliter*** la coopération stratégique et l'échange d'informations ***en temps réel***.

Amendement 76

Proposition de directive
Article 13 – paragraphe 2

Texte proposé par la Commission	*Amendement*
2. Le réseau des CSIRT est composé de représentants des CSIRT des États membres 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.	2. Le réseau des CSIRT est composé de représentants des CSIRT des États membres et du CERT-UE. La Commission ***et le Centre européen de lutte contre la cybercriminalité d'Europol participent*** au réseau des CSIRT en qualité ***d'observateurs***. L'ENISA assure le secrétariat et soutient activement la coopération entre les CSIRT.

Amendement 77

Proposition de directive
Article 14 – paragraphe 2

Texte proposé par la Commission	*Amendement*
2. Le réseau UE-CyCLONe est composé des représentants de la Commission, de l'ENISA et des autorités des États membres chargées de la gestion des crises désignées conformément à l'article 7. L'ENISA assure le secrétariat du réseau et soutient l'échange sécurisé d'informations.	2. Le réseau UE-CyCLONe est composé des représentants de la Commission, de l'ENISA et des autorités des États membres chargées de la gestion des crises désignées conformément à l'article 7. ***Le Centre européen de lutte contre la cybercriminalité d'Europol participe aux activités du réseau UE-CyCLONe en qualité d'observateur.*** L'ENISA assure le secrétariat du réseau et soutient l'échange sécurisé d'informations.

Amendement 78

Proposition de directive
Article 14 – paragraphe 6

Texte proposé par la Commission	*Amendement*
6. EU-CyCLONe coopère avec le réseau des CSIRT sur la base des modalités procédurales convenues.	6. EU-CyCLONe coopère avec le réseau des CSIRT sur la base des modalités procédurales convenues***, et avec les services répressifs dans le cadre du protocole de réaction d'urgence des services répressifs de l'Union***.

Amendement 79

Proposition de directive
Article 15 – paragraphe 1 – partie introductive

Texte proposé par la Commission	*Amendement*
1. L'ENISA publie, en coopération avec la Commission, un rapport ***bisannuel*** sur l'état de la cybersécurité dans l'Union. Le rapport comporte notamment une évaluation des éléments suivants:	1. L'ENISA publie, en coopération avec la Commission, un rapport ***annuel*** sur l'état de la cybersécurité dans l'Union. Le rapport ***est publié dans un format lisible par machine et*** comporte notamment une évaluation des éléments suivants:

Amendement 80

Proposition de directive
Article 15 – paragraphe 1 – point c bis (nouveau)

Texte proposé par la Commission	*Amendement*
	c bis) l'incidence des incidents de cybersécurité sur la protection des données à caractère personnel dans l'Union.

Amendement 81

Proposition de directive
Article 15 – paragraphe 1 – point d ter (nouveau)

Texte proposé par la Commission	*Amendement*
	c ter) une vue d'ensemble du niveau général de sensibilisation à la cybersécurité et d'utilisation des technologies de cybersécurité parmi les

	citoyens, ainsi que du niveau général de sécurité des dispositifs connectés orientés vers le consommateur mis sur le marché au sein de l'Union.

Amendement 82

Proposition de directive
Article 17 – paragraphe 2

Texte proposé par la Commission	*Amendement*
2. Les États membres veillent à ce que les membres de l'organe de direction suivent régulièrement des formations spécifiques 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.	2. Les États membres veillent à ce que les membres de l'organe de direction ***et les spécialistes chargés de la cybersécurité*** suivent régulièrement des formations spécifiques afin d'acquérir des connaissances et des compétences suffisantes pour appréhender et évaluer ***l'évolution des*** risques et ***des*** pratiques de gestion en matière de cybersécurité et leur incidence sur les activités de l'entité.

Amendement 83

Proposition de directive
Article 18 – paragraphe 1

Texte proposé par la Commission	*Amendement*
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.	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 ***cybersécurité*** des réseaux et des systèmes d'information ***utilisés*** dans le cadre de la fourniture de leurs services***, pour assurer la continuité de ces services et pour réduire les risques qui se posent pour les droits des personnes lors du traitement de leurs données à caractère personnel***. Ces mesures garantissent, pour les réseaux et les systèmes d'information, un niveau de ***cybersécurité*** adapté au risque existant, compte tenu de l'état des

connaissances.

Amendement 84

Proposition de directive
Article 18 – paragraphe 2 – point g

Texte proposé par la Commission	*Amendement*
g) l'utilisation de la cryptographie et du cryptage.	g) l'utilisation de la cryptographie et du cryptage ***renforcé***.

Amendement 85

Proposition de directive
Article 18 – paragraphe 3

Texte proposé par la Commission	*Amendement*
3. Les États membres veillent à ce que, lorsqu'elles envisagent de prendre les mesures appropriées visées au paragraphe 2, point d), les entités tiennent compte des vulnérabilités propres à chaque fournisseur et prestataire de services et de 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.	3. Les États membres veillent à ce que, lorsqu'elles envisagent de prendre les mesures appropriées ***et proportionnées*** visées au paragraphe 2, point d), les entités tiennent compte des vulnérabilités propres à chaque fournisseur et prestataire de services et de 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 autorités compétentes fournissent des orientations aux entités sur l'application pratique et proportionnée.***

Amendement 86

Proposition de directive
Article 18 – paragraphe 6 bis (nouveau)

Texte proposé par la Commission	*Amendement*
	6 bis. Les États membres confèrent à l'utilisateur d'un réseau et d'un système d'information fournis par une entité essentielle ou importante le droit d'obtenir de la part de celle-ci des informations concernant les mesures techniques et organisationnelles qui ont été mises en

place pour gérer les risques qui menacent la sécurité du réseau et des systèmes d'information. Les États membres définissent les limitations à ce droit.

Amendement 87

Proposition de directive
Article 19 – paragraphe 1

Texte proposé par la Commission	*Amendement*
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.	1. Le groupe de coopération, en coopération avec la Commission et l'ENISA, ***procède*** 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.

Amendement 88

Proposition de directive
Article 20 – paragraphe 1

Texte proposé par la Commission	*Amendement*
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 les 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.	1. Les États membres veillent à ce que les entités essentielles et importantes notifient dans les meilleurs délais***, et en tout cas dans les 24 heures,*** aux autorités compétentes ou au CSIRT conformément aux paragraphes 3 et 4 tout incident ayant une incidence significative sur la fourniture de leurs services***, et informent les autorités répressives dans*** le cas ***où l'incident est de nature malveillante suspectée ou avérée.*** Ces entités notifient dans les meilleurs délais***, et en tout cas dans les 24 heures,*** aux destinataires de leurs services les incidents susceptibles de nuire à la fourniture de ces services ***et donnent des informations pouvant leur permettre d'atténuer les effets néfastes des***

	cyberattaques. À titre exceptionnel, lorsqu'une information publique pourrait déclencher de nouvelles cyberattaques, ces entités peuvent retarder la notification. 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.

Amendement 89

Proposition de directive
Article 20 – paragraphe 2 – partie introductive

Texte proposé par la Commission	*Amendement*
2. Les États membres veillent à ce que les entités essentielles et importantes ***notifient dans les meilleurs délais*** aux autorités compétentes ou au CSIRT toute cybermenace importante que ces entités décèlent et qui aurait pu entraîner un incident significatif.	2. Les États membres veillent à ce que les entités essentielles et importantes ***soient en mesure de notifier*** aux autorités compétentes ou au CSIRT toute cybermenace importante que ces entités décèlent et qui aurait pu entraîner un incident significatif.

Amendement 90

Proposition de directive
Article 20 – paragraphe 2 – alinéa 1

Texte proposé par la Commission	*Amendement*
Le cas échéant, ces entités ***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. La notification n'accroît pas la responsabilité de l'entité qui en est à l'origine.	Le cas échéant, ces entités ***sont autorisées à notifier*** aux destinataires de leurs services qui ***peuvent être*** affectés par une cybermenace importante toutes les mesures ou corrections que ces destinataires peuvent appliquer en réponse à cette menace. ***Lorsque cette notification est effectuée***, les entités informent également leurs destinataires de la menace elle-même. La notification n'accroît pas la responsabilité de l'entité qui en est à l'origine.

Amendement 91

Proposition de directive
Article 20 – paragraphe 4 – point c – partie introductive

Texte proposé par la Commission	*Amendement*
c) un rapport ***final*** au plus tard un mois après la présentation du rapport visé au point a), comprenant au moins les éléments suivants:	c) un rapport ***complet*** au plus tard un mois après la présentation du rapport visé au point a), comprenant au moins les éléments suivants:

Amendement 92

Proposition de directive
Article 20 – paragraphe 4 – point c – sous-point ii

Texte proposé par la Commission	*Amendement*
ii) le type de ***menace*** ou la cause profonde qui a probablement déclenché l'incident;	ii) le type de ***cybermenace*** ou la cause profonde qui a probablement déclenché l'incident;

Amendement 93

Proposition de directive
Article 20 – paragraphe 4 – point c – sous-point iii

Texte proposé par la Commission	*Amendement*
iii) les mesures d'atténuation appliquées et en cours.	iii) les mesures d'atténuation ***ou de correction*** appliquées et en cours.

Amendement 94

Proposition de directive
Article 20 – paragraphe 6

Texte proposé par la Commission	*Amendement*
6. Lorsque c'est approprié, et notamment si l'incident visé au paragraphe 1 concerne deux États membres ou plus, l'autorité compétente ou le CSIRT informe les autres États membres touchés et l'ENISA de l'incident. Ce faisant, les	6. Lorsque c'est approprié, et notamment si l'incident visé au paragraphe 1 concerne deux États membres ou plus, l'autorité compétente ou le CSIRT informe les autres États membres touchés et l'ENISA de l'incident. ***Si l'incident***

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.

concerne deux États membres ou plus et s'il est suspecté qu'il est de nature criminelle, l'autorité compétente ou le CSIRT informe Europol. 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.

Amendement 95

Proposition de directive
Article 22 – paragraphe 2

Texte proposé par la Commission	*Amendement*
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.	2. ***Après avoir consulté le comité européen de la protection des données, 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.

Amendement 96

Proposition de directive
Article 23 – paragraphe 1

Texte proposé par la Commission	*Amendement*
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***	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 ***mettent en place*** des ***politiques et des procédures*** pour ***assurer la collecte et le maintien des*** données d'enregistrement 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, sous réserve du*** droit de l'Union en matière de protection des données à caractère personnel.	noms de domaines exactes et complètes au sein d'une base de données dédiée ***conformément au*** droit de l'Union en matière de protection des données à caractère personnel. ***Les États membres veillent à ce que ces politiques et procédures soient mises à la disposition du public.***

Amendement 97

Proposition de directive
Article 23 – paragraphe 2

Texte proposé par la Commission	*Amendement*
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.	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 ***les*** informations ***nécessaires*** pour identifier et contacter les titulaires des noms de domaines***, à savoir leur nom, leur adresse physique et de courrier électronique, ainsi que leur numéro de téléphone,*** et les points de contact qui gèrent les noms de domaines dans les registres des noms de domaines de premier niveau.

Amendement 98

Proposition de directive
Article 23 – paragraphe 3

Texte proposé par la Commission	*Amendement*
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	***supprimé***

mises à la disposition du public.

Justification

Ce paragraphe est intégré à l'article 23, paragraphe 1.

Amendement 99

Proposition de directive
Article 23 – paragraphe 4

Texte proposé par la Commission	*Amendement*
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***.	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, ***conformément à l'article 6, paragraphe 1, point c), et à l'article 6, paragraphe 3, du règlement (UE) 2016/679 et*** dans les meilleurs délais après l'enregistrement d'un nom de domaine, ***certaines*** données d'enregistrement de ***nom de*** domaine***, telles que le nom de domaine et le nom de la personne morale***.

Amendement 100

Proposition de directive
Article 23 – paragraphe 5

Texte proposé par la Commission	*Amendement*
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	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 ***autorités publiques, y compris les autorités compétentes au titre de la présente***

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 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.

directive, 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, ou les autorités de contrôle au titre du règlement (UE) 2016/679, 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 à toutes les demandes d'accès ***légitimes et dûment justifiées***. Les États membres veillent à ce que les politiques et procédures de divulgation de ces données soient rendues publiques.

Amendement 101

Proposition de directive
Article 24 – paragraphe 3

Texte proposé par la Commission	*Amendement*
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.	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. ***Sans préjudice des compétences des autorités de contrôle au titre du règlement (UE) 2016/679,*** 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.

Amendement 102

Proposition de directive
Article 25 – paragraphe 1 – partie introductive

Texte proposé par la Commission	*Amendement*
1. L'ENISA crée et tient un registre des entités essentielles et importantes visées à l'article 24, paragraphe 1. Les entités doivent soumettre les informations suivantes à l'ENISA au plus tard [12 mois après l'entrée en vigueur de la directive]:	1. L'ENISA crée et tient un registre ***sécurisé*** des entités essentielles et importantes visées à l'article 24, paragraphe 1. Les entités doivent soumettre les informations suivantes à l'ENISA au plus tard [12 mois après l'entrée en vigueur de la directive]:

Amendement 103

Proposition de directive
Article 26 – paragraphe 1 – partie introductive

Texte proposé par la Commission	*Amendement*
1. Sans préjudice du règlement (UE) 2016/679, les États membres veillent à ce que les entités essentielles et importantes puissent échanger entre elles des informations pertinentes en matière de cybersécurité, y compris des informations relatives aux cybermenaces, 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:	1. Sans préjudice du règlement (UE) 2016/679 ***ou de la directive 2002/58/CE***, les États membres veillent à ce que les entités essentielles et importantes puissent échanger entre elles des informations pertinentes en matière de cybersécurité, y compris des informations relatives aux cybermenaces, aux vulnérabilités, aux indicateurs de compromission, aux tactiques, techniques et procédures, aux alertes de cybersécurité et aux outils de configuration***, ainsi qu'à la localisation ou à l'identité de l'auteur de l'attaque***, lorsque ce partage d'informations:

Amendement 104

Proposition de directive
Article 28 – paragraphe 2

Texte proposé par la Commission	*Amendement*
2. Pour traiter des incidents donnant lieu à des violations de données à caractère	2. Pour traiter des incidents donnant lieu à des violations de données à caractère

personnel, les autorités compétentes coopèrent étroitement avec les autorités ***chargées*** de la ***protection*** des données.	personnel, les autorités compétentes coopèrent étroitement avec les autorités ***de contrôle, sans préjudice des compétences, des tâches et des pouvoirs des autorités de contrôle au titre du règlement (UE) 2016/679. À cette fin, les autorités compétentes et les autorités de de contrôle échangent des informations pertinentes pour leurs domaines de compétence respectifs. En outre, à la demande des autorités de contrôle compétentes, les autorités compétentes leur communiquent toutes les informations obtenues dans le cadre de tout audit ou enquête ayant trait au traitement de données à caractère personnel.***

Amendement 105

Proposition de directive
Article 29 – paragraphe 4 – point h

Texte proposé par la Commission	*Amendement*
h) d'ordonner à ces entités de rendre publics les aspects de non-respect des obligations énoncées dans la présente directive de manière spécifique;	***supprimé***

Amendement 106

Proposition de directive
Article 29 – paragraphe 5 – point b

Texte proposé par la Commission	*Amendement*
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	***supprimé***

responsabilités dirigeantes dans cette entité.

Amendement 107

Proposition de directive
Article 29 – paragraphe 5 – alinéa 1

Texte proposé par la Commission	*Amendement*
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.	***Cette sanction est appliquée*** 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.

Amendement 108

Proposition de directive
Article 29 – paragraphe 7 – point c

Texte proposé par la Commission	*Amendement*
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;	c) des dommages effectifs causés, ***matériels ou non matériels,*** ou des pertes ***subies***, 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;

Amendement 109

Proposition de directive
Article 29 – paragraphe 7 – point c bis (nouveau)

Texte proposé par la Commission	*Amendement*
	c bis) toute infraction antérieure pertinente commise par l'entité

concernée;

Amendement 110

Proposition de directive
Article 29 – paragraphe 7 – point c ter (nouveau)

Texte proposé par la Commission	*Amendement*
	c ter) la manière dont l'autorité compétente a eu connaissance de la violation, notamment si, et dans quelle mesure, l'entité a notifié la violation;

Amendement 111

Proposition de directive
Article 29 – paragraphe 7 – point g

Texte proposé par la Commission	*Amendement*
g) ***du*** degré de coopération ***de la ou des personnes physiques ou morales tenues pour responsables avec*** les ***autorités compétentes.***	g) ***le*** degré de coopération ***établi avec les autorités compétentes en vue de remédier à la violation et d'en atténuer*** les ***éventuels effets négatifs;***

Amendement 112

Proposition de directive
Article 29 – paragraphe 7 – point g bis (nouveau)

Texte proposé par la Commission	*Amendement*
	g bis) toute autre circonstance aggravante ou atténuante applicable aux circonstances de l'espèce, telle que les avantages financiers obtenus ou les pertes évitées, directement ou indirectement, du fait de la violation.

Amendement 113

Proposition de directive
Article 29 – paragraphe 9

Texte proposé par la Commission	*Amendement*
9. Les États membres veillent à ce que leurs autorités compétentes informent les autorités compétentes de ***l'État membre concerné*** 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. Sur demande des autorités compétentes au titre de la directive (UE) XXXX/XXXX [directive relative à la résilience des entités critiques], les autorités compétentes peuvent exercer leurs pouvoirs de surveillance et d'exécution sur une entité essentielle définie comme critique ou équivalente.	9. Les États membres veillent à ce que leurs autorités compétentes informent ***en temps réel*** les autorités compétentes de ***tous les États membres concernés*** 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. Sur demande des autorités compétentes au titre de la directive (UE) XXXX/XXXX [directive relative à la résilience des entités critiques], les autorités compétentes peuvent exercer leurs pouvoirs de surveillance et d'exécution sur une entité essentielle définie comme critique ou équivalente.

Amendement 114

Proposition de directive
Article 30 – paragraphe 4 – point g

Texte proposé par la Commission	*Amendement*
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;	***supprimé***

Amendement 115

Proposition de directive
Article 30 – paragraphe 4 – point h

Texte proposé par la Commission	*Amendement*
h) de faire une déclaration publique	h) de faire une déclaration publique

désignant la ou les personnes physiques ***et morales*** responsables de la violation d'une obligation énoncée dans la présente directive et la nature de cette violation;	désignant la ou les personnes physiques responsables de la violation d'une obligation énoncée dans la présente directive et la nature de cette violation;

Amendement 116

Proposition de directive
Article 31 – paragraphe 2

Texte proposé par la Commission	*Amendement*
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).	2. ***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)***, en fonction des circonstances propres à chaque cas***.

Amendement 117

Proposition de directive
Article 31 – paragraphe 3

Texte proposé par la Commission	*Amendement*
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.	3. ***La décision d'imposer une amende administrative est fonction des circonstances propres à chaque cas*** 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.

Amendement 118

Proposition de directive
Article 32 – paragraphe 1

Texte proposé par la Commission	*Amendement*
1. Lorsque les autorités compétentes disposent d'indications selon lesquelles l'infraction commise par une entité essentielle ou importante à l'égard des	1. Lorsque les autorités compétentes disposent d'indications selon lesquelles l'infraction commise par une entité essentielle ou importante à l'égard des

obligations énoncées aux articles 18 et 20 donne 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 les autorités de contrôle compétentes en vertu des articles 55 et 56 dudit règlement dans un délai ***raisonnable***.	obligations énoncées aux articles 18 et 20 donne 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 les autorités de contrôle compétentes en vertu des articles 55 et 56 dudit règlement ***sans retard injustifié et, dans tous les cas,*** dans un délai ***de 24 heures***.

Amendement 119

Proposition de directive
Article 32 – paragraphe 3

Texte proposé par la Commission	*Amendement*
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.	*(Ne concerne pas la version française.)*

Amendement 120

Proposition de directive
Article 34 bis (nouveau)

Texte proposé par la Commission	*Amendement*
	Article 34 bis
	Responsabilité pour non-respect
	Sans préjudice de tout recours administratif ou non juridictionnel disponible, les destinataires de services fournis par des entités essentielles et importantes, ayant subi des dommages dus au non-respect de la présente directive par les prestataires, ont droit à un recours juridictionnel effectif.

Amendement 121

Proposition de directive
Article 35 – alinéa 1

Texte proposé par la Commission	*Amendement*
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. À cette fin et en vue de faire progresser la coopération stratégique et opérationnelle, la Commission tient compte des rapports du groupe de coopération et du réseau des CSIRT sur l'expérience acquise au niveau tant stratégique qu'opérationnel. Le premier rapport est présenté au plus tard le… [***54*** mois après la date d'entrée en vigueur de la présente directive].	La Commission réexamine ***tous les trois ans*** le fonctionnement de la présente directive et en rend compte au Parlement européen et au Conseil. Le compte rendu évalue notamment ***dans quelle mesure la directive a contribué à assurer un niveau commun élevé en matière de sécurité et d'intégrité des réseaux et des systèmes d'information, tout en dotant la vie privée et les données à caractère personnel d'une protection optimale, ainsi que*** 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. À cette fin et en vue de faire progresser la coopération stratégique et opérationnelle, la Commission tient compte des rapports du groupe de coopération et du réseau des CSIRT sur l'expérience acquise au niveau tant stratégique qu'opérationnel. Le premier rapport est présenté au plus tard le… [***36*** mois après la date d'entrée en vigueur de la présente directive].

Amendement 122

Proposition de directive
Annexe I – point 5 (Santé) – tiret 6 (nouveau)

Texte proposé par la Commission

Secteur	Sous-secteur	Type d'entité
5. Santé		– Prestataires de soins de santé au sens de l'article 3, point g), de la directive 2011/24/UE([90])
		– Laboratoires de référence de l'Union européenne visés à l'article 15 du règlement XXXX/XXXX relatif aux menaces transfrontières graves sur la santé([91])
		– 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([92]) – 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 publique («liste des dispositifs médicaux critiques en cas d'urgence de santé publique») au sens de l'article 20 du règlement XXXX([93])

[91] [Règlement du Parlement européen et du Conseil relatif aux menaces transfrontières graves sur la santé et abrogeant la décision nº 1082/2013/UE, référence à mettre à jour une fois que la proposition COM (2020) 727 final sera adoptée].

[92] 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).

[93] [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].

Amendement

Secteur	Sous-secteur	Type d'entité
5. Santé		– Prestataires de soins de santé au sens de l'article 3, point g), de la directive 2011/24/UE([90]) – Laboratoires de référence de l'Union européenne visés à l'article 15 du règlement XXXX/XXXX relatif aux menaces transfrontières graves sur la santé([91]) – 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([92]) – 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 publique («liste des dispositifs médicaux critiques en cas d'urgence de santé publique») au sens de l'article 20 du règlement XXXX([93]) – ***Entités titulaires d'une autorisation de***

distribution au sens de l'article 79 de la directive 2001/83/CE

[91] [Règlement du Parlement européen et du Conseil relatif aux menaces transfrontières graves sur la santé et abrogeant la décision nº 1082/2013/UE, référence à mettre à jour une fois que la proposition COM (2020) 727 final sera adoptée].

[92] 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).

[93] [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].

PROCÉDURE DE LA COMMISSION SAISIE POUR AVIS

Titre	Mesures en vue d'un niveau commun élevé de cybersécurité à travers l'Union, abrogation de la directive (UE) 2016/1148
Références	COM(2020)0823 – C9-0422/2020 – 2020/0359(COD)
Commission compétente au fond Date de l'annonce en séance	ITRE 21.1.2021
Avis émis par Date de l'annonce en séance	LIBE 21.1.2021
Commissions associées - date de l'annonce en séance	20.5.2021
Rapporteur(e) pour avis Date de la nomination	Lukas Mandl 12.4.2021
Examen en commission	16.6.2021 3.9.2021 11.10.2021
Date de l'adoption	12.10.2021
Résultat du vote final	+: 44 –: 14 0: 4
Membres présents au moment du vote final	Magdalena Adamowicz, Katarina Barley, Pernando Barrena Arza, Pietro Bartolo, Nicolas Bay, Vladimír Bilčík, Vasile Blaga, Ioan-Rareş Bogdan, Patrick Breyer, Saskia Bricmont, Jorge Buxadé Villalba, Damien Carême, Caterina Chinnici, Clare Daly, Marcel de Graaff, Anna Júlia Donáth, Lena Düpont, Cornelia Ernst, Laura Ferrara, Nicolaus Fest, Maria Grapini, Sophia in 't Veld, Patryk Jaki, Marina Kaljurand, Assita Kanko, Fabienne Keller, Peter Kofod, Moritz Körner, Jeroen Lenaers, Juan Fernando López Aguilar, Lukas Mandl, Roberta Metsola, Nadine Morano, Javier Moreno Sánchez, Maite Pagazaurtundúa, Nicola Procaccini, Emil Radev, Paulo Rangel, Terry Reintke, Diana Riba i Giner, Ralf Seekatz, Michal Šimečka, Birgit Sippel, Sara Skyttedal, Martin Sonneborn, Tineke Strik, Ramona Strugariu, Annalisa Tardino, Milan Uhrík, Tom Vandendriessche, Bettina Vollath, Elissavet Vozemberg-Vrionidi, Jadwiga Wiśniewska, Javier Zarzalejos
Suppléants présents au moment du vote final	Olivier Chastel, Tanja Fajon, Jan-Christoph Oetjen, Philippe Olivier, Anne-Sophie Pelletier, Thijs Reuten, Rob Rooken, Maria Walsh

VOTE FINAL PAR APPEL NOMINAL
EN COMMISSION SAISIE POUR AVIS

44	+
ID	Nicolas Bay, Nicolaus Fest, Peter Kofod, Philippe Olivier, Annalisa Tardino, Tom Vandendriessche
NI	Laura Ferrara
PPE	Magdalena Adamowicz, Vladimír Bilčík, Vasile Blaga, Ioan-Rareş Bogdan, Lena Düpont, Jeroen Lenaers, Lukas Mandl, Roberta Metsola, Nadine Morano, Emil Radev, Paulo Rangel, Ralf Seekatz, Sara Skyttedal, Elissavet Vozemberg-Vrionidi, Maria Walsh, Javier Zarzalejos
Renew	Olivier Chastel, Anna Júlia Donáth, Sophia in 't Veld, Fabienne Keller, Moritz Körner, Jan-Christoph Oetjen, Maite Pagazaurtundúa, Michal Šimečka, Ramona Strugariu
S&D	Katarina Barley, Pietro Bartolo, Caterina Chinnici, Tanja Fajon, Maria Grapini, Marina Kaljurand, Juan Fernando López Aguilar, Javier Moreno Sánchez, Thijs Reuten, Birgit Sippel, Bettina Vollath
Verts/ALE	Damien Carême

14	-
ECR	Jorge Buxadé Villalba, Patryk Jaki, Assita Kanko, Nicola Procaccini, Rob Rooken, Jadwiga Wiśniewska
ID	Marcel de Graaff
NI	Martin Sonneborn, Milan Uhrík
Verts/ALE	Patrick Breyer, Saskia Bricmont, Terry Reintke, Diana Riba i Giner, Tineke Strik

4	0
The Left	Pernando Barrena Arza, Clare Daly, Cornelia Ernst, Anne-Sophie Pelletier

Légende des signes utilisés:
+ : pour
- : contre
0 : abstention