Informations de base

2020/0359(COD) COD - Procédure législative ordinaire (ex-procedure codécision) Directive	Procédure terminée
Un niveau élevé commun de cybersécurité Abrogation Directive (EU) 2016/1148 2013/0027(COD) **Subject** 2.80 Coopération et simplification administratives 3.30.06 Technologies de l'information et de la communication, technologies numériques 3.30.07 Cybersécurité, politique cyberespace 3.30.25 Réseaux mondiaux et société de l'information, internet 7.30.09 Sécurité publique **Priorités législatives** Déclaration commune 2021 Déclaration commune 2022	

Acteurs principaux

Parlement européen

Commission au fond	Rapporteur(e)	Date de nomination
ITRE Industrie, recherche et énergie	GROOTHUIS Bart (Renew)	14/01/2021
	Rapporteur(e) fictif/fictive MAYDELL Eva (EPP) KAILI Eva (S&D) ANDRESEN Rasmus (Greens/EFA) TOŠENOVSKÝ Evžen (ECR) MARIANI Thierry (ID) MATIAS Marisa (The Left)	

Commission pour avis	Rapporteur(e) pour avis	Date de nomination
AFET Affaires étrangères	GREGOROVÁ Markéta (Greens/EFA)	22/02/2021
ECON Affaires économiques et monétaires	La commission a décidé de ne pas donner d'avis.	

	IMCO Marché intérieur et protection des consommateurs	LØKKEGAARD Morten (Renew)	09/02/2021
	TRAN Transports et tourisme	DALUNDE Jakop G. (Greens /EFA)	03/02/2021
	CULT Culture et éducation	La commission a décidé de ne pas donner d'avis.	
	LIBE Libertés civiles, justice et affaires intérieures (Commission associée)	MANDL Lukas (EPP)	12/04/2021

Conseil de l'Union européenne	

Commission européenne	DG de la Commission	Commissaire
	Réseaux de communication, contenu et technologies	BRETON Thierry

Comité économique et social européen

Evénements clés

Date	Evénement	Référence	Résumé
16/12/2020	Publication de la proposition législative	COM(2020)0823	Résumé
21/01/2021	Annonce en plénière de la saisine de la commission, 1ère lecture		
20/05/2021	Annonce en plénière de la saisine des commissions associées		
28/10/2021	Vote en commission,1ère lecture		
28/10/2021	Décision de la commission parlementaire d'ouvrir des négociations interinstitutionnelles à travers d'un rapport adopté en commission		
04/11/2021	Dépôt du rapport de la commission, 1ère lecture	A9-0313/2021	Résumé
10/11/2021	Décision de la commission parlementaire d'engager des négociations interinstitutionnelles annoncée en plénière (Article 72)		
22/11/2021	Décision de la commission parlementaire d'engager des négociations interinstitutionnelles confirmée par la plénière (Article 72)		
13/07/2022	Approbation en commission du texte adopté en négociations interinstitutionnelles de la 1ère lecture		
10/11/2022	Décision du Parlement, 1ère lecture	T9-0383/2022	Résumé
10/11/2022	Résultat du vote au parlement		
10/11/2022	Débat en plénière		
28/11/2022	Adoption de l'acte par le Conseil après la 1ère lecture du Parlement		
14/12/2022	Signature de l'acte final		

27/12/2022	Publication de l'acte final au Journal officiel		

Informations techniques	
Référence de la procédure	2020/0359(COD)
Type de procédure	COD - Procédure législative ordinaire (ex-procedure codécision)
Sous-type de procédure	Note thématique
Instrument législatif	Directive
Modifications et abrogations	Abrogation Directive (EU) 2016/1148 2013/0027(COD)
Base juridique	Règlement du Parlement EP 57_o Traité sur le fonctionnement de l'Union européenne TFEU 114-p1
Autre base juridique	Règlement du Parlement EP 165
Consultation obligatoire d'autres institutions	Comité économique et social européen
État de la procédure	Procédure terminée
Dossier de la commission	ITRE/9/04961

Portail de documentation

Parlement Européen

Type de document	Commission	Référence	Date	Résumé
Projet de rapport de la commission		PE692.602	03/05/2021	
Amendements déposés en commission		PE693.680	03/06/2021	
Amendements déposés en commission		PE693.723	03/06/2021	
Avis de la commission	TRAN	PE689.861	14/07/2021	
Avis de la commission	IMCO	PE691.156	14/07/2021	
Avis de la commission	AFET	PE691.371	15/07/2021	
Avis de la commission	LIBE	PE693.822	15/10/2021	
Rapport déposé de la commission, 1ère lecture/lecture unique		A9-0313/2021	04/11/2021	Résumé
Texte adopté du Parlement, 1ère lecture/lecture unique		T9-0383/2022	10/11/2022	Résumé

Conseil de l'Union

Type de document	Référence	Date	Résumé
Projet d'acte final	00032/2022/LEX	14/12/2022	

Commission Européenne

Type de document	Référence	Date	Résumé
Document de base législatif	COM(2020)0823	16/12/2020	Résumé

Document annexé à la procédure	SEC(2020)0430	16/12/2020	
Document annexé à la procédure	SWD(2020)0344	16/12/2020	
Document annexé à la procédure	SWD(2020)0345	16/12/2020	
Réaction de la Commission sur le texte adopté en plénière	SP(2022)688	17/01/2023	

Parlements nationaux

Type de document	Parlement /Chambre	Référence	Date	Résumé
Contribution	CZ_CHAMBER	COM(2020)0823	25/02/2021	
Contribution	ES_PARLIAMENT	COM(2020)0823	18/03/2021	
Contribution	PT_PARLIAMENT	COM(2020)0823	18/03/2021	
Contribution	ES_PARLIAMENT	SWD(2020)0344	22/03/2021	
Contribution	ES_PARLIAMENT	SWD(2020)0345	22/03/2021	
Contribution	CZ_SENATE	COM(2020)0823	24/03/2021	

Autres Institutions et organes

Institution/organe	Type de document	Référence	Date	Résumé
EDPS	Document annexé à la procédure	N9-0025/2021 JO C 183 11.05.2021, p. 0003	11/03/2021	
EESC	Comité économique et social: avis, rapport	CES5749/2020	27/04/2021	
ECB	Banque centrale européenne: avis, orientation, rapport	CON/2022/0014 JO C 233 16.06.2022, p. 0022	11/04/2022	

Informations complémentaires

Source	Document	Date
Parlement européen	Briefing	19/02/2021
Commission européenne	EUR-Lex	

Réunions avec des représentant(e)s d'intérêts, publiées conformément au règlement intérieur

Rapporteur(e)s, rapporteur(e)s fictifs/fictives et président(e)s des commissions

Transparence

Nom	Rôle	Commission	Date	Représentant(e)s d'intérêts
GROOTHUIS Bart	Rapporteur(e)	ITRE	21/06/2022	Considerati Brussels B.V.

GROOTHUIS Bart	Rapporteur(e)	ITRE	20/06/2022	ICANN
GROOTHUIS Bart	Rapporteur(e)	ITRE	10/06/2022	ICANN
GROOTHUIS Bart	Rapporteur(e)	ITRE	24/03/2022	ICANN
GROOTHUIS Bart	Rapporteur(e)	ITRE	23/03/2022	Broadcom
GROOTHUIS Bart	Rapporteur(e)	ITRE	17/03/2022	BUSINESSEUROPE
GROOTHUIS Bart	Rapporteur(e)	ITRE	09/03/2022	Palo Alto Networks Inc.
GROOTHUIS Bart	Rapporteur(e)	ITRE	03/03/2022	Hanbury Strategy and Communications Limited
GROOTHUIS Bart	Rapporteur(e)	ITRE	03/03/2022	DIGITALEUROPE
GROOTHUIS Bart	Rapporteur(e)	ITRE	10/02/2022	Provincie Flevoland

Autres membres

Transparence		
Nom	Date	Représentant(e)s d'intérêts
PETERSEN Morten	11/11/2021	Euritas

Acte final	
Rectificatif à l'acte final 32022L2555R(04) JO L 000 22.12.2023, p. 0000	
Directive 2022/2555 JO L 333 27.12.2022, p. 0080	Résumé

Un niveau élevé commun de cybersécurité

2020/0359(COD) - 27/12/2022 - Acte final

OBJECTIF : renforcer la cybersécurité et la résilience dans l'ensemble de l'Union.

ACTE LÉGISLATIF : Directive (UE) 2022/2555 du Parlement européen et du Conseil concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union, modifiant le règlement (UE) no 910/2014 et la directive (UE) 2018/1972, et abrogeant la directive (UE) 2016/1148 (directive SRI 2).

CONTENU : la directive établit des mesures qui ont pour but d'obtenir **un niveau commun élevé de cybersécurité** dans l'ensemble de l'Union en vue améliorer encore la résilience et les capacités de réaction aux incidents du secteur public comme du secteur privé et de l'UE dans son ensemble. La nouvelle directive, appelée «SRI 2», remplacera l'actuelle directive sur la sécurité des réseaux et des systèmes d'information (directive SRI).

Objectifs

La directive révisée a pour objectif **d'harmoniser les exigences en matière de cybersécurité** et la mise en œuvre des mesures de cybersécurité dans les différents États membres. À cette fin, elle fixe les règles minimales d'un cadre réglementaire et définit les mécanismes d'une coopération efficace entre les autorités compétentes de chaque État membre.

La directive SRI 2 constituera la base des mesures de **gestion des risques** en matière de cybersécurité et des obligations en matière de **signalement** dans tous les secteurs essentiels couverts par la directive, à savoir l'énergie, les transports, la banque, les infrastructures des marchés financiers, la santé, l'eau potable, l'infrastructure numérique, les administrations publiques et le secteur de l'espace, ainsi que dans les secteurs importants comme les services postaux, la gestion des déchets, les produits chimiques, l'alimentation, la fabrication de dispositifs médicaux, l'électronique, les machines, les moteurs de véhicules et les fournisseurs numériques.

Champ d'application

La nouvelle directive SRI 2 introduit comme règle générale pour l'identification des entités réglementées **une règle associée à un plafond**. Cela signifie que toutes les moyennes et grandes entités opérant dans les secteurs couverts par la directive ou fournissant des services qui en relèvent rentreront dans son champ d'application.

La directive s'appliquera aux entités de l'administration publique aux niveaux central et régional. En outre, les États membres pourront décider de l'appliquer également à ce type d'entités au niveau local ainsi qu'aux établissements d'enseignement, en particulier lorsqu'ils mènent des activités de recherche critiques.

La directive ne s'appliquera pas aux entités de l'administration publique qui exercent leurs activités dans les domaines de la sécurité nationale, de la sécurité publique, de la défense ou de l'application de la loi, y compris la prévention et la détection des infractions pénales, ainsi que les enquêtes et les poursuites en la matière. Les parlements et les banques centrales sont également exclus du champ d'application.

La directive fixe les règles minimum d'un cadre réglementaire et ne fait pas obstacle à l'adoption ou au maintien par les États membres de dispositions assurant un niveau plus élevé de cybersécurité.

La directive comprend des dispositions supplémentaires visant à garantir **la proportionnalité**, un niveau plus élevé de gestion des risques et des **critères clairs** relatifs au caractère critique des entités pour permettre aux autorités nationales d'inclure d'autres entités.

Cadres coordonnés en matière de cybersécurité

La directive fixe des obligations qui imposent aux États membres d'adopter des **stratégies nationales** en matière de cybersécurité, de désigner ou de mettre en place des autorités compétentes, des autorités chargées de la gestion des cybercrises, des points de contact uniques en matière de cybersécurité et des centres de réponse aux incidents de sécurité informatique (CSIRT).

Coopération au niveau de l'Union

La directive définit les mécanismes d'une coopération efficace entre les autorités compétentes de chaque État membre. Elle institue un **groupe de coopération** afin de soutenir et de faciliter la coopération stratégique et l'échange d'informations entre les États membres et de renforcer la confiance. Un **réseau des CSIRT nationaux** est institué afin de contribuer au renforcement de la confiance et de promouvoir une coopération opérationnelle rapide et effective entre les États membres.

La directive instaure également officiellement le réseau européen pour la préparation et la gestion des crises de cybersécuriyé (**UE-CyCLONe**), qui soutiendra la gestion coordonnée des incidents de cybersécurité majeurs.

Mécanisme volontaire d'apprentissage par les pairs

Un mécanisme volontaire d'apprentissage par les pairs renforcera la confiance mutuelle et les enseignements à tirer des bonnes pratiques et des expériences dans l'Union, contribuant ainsi à un niveau élevé commun de cybersécurité.

Le groupe de coopération établira, au plus tard le 17 janvier 2025, avec l'aide de la Commission et de l'ENISA et, s'il y a lieu, du réseau des CSIRT, la méthodologie et les aspects organisationnels des évaluations par les pairs en vue de tirer des enseignements des expériences partagées, de renforcer la confiance mutuelle, de parvenir à un niveau élevé commun de cybersécurité, ainsi que de renforcer les capacités et les politiques des États membres en matière de cybersécurité qui sont nécessaires à la mise en œuvre de la directive.

Simplification des obligations de signalement

La directive rationalise les obligations en matière de signalement afin d'éviter d'engendrer un phénomène de surdéclaration et de créer une charge excessive pour les entités concernées.

Afin de simplifier la communication des informations requises en vertu de la directive, les États membres devront fournir des moyens techniques, tels qu'un point d'entrée unique, des systèmes automatisés, des formulaires en ligne, des interfaces conviviales, des modèles et des plateformes dédiées à l'utilisation des entités, indépendamment du fait qu'elles relèvent ou non du champ d'application de la directive, pour la communication des informations pertinentes à transmettre.

Enfin, la directive prévoit **des voies de recours et des sanctions** pour assurer le respect de la législation.

ENTRÉE EN VIGUEUR : 16.1.2023

TRANSPOSITION : au plus tard le 17.10.2024. Les dispositions sont applicables à partir du 18.10.2024.

Un niveau élevé commun de cybersécurité

2020/0359(COD) - 16/12/2020 - Document de base législatif

OBJECTIF : introduire des mesures visant à un niveau commun élevé de cybersécurité dans toute l'Union.

ACTE PROPOSÉ : Règlement du Parlement européen et du Conseil

RÔLE DU PARLEMENT EUROPÉEN : le Parlement européen décide conformément à la procédure législative ordinaire et sur un pied d'égalité avec le Conseil.

CONTEXTE : la directive (UE) 2016/1148 du Parlement européen et du Conseil vise à renforcer les capacités de cybersécurité dans l'UE, à atténuer les menaces pesant sur les systèmes de réseaux et d'information utilisés pour fournir des services essentiels dans des secteurs clés et à assurer la continuité de ces services en cas d'incidents de cybersécurité, contribuant ainsi au bon fonctionnement de l'économie et de la société de l'UE.

Toutefois, depuis l'entrée en vigueur de la directive (UE) 2016/1148, des progrès significatifs ont été réalisés pour accroître le niveau de résilience de l'Union en matière de cybersécurité.

CONTENU : la présente proposition vise à remplacer la directive (UE) 2016/1148 relative à la sécurité des réseaux et des systèmes d'information (directive NIS). Il s'agit du premier acte législatif européen en matière de cybersécurité, qui prévoit des mesures juridiques visant à renforcer le niveau général de cybersécurité dans l'UE. La proposition modernise le cadre juridique existant en tenant compte de la numérisation accrue du marché intérieur au cours des dernières années et de l'évolution du paysage des menaces en matière de cybersécurité.

Champ d'application

La proposition devrait s'appliquer à certaines entités essentielles publiques ou privées opérant dans les secteurs énumérés à l'annexe I (énergie ; transports ; banques ; infrastructures des marchés financiers ; santé, eau potable ; eaux usées ; infrastructures numériques ; administration publique et espace) et à certaines entités importantes opérant dans les secteurs énumérés à l'annexe II (services postaux et de courrier ; gestion des déchets ; fabrication, production et distribution de produits chimiques ; production, transformation et distribution de denrées alimentaires ; fabrication et fournisseurs numériques).

Les micro et petites entités seraient exclues du champ d'application de la directive, à l'exception des fournisseurs de réseaux de communications électroniques ou de services de communications électroniques accessibles au public, des fournisseurs de services fiduciaires, des registres de noms de domaine de premier niveau (TLD) et de l'administration publique, ainsi que de certaines autres entités, telles que le fournisseur unique d'un service dans un État membre.

Cadres nationaux de cybersécurité

La proposition prévoit que les États membres seront tenus d'adopter une stratégie nationale de cybersécurité définissant les objectifs stratégiques et les mesures politiques et réglementaires appropriées en vue d'atteindre et de maintenir un niveau élevé de cybersécurité.

Elle établit également un cadre pour la divulgation coordonnée des vulnérabilités et exige des États membres qu'ils désignent des équipes d'intervention en cas d'incident de sécurité informatique qui agiront comme intermédiaires de confiance et faciliteront l'interaction entre les entités déclarantes et les fabricants ou fournisseurs de produits et services de technologies de l'information et de la communication (TIC).

Les États membres seraient tenus de mettre en place des cadres nationaux de gestion des crises de cybersécurité, en désignant des autorités nationales compétentes chargées de la gestion des incidents et des crises de cybersécurité à grande échelle.

Gestion des risques liés à la cybersécurité et obligations d'information

La proposition exige des États membres qu'ils prévoient que les organes de gestion de toutes les entités relevant du champ d'application approuvent les mesures de gestion des risques en matière de cybersécurité prises par les entités respectives et suivent une formation spécifique à la cybersécurité. Les entités relevant du champ d'application devraient des mesures techniques et organisationnelles appropriées et proportionnées pour gérer les risques de cybersécurité posés à la sécurité des réseaux et des systèmes d'information.

Les registres du TLD et les entités fournissant des services d'enregistrement de noms de domaine pour le TLD devraient collecter et conserver des données exactes et complètes sur l'enregistrement des noms de domaine. En outre, ces entités seraient tenues de fournir un accès efficace aux données d'enregistrement de domaine pour les demandeurs d'accès légitimes.

Compétence et enregistrement

En règle générale, les entités essentielles et importantes sont considérées comme relevant de la juridiction de l'État membre où elles fournissent leurs services. La proposition prévoit que certains types d'entités (fournisseurs de services DNS, registres de noms de TLD, fournisseurs de services d'informatique en nuage, fournisseurs de services de centres de données et fournisseurs de réseaux de diffusion de contenu, ainsi que certains fournisseurs numériques) seraient réputés relever de la juridiction de l'État membre dans lequel ils ont leur principal établissement dans l'Union.

Partage d'informations

Les États membres devraient prévoir des règles permettant aux entités de s'engager dans le partage d'informations liées à la cybersécurité dans le cadre d'accords spécifiques de partage d'informations sur la cybersécurité.

Supervision et application

Les autorités compétentes seraient tenues de superviser les entités relevant du champ d'application de la directive proposée, et notamment de veiller à ce qu'elles respectent les exigences en matière de sécurité et de notification des incidents. La proposition exige également que les États membres imposent des amendes administratives aux entités essentielles et importantes et définit certaines amendes maximales.

Un niveau élevé commun de cybersécurité

2020/0359(COD) - 04/11/2021 - Rapport déposé de la commission, 1ère lecture/lecture unique

La commission de l'industrie, de la recherche et de l'énergie a adopté le rapport de Bart GROOTHUIS (Renew Europe, NL) 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

La commission compétente a recommandé que la position du Parlement européen adoptée en première lecture dans le cadre de la procédure législative ordinaire modifie la proposition comme suit:

Objet et champ d'application

La directive s'appliquerait aux entités publiques et privées essentielles et importantes d'un type appelé «**entités essentielles**» à l'annexe I et «**entités importantes**» à l'annexe II, qui fournissent leurs services ou mènent leurs activités au sein de l'Union. Elle ne s'appliquerait pas aux petites entreprises ou aux microentreprises. Au plus tard 6 mois après le délai de transposition, les États membres devraient établir une **liste des entités essentielles et importantes**. Cette liste devrait être mise à jour régulièrement et au moins tous les deux ans.

Les entités essentielles et importantes devraient **soumettre au moins les informations suivantes aux autorités compétentes**: i) le nom de l'entité, ii) l' adresse et les coordonnées actualisées, y compris les adresses électroniques, iii) les plages d'IP, iv) les numéros de téléphone et v) le ou les secteurs et sous-secteurs concernés mentionnés aux annexes I et II. Les entités devraient informer les autorités compétentes de toute modification de ces informations.

À cette fin, l'Agence de l'Union européenne pour la cybersécurité (ENISA), en coopération avec le groupe de coopération, devrait publier dans les meilleurs délais des **lignes directrices** et des modèles concernant les obligations de notification. Le traitement de données à caractère personnel au titre de la directive serait effectué conformément au règlement général sur la protection des données (RGPD).

Stratégie nationale en matière de cybersécurité

Cette stratégie devrait également comprendre un cadre pour la répartition des rôles et des responsabilités des organismes et entités publics ainsi que des autres acteurs concernés, un point de contact unique en matière de cybersécurité pour les PME ainsi qu'une évaluation du niveau général de sensibilisation des citoyens à la cybersécurité.

Les États membres devraient par ailleurs adopter :

- une politique en matière de cybersécurité pour chaque secteur couvert par la directive;

- des prescriptions relatives au cryptage et l'utilisation de produits de cybersécurité à code source ouvert;

- une politique liée au maintien de la disponibilité générale et de **l'intégrité du noyau public de l'internet ouvert**, y compris la cybersécurité des câbles de communications sous-marins;

- une politique visant à promouvoir le développement et l'intégration de technologies émergentes, telles que **l'intelligence artificielle**, dans les outils et applications de renforcement de la cybersécurité;

- une politique de promotion de **l'hygiène informatique** augmentant la sensibilisation générale des citoyens aux menaces et aux meilleures pratiques en matière de cybersécurité;

- une politique de promotion de la **cyberdéfense** active;

- une politique pour aider les autorités à développer des compétences et à mieux comprendre les aspects de sécurité nécessaires pour concevoir, construire et gérer des lieux connectés;

- une politique traitant spécifiquement de la menace des **logiciels rançonneurs** et s'efforçant de désorganiser le modèle économique de ces derniers;

- une politique comprenant des procédures et des **cadres de gouvernance** pour soutenir la mise en place de partenariats public-privé en matière de cybersécurité.

L'ENISA devrait fournir des conseils aux États membres afin d'aligner les stratégies nationales de cybersécurité sur les exigences et les obligations énoncées dans la directive.

Divulgation coordonnée des vulnérabilités et base de données européenne des vulnérabilités

L'ENISA devrait élaborer et tenir à jour une base de données européenne des vulnérabilités qui exploite le registre mondial Common Vulnerabilities and Exposures (CVE). À cette fin, l'ENISA devrait adopter les mesures techniques et organisationnelles nécessaires pour assurer la sécurité et l' intégrité de la base de données.

Centres de réponse aux incidents de sécurité informatique (CSIRT)

Les États membres devraient garantir la possibilité d'un échange d'informations efficace et sécurisé à tous les niveaux de classification entre leurs propres CSIRT et les CSIRT de pays tiers au même niveau de classification. Les CSIRT devraient développer au moins les capacités techniques suivantes:

- mener une surveillance en temps réel ou quasi-réel des réseaux et des systèmes d'information, et à détecter les anomalies;

- soutenir la prévention et la détection des intrusions;

- collecter et analyser les données de police scientifique;

- filtrer le trafic malveillant;

- mettre en œuvre une authentification poussée et des privilèges et contrôles d'accès forts;

- analyser les cybermenaces.

Les CSIRT devraient assumer la surveillance des cybermenaces, des vulnérabilités et des incidents au niveau national et **l'acquisition de renseignements sur les menaces en temps réel**, la réaction aux incidents et l'assistance aux entités concernées ainsi que la contribution au déploiement d'outils de partage d'informations sécurisés.

L'ENISA devrait publier, en coopération avec la Commission, un rapport bisannuel sur l'état de la cybersécurité dans l'Union et le soumettre au Parlement européen.

Obligations en matière de communication d'informations

Les États membres devraient mettre en place un **point d'entrée unique** pour toutes les notifications requises en vertu de la directive et d'autres actes pertinents de l'Union.

Les entités essentielles et importantes devraient informer les CSIRT des incidents importants qui ont une incidence sur la disponibilité de leur service **dans les 24 heures** suivant la prise de connaissance de l'incident. Elles devront informer les CSIRT des incidents importants qui portent atteinte à la confidentialité et à l'intégrité de leurs services **dans un délai de 72 heures** à compter de la prise de connaissance de l'incident.

Amendes

Afin de garantir une application efficace des obligations prévues par la directive, chaque autorité compétente pourrait imposer ou demander l' imposition d'amendes administratives si la violation a été commise délibérément ou par négligence ou si l'entité concernée avait été informée de son infraction.

Un niveau élevé commun de cybersécurité

2020/0359(COD) - 10/11/2022 - Texte adopté du Parlement, 1ère lecture/lecture unique

Le Parlement européen a adopté par 577 voix pour, 6 contre et 31 abstentions, une résolution législative 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.

La position du Parlement européen arrêtée en première lecture dans le cadre de la procédure législative ordinaire modifie la proposition comme suit:

Renforcer la cybersécurité et la résilience à l'échelle de l'UE

La directive établit des mesures qui ont pour but d'obtenir un **niveau commun élevé de cybersécurité** dans l'ensemble de l'Union, afin d'améliorer le fonctionnement du marché intérieur et d'améliorer encore la résilience et les capacités de réaction aux incidents du secteur public comme du secteur privé et de l'UE dans son ensemble. À cette fin, la présente directive fixe:

- **des obligations** qui imposent aux États membres d'adopter des stratégies nationales en matière de cybersécurité, de désigner ou de mettre en place des autorités compétentes, des autorités chargées de la gestion des cybercrises, des points de contact uniques en matière de cybersécurité et des centres de réponse aux incidents de sécurité informatique (CSIRT);

- **des mesures de gestion des risques** en matière de cybersécurité et des obligations d'information pour les entités relevant des secteurs «essentiels» comme l'énergie, les transports, la banque, les infrastructures des marchés financiers, la santé, l'eau potable, l'infrastructure numérique, les administrations publiques et le secteur de l'espace, ainsi que des secteurs «importants» comme les services postaux, la gestion des déchets, les produits chimiques, l'alimentation, la fabrication de dispositifs médicaux, l'électronique, les machines, les moteurs de véhicules et les fournisseurs numériques;

- des règles et des obligations pour le **partage d'informations** en matière de cybersécurité;

- les obligations des États membres en matière de surveillance et d'exécution.

La directive fixe les **règles minimum** d'un cadre réglementaire et ne fait pas obstacle à l'adoption ou au maintien par les États membres de dispositions assurant un niveau plus élevé de cybersécurité.

Champ d'application

Toutes **les moyennes et grandes entités** opérant dans les secteurs couverts par la directive ou fournissant des services qui en relèvent rentreront dans son champ d'application.

Les **administrations publiques** étant souvent la cible de cyberattaques, la directive s'appliquera aux entités de l'administration publique aux niveaux central et régional. En outre, les États membres pourront décider de l'appliquer également à ce type d'entités au niveau local ainsi qu'aux établissements d'enseignement, en particulier lorsqu'ils mènent des activités de recherche critiques.

La directive ne s'appliquera pas aux entités de l'administration publique qui exercent leurs activités dans les domaines de la sécurité nationale, de la sécurité publique, de la défense ou de l'application de la loi, y compris la prévention et la détection des infractions pénales, ainsi que les enquêtes et les poursuites en la matière. Les parlements et les banques centrales sont également exclus du champ d'application.

La directive comporte des dispositions supplémentaires visant à garantir la **proportionnalité**, un niveau plus élevé de gestion des risques ainsi que des **critères clairs** relatifs au caractère critique des entités afin de déterminer celles qui sont couvertes.

Coopération au niveau de l'Union

La directive définit les mécanismes d'une coopération efficace entre les autorités compétentes de chaque État membre. Elle institue un **groupe de coopération** afin de soutenir et de faciliter la coopération stratégique et l'échange d'informations entre les États membres et de renforcer la confiance. Un **réseau des CSIRT nationaux** est institué afin de contribuer au renforcement de la confiance et de promouvoir une coopération opérationnelle rapide et effective entre les États membres.

La directive instaure également officiellement le réseau européen pour la préparation et la gestion des crises de cybersécuriyé (**UE-CyCLONe**), qui soutiendra la gestion coordonnée des incidents de cybersécurité majeurs.

Mécanisme volontaire d'apprentissage par les pairs

Des évaluations par les pairs seront introduites afin de contribuer à tirer les enseignements des expériences partagées, de **renforcer la confiance mutuelle** et d'atteindre un niveau commun élevé de cybersécurité. Le groupe de coopération établira, au plus tard 2 ans après la date d'entrée en vigueur de la directive, avec l'aide de la Commission et de l'ENISA et, s'il y a lieu, du réseau des CSIRT, la méthodologie et les aspects organisationnels des évaluations par les pairs. La participation aux évaluations par les pairs s'effectuera à titre volontaire.

Simplification des obligations de signalement

La directive rationalise les obligations en matière de signalement afin d'éviter d'engendrer un phénomène de surdéclaration et de créer une charge excessive pour les entités concernées.

Afin de simplifier la communication des informations requises en vertu de la directive et de réduire la charge administrative pesant sur les entités, les États membres devront fournir des moyens techniques, tels qu'un point d'entrée unique, des systèmes automatisés, des formulaires en ligne, des interfaces conviviales, des modèles et des plateformes dédiées à l'utilisation des entités, indépendamment du fait qu'elles relèvent ou non du champ d' application de la directive, pour la communication des informations pertinentes à transmettre.

Enfin, la directive prévoit **des voies de recours et des sanctions** pour assurer le respect de la législation.