CHAMBRE DES DÉPUTÉS
GRAND-DUCHÉ DE LUXEMBOURG

Dossier consolidé

Projet de loi 8316

Projet de loi portant modification du Code pénal en vue de la transposition de la directive 2013/40/UE du Parlement et du Conseil du 12 août 2013 relative aux attaques visant les systèmes d'information et remplaçant la décision-cadre 2005/222/JAI du Conseil

Date de dépôt : 28-09-2023
Date de l'avis du Conseil d'État : 24-10-2023
Auteur(s) : Madame Sam Tanson, Ministre de la Justice

Liste des documents

Date	Description	Nom du document	Page
28-09-2023	Déposé	8316/00	3
24-10-2023	Avis du Conseil d'État (24.10.2023)	8316/01	24
21-12-2023	Commission de la Justice Procès verbal (03) de la reunion du 21 décembre 2023	03	27
25-01-2024	Rapport de commission(s) : Commission de la Justice Rapporteur(s) : Monsieur Alex Donnersbach	8316/02	55
25-01-2024	Commission de la Justice Procès verbal (07) de la reunion du 25 janvier 2024	07	60
30-01-2024	Premier vote constitutionnel (Vote Positif) En séance publique n°10 Une demande de dispense du second vote a été introduite	Bulletin de vote n°6 - Projet de loi N°8316	64
30-01-2024	Premier vote constitutionnel (Vote Positif) En séance publique n°10 Une demande de dispense du second vote a été introduite	Texte voté - projet de loi N°8316	67
06-02-2024	Dispense du second vote constitutionnel par le Conseil d'Etat (06-02-2024) Evacué par dispense du second vote (06-02-2024)	8316/03	69
04-03-2024	Publié au Mémorial A n°83 en page 1	Mémorial A N° 83 de 2024	72
	Résumé du dossier	Résumé	74

8316/00

N° 8316

CHAMBRE DES DEPUTES

Session ordinaire 2022-2023

PROJET DE LOI

portant modification du Code pénal aux fins de la transposition de la directive (UE) 2013/40 du Parlement et du Conseil du 12 août 2013 relative aux attaques visant les systèmes d'information et remplaçant la décision-cadre 2005/222/JAI du Conseil

* * *

Document de dépôt

Dépôt: le 28.9.2023

*

Le Premier Ministre,

Vu les articles 76 et 95, alinéa 1er, de la Constitution ;

Vu l'article 10 du Règlement interne du Gouvernement ;

Vu l'article 58, paragraphe 1er, du Règlement de la Chambre des Députés ;

Vu l'article 1er, paragraphe 1er, de la loi modifiée du 16 juin 2017 sur l'organisation du Conseil d'État ;

Considérant la décision du Gouvernement en conseil du 22 septembre 2023 approuvant sur proposition du Ministre de la Défense le projet de loi ci-après ;

Arrête :

Art. 1er. La Ministre de la Justice est autorisée à déposer au nom du Gouvernement à la Chambre des Députés le projet de loi portant modification du Code pénal aux fins de la transposition de la directive (UE) 2013/40 du Parlement et du Conseil du 12 août 2013 relative aux attaques visant les systèmes d'information et remplaçant la décision-cadre 2005/222/JAI du Conseil et à demander l'avis y relatif au Conseil d'État.

Art. 2. Le Ministre aux Relations avec le Parlement est chargé, pour le compte du Premier Ministre et de la Ministre de la Justice, de l'exécution du présent arrêté.

Luxembourg, le 28 septembre 2023

Le Premier Ministre,
Ministre d'État,
Xavier BETTEL

La Ministre de la Justice,
Sam TANSON

*

EXPOSE DES MOTIFS

Les systèmes d'information représentent un élément essentiel de l'interaction politique, sociale et économique. On assiste à une évolution rapide des nouvelles technologies, de la numérisation, de la convergence et de la mondialisation des réseaux informatiques.

Le bon fonctionnement et la sécurité de ces systèmes est essentiel pour le développement d'une véritable société de l'information.

La sécurité informatique est un élément important de l'espace de liberté, de sécurité et de justice.

Ainsi, garantir un niveau de protection approprié des systèmes d'information doit faire partie d'un cadre européen de mesures de prévention efficaces accompagnées de sanctions pénales en cas de cybercriminalité.

C'est pourquoi le Parlement européen et le Conseil ont adopté, le 12 août 2013, la directive 2013/40/UE relative aux attaques visant les systèmes d'information[1] qui vise à mettre en place des sanctions pénales effectives, proportionnées et dissuasives en ce qui concerne la création de réseaux zombies[2] ayant pour but une cyberattaque à grande échelle.

Dans le cadre de la législation nationale, cette directive a été transposée par la loi du 18 juillet 2014 portant 1) approbation de la Convention du conseil de l'Europe sur la cybercriminalité ouverte à la signature à Budapest le 23 novembre 2001, 2) approbation du Protocole additionnel à la convention sur la cybercriminalité, relatif à l'incrimination d'actes de nature raciste et xénophobe commis par le biais de systèmes informatiques, fait à Strasbourg le 28 janvier 20003, 3) modification du Code pénal, 4) modification du Code d'instruction criminelle, 5) modification de la loi modifiée du 30 mai 2005 concernant la protection de la vie privée dans le secteur des communications électroniques.

Néanmoins, dans le cadre de l'évaluation de conformité de transposition en droit national de la directive 2013/40/UE, la Commission européenne a estimé que le Luxembourg n'a pas correctement transposé certaines dispositions de ladite directive.

En effet, la Commission européenne a estimé que le Luxembourg n'avait pas correctement transposé dans sa législation nationale l'article 9, paragraphe 4 de la directive qui impose aux Etats membres de prendre les mesures nécessaires pour que les infractions d'atteinte à l'intégrité d'un système d'information et d'atteinte à l'intégrité des données prévues aux articles 4 et 5 de la directive, soient passibles d'une peine d'emprisonnement maximale d'au moins cinq ans lorsqu'elles sont commises dans le cadre d'une organisation criminelle, qu'elles causent un préjudice grave ou qu'elles sont commises contre un système d'information d'une infrastructure critique.

Par conséquent, il a été recommandé au Luxembourg d'élaborer une disposition légale permettant une application conforme avec la législation européenne.

Ainsi, ce projet de loi prévoit d'étendre le champ d'application matériel, tout en y appliquant une sanction effective, proportionnée et dissuasive.

*

TEXTE DU PROJET DE LOI

Article unique.

A l'article 509-4 du Code pénal est ajouté un alinéa 2 qui prend la teneur suivante :

« Sera puni des mêmes peines, celui qui aura commis les infractions visées aux articles 509-1 à 509-3 contre un système d'information d'une infrastructure critique ou qui, par la commission de ces infractions, aura causé un préjudice grave à un tel système d'information. »

*

1 Directive 2013/40/UE du Parlement européen et du Conseil du 12 août 2013 relative aux attaques contre les systèmes d'information et remplaçant la décision-cadre 2005/222/JAI du Conseil

2 "Acte qui vise à établir un contrôle à distance d'un nombre important d'ordinateurs en les contaminant au moyen de logiciels malveillants dans le cadre de cyberattaques ciblées » – définition donnée par l'Agence Nationale de la Sécurité des Systèmes d'Information

COMMENTAIRE DE L'ARTICLE UNIQUE

Cette modification de l'article 509-4 du Code pénal vise à se conformer parfaitement à l'article 9, paragraphe 4, points b) et c) de la directive relative aux attaques visant les systèmes d'information, en introduisant les attaques visant le système d'information d'une infrastructure critique et le préjudice grave comme circonstances aggravantes des infractions incriminées aux articles 4 et 5 de la directive, étant précisé que ces deux articles ne nécessitent pas d'adaptation spécifique étant donné que les libellés des articles 509-1 à 509-3 du Code pénal prévoient les infractions d'atteinte à l'intégrité d'un système et des données.

Cette modification de l'article prévoit que l'auteur d'une atteinte à l'intégrité d'un système d'information ou à l'intégrité de données sera désormais puni d'un emprisonnement de quatre mois à cinq ans et d'une amende de 1.250 euros à 30.000 euros lorsque l'attaque est dirigée contre un système d'information d'une infrastructure critique telle que définie à l'article 2, point 4 de la loi du 23 juillet 2016 portant création d'un Haut-Commissariat à la protection nationale et modifiant a) la loi modifiée du 23 juillet 1952 concernant l'organisation militaire ; b) la loi du 8 décembre 1981 sur les réquisitions en cas de conflit armé, de crise internationale grave ou de catastrophe ; c) la loi modifiée du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel ; d) la loi modifiée du 25 juin 2009 sur les marchés publics ; e) la loi modifiée du 9 décembre 2005 déterminant les conditions et modalités de nomination de certains fonctionnaires occupant des fonctions dirigeantes dans les administrations et services de l'Etat ; f) la loi modifiée du 25 mars 2015 fixant le régime des traitements et les conditions et modalités d'avancement des fonctionnaires de l'Etat[3].

Il en va de même lorsque de ces agissements aura résulté un préjudice grave pour une personne physique ou morale.

Cette modification de l'article 509-4 s'inscrit dans le cadre du maximum des peines d'emprisonnement fixées à l'article 9, paragraphe 4 de la directive, à savoir un maximum d'au moins cinq ans.

Le plafond de l'amende reflète la nécessité de punir les infractions d'atteinte à l'intégrité d'un système ou des données par une sanction effective, proportionnée et dissuasive adaptée au but poursuivi par leur auteur et le préjudice subi par une personne.

*

TEXTE COORDONNE DU CODE PENAL PAR EXTRAIT

L'article 509-4 du Code pénal est modifié comme suit :

« **Art. 509-4.** Lorsque dans les cas visés aux articles 509-1 à 509-3, il y a eu transfert d'argent ou de valeur monétaire, causant ainsi une perte de propriété à un tiers dans un but de procurer un avantage économique à la personne qui commet l'infraction ou à une tierce personne, la peine encourue sera un emprisonnement de quatre mois à cinq ans et une amende de 1.250 euros à 30.000 euros.

Sera puni des mêmes peines, celui qui aura commis les infractions visées aux articles 509-1 à 509-3 contre un système d'information d'une infrastructure critique ou qui, par la commission de ces infractions, aura causé un préjudice grave à un tel système d'information. »

*

FICHE FINANCIERE

Conformément à l'article 79 de la loi modifiée du 8 juin 1999 sur le Budget, la Comptabilité et la Trésorerie de l'Etat, Madame la Ministre de la justice déclare que le présent projet de loi ne comporte pas de dispositions dont l'application est susceptible de grever le budget de l'Etat.

*

3 Art. 2 : « Pour l'application de la présente loi, on entend par 4. « infrastructure critique » : tout point, système ou partie de celui-ci qui est indispensable à la sauvegarde des intérêts vitaux ou des besoins essentiels de tout ou partie du pays ou de la population ».

FICHE D'ÉVALUATION D'IMPACT
MESURES LÉGISLATIVES, RÉGLEMENTAIRES ET AUTRES

Coordonnées du projet

Intitulé du projet :	Projet de loi portant modification du Code pénal aux fins de la transposition de la directive (UE) 2013/40 du Parlement et du Conseil du 12 août 2013 relative aux attaques visant les systèmes d'information et remplaçant la décision-cadre 2005/222/JAI du Conseil
Ministère initiateur :	Ministère de la Justice
Auteur(s) :	Cindy Coutinho
Téléphone :	247-88526
Courriel :	cindy.coutinho@mj.etat.lu
Objectif(s) du projet :	Le projet de loi a pour objet une transposition conforme de l'article 9, paragraphe 4, point b) de la directive relative aux attaques visant les systèmes d'information.
Autre(s) Ministère(s) / Organisme(s) / Commune(s) impliqué(e)(s)	/
Date :	11/09/2023

Mieux légiférer

1 Partie(s) prenante(s) (organismes divers, citoyens,...) consultée(s) : ☐ Oui ☒ Non

Si oui, laquelle / lesquelles :

Remarques / Observations :

2 Destinataires du projet :

- Entreprises / Professions libérales : ☒ Oui ☐ Non
- Citoyens : ☒ Oui ☐ Non
- Administrations : ☐ Oui ☒ Non

3 Le principe « Think small first » est-il respecté ? (c.-à-d. des exemptions ou dérogations sont-elles prévues suivant la taille de l'entreprise et/ou son secteur d'activité ?) ☐ Oui ☐ Non ☒ N.a. [1]

Remarques / Observations :

[1] N.a. : non applicable.

4 Le projet est-il lisible et compréhensible pour le destinataire ? ☒ Oui ☐ Non

Existe-t-il un texte coordonné ou un guide pratique, mis à jour et publié d'une façon régulière ? ☐ Oui ☒ Non

Remarques / Observations :

5 Le projet a-t-il saisi l'opportunité pour supprimer ou simplifier des régimes d'autorisation et de déclaration existants, ou pour améliorer la qualité des procédures ? ☐ Oui ☒ Non

Remarques / Observations : Non applicable

6 Le projet contient-il une charge administrative [2] pour le(s) destinataire(s) ? (un coût imposé pour satisfaire à une obligation d'information émanant du projet ?) ☐ Oui ☒ Non

Si oui, quel est le coût administratif [3] approximatif total ? (nombre de destinataires x coût administratif par destinataire)

[2] Il s'agit d'obligations et de formalités administratives imposées aux entreprises et aux citoyens, liées à l'exécution, l'application ou la mise en œuvre d'une loi, d'un règlement grand-ducal, d'une application administrative, d'un règlement ministériel, d'une circulaire, d'une directive, d'un règlement UE ou d'un accord international prévoyant un droit, une interdiction ou une obligation.

[3] Coût auquel un destinataire est confronté lorsqu'il répond à une obligation d'information inscrite dans une loi ou un texte d'application de celle-ci (exemple : taxe, coût de salaire, perte de temps ou de congé, coût de déplacement physique, achat de matériel, etc.).

7 a) Le projet prend-il recours à un échange de données inter-administratif (national ou international) plutôt que de demander l'information au destinataire ? ☐ Oui ☒ Non ☐ N.a.

Si oui, de quelle(s) donnée(s) et/ou administration(s) s'agit-il ?

b) Le projet en question contient-il des dispositions spécifiques concernant la protection des personnes à l'égard du traitement des données à caractère personnel [4] ? ☐ Oui ☒ Non ☐ N.a.

Si oui, de quelle(s) donnée(s) et/ou administration(s) s'agit-il ?

[4] Loi modifiée du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel (www.cnpd.lu)

8 Le projet prévoit-il :

- une autorisation tacite en cas de non réponse de l'administration ? ☐ Oui ☐ Non ☒ N.a.
- des délais de réponse à respecter par l'administration ? ☐ Oui ☐ Non ☒ N.a.
- le principe que l'administration ne pourra demander des informations supplémentaires qu'une seule fois ? ☐ Oui ☐ Non ☒ N.a.

9 Y a-t-il une possibilité de regroupement de formalités et/ou de procédures (p.ex. prévues le cas échéant par un autre texte) ? ☐ Oui ☐ Non ☒ N.a.

Si oui, laquelle :

10 En cas de transposition de directives communautaires, le principe « la directive, rien que la directive » est-il respecté ? ☒ Oui ☐ Non ☐ N.a.

Sinon, pourquoi ?

11 Le projet contribue-t-il en général à une :

a) simplification administrative, et/ou à une ☐ Oui ☒ Non

b) amélioration de la qualité réglementaire ? ☐ Oui ☒ Non

Remarques / Observations :

12 Des heures d'ouverture de guichet, favorables et adaptées aux besoins du/des destinataire(s), seront-elles introduites ? ☐ Oui ☐ Non ☒ N.a.

13 Y a-t-il une nécessité d'adapter un système informatique auprès de l'Etat (e-Government ou application back-office) ☐ Oui ☒ Non

Si oui, quel est le délai pour disposer du nouveau système ?

14 Y a-t-il un besoin en formation du personnel de l'administration concernée ? ☐ Oui ☐ Non ☒ N.a.

Si oui, lequel ?

Remarques / Observations :

Egalité des chances

15 Le projet est-il :

- principalement centré sur l'égalité des femmes et des hommes ? ☐ Oui ☒ Non
- positif en matière d'égalité des femmes et des hommes ? ☐ Oui ☒ Non

Si oui, expliquez de quelle manière :

- neutre en matière d'égalité des femmes et des hommes ? ☒ Oui ☐ Non

Si oui, expliquez pourquoi : Il s'agit d'une disposition légale qui s'applique de manière uniforme et sans distinction eu égard au sexe de la personne concernée.

- négatif en matière d'égalité des femmes et des hommes ? ☐ Oui ☒ Non

Si oui, expliquez de quelle manière :

16 Y a-t-il un impact financier différent sur les femmes et les hommes ? ☐ Oui ☒ Non ☐ N.a.

Si oui, expliquez de quelle manière :

Directive « services »

17 Le projet introduit-il une exigence relative à la liberté d'établissement soumise à évaluation [5] ? ☐ Oui ☒ Non ☐ N.a.

Si oui, veuillez annexer le formulaire A, disponible au site Internet du Ministère de l'Economie et du Commerce extérieur :

www.eco.public.lu/attributions/dg2/d_consommation/d_march___int__rieur/Services/index.html

[5] Article 15 paragraphe 2 de la directive « services » (cf. Note explicative, p.10-11)

18 Le projet introduit-il une exigence relative à la libre prestation de services transfrontaliers [6] ? ☐ Oui ☒ Non ☐ N.a.

Si oui, veuillez annexer le formulaire B, disponible au site Internet du Ministère de l'Economie et du Commerce extérieur :

www.eco.public.lu/attributions/dg2/d_consommation/d_march___int__rieur/Services/index.html

[6] Article 16, paragraphe 1, troisième alinéa et paragraphe 3, première phrase de la directive « services » (cf. Note explicative, p.10-11)

CHECK DE DURABILITÉ - NOHALTEGKEETSCHECK

La présente page interactive nécessite au minimum la version 8.1.3 d'Adobe Acrobat® Reader®. La dernière version d'Adobe Acrobat Reader pour tous systèmes (Windows®, Mac, etc.) est téléchargeable gratuitement sur le site de Adobe Systems Incorporated.

Ministre responsable :	La Ministre de la Justice
Projet de loi ou amendement :	Projet de loi portant modification du Code pénal aux fins de la transposition de la directive (UE) 2013/40 du Parlement et du Conseil du 12 août 2013 relative aux attaques visant les systèmes d'information et remplaçant la décision-cadre 2005/222/JAI du Conseil

Le check de durabilité est un outil d'évaluation des actes législatifs par rapport à leur impact sur le developpement durable. Son objectif est de donner l'occasion d'introduire des aspects relatifs au développement durable à un stade préparatoire des projets de loi. Tout en faisant avancer ce thème transversal qu'est le developpement durable, il permet aussi d'assurer une plus grande cohérence politique et une meilleure qualité des textes législatifs.

1. Est-ce que le projet de loi sous rubrique a un impact sur le champ d'action (1-10) du 3ième Plan national pour un développement durable (PNDD) ?
   En cas de réponse négative, expliquez-en succinctement les raisons.
   En cas de réponse positive sous 1., quels seront les effets positifs et/ou négatifs éventuels de cet impact ?

2. Quelles catégories de personnes seront touchées par cet impact ?

3. Quelles mesures sont envisagées afin de pouvoir atténuer les effets négatifs et comment pourront être renforcés les aspects positifs de cet impact ?

Afin de faciliter cet exercice, l'instrument du contrôle de la durabilité est accompagné par des points d'orientation – **auxquels il n'est pas besoin de réagir ou répondre mais qui servent uniquement d'orientation**, ainsi que par une documentation sur les dix champs d'actions précités.

1. Assurer une inclusion sociale et une éducation pour tous. Points d'orientation Documentation ☐ Oui ☒ Non

Le projet de loi a pour unique but d'insérer une circonstance aggravante dans le Code pénal afin de se conformer à la directive UE.

2. Assurer les conditions d'une population en bonne santé. Points d'orientation Documentation ☐ Oui ☒ Non

idem

3. Promouvoir une consommation et une production durables. Points d'orientation Documentation ☐ Oui ☒ Non

idem

4. Diversifier et assurer une économie inclusive et porteuse d'avenir. Points d'orientation Documentation ☐ Oui ☒ Non

idem

5. Planifier et coordonner l'utilisation du territoire. Points d'orientation Documentation ☐ Oui ☒ Non

idem

6. Assurer une mobilité durable. Points d'orientation Documentation ☐ Oui ☒ Non

idem

7. Arrêter la dégradation de notre environnement et respecter les capacités des ressources naturelles. Points d'orientation Documentation ☐ Oui ☒ Non

idem

8. Protéger le climat, s'adapter au changement climatique et assurer une énergie durable. Points d'orientation Documentation ☐ Oui ☒ Non

idem

9. Contribuer, sur le plan global, à l'éradication de la pauvreté et à la cohérence des politiques pour le développement durable. Points d'orientation Documentation ☐ Oui ☒ Non

idem

10. Garantir des finances durables. Points d'orientation Documentation ☐ Oui ☒ Non

idem

Cette partie du formulaire est facultative - Veuillez cocher la case correspondante

En outre, et dans une optique d'enrichir davantage l'analyse apportée par le contrôle de la durabilité, il est proposé de recourir, de manière facultative, à une évaluation de l'impact des mesures sur base d'indicateurs retenus dans le PNDD. Ces indicateurs sont suivis par le STATEC.

Continuer avec l'évaluation ? ☐ Oui ☒ Non

(1) Dans le tableau, choisissez l'évaluation : **non applicable**, ou de 1 = **pas du tout probable** à 5 = **très possible**

DIRECTIVE 2013/40/UE DU PARLEMENT EUROPÉEN ET DU CONSEIL

du 12 août 2013

relative aux attaques contre les systèmes d'information et remplaçant la décision-cadre 2005/222/JAI du Conseil

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

vu le traité sur le fonctionnement de l'Union européenne, et notamment son article 83, paragraphe 1,

vu la proposition de la Commission européenne,

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

vu l'avis du Comité économique et social européen ([1]),

statuant conformément à la procédure législative ordinaire ([2]),

considérant ce qui suit:

(1) La présente directive a pour objectif de rapprocher le droit pénal des États membres dans le domaine des attaques contre les systèmes d'information en fixant des règles minimales concernant la définition des infractions pénales et les sanctions applicables, et de renforcer la coopération entre les autorités compétentes, notamment la police et les autres services spécialisés chargés de l'application de la loi dans les États membres, ainsi que les agences et organes spécialisés compétents de l'Union, tels qu'Eurojust, Europol et son Centre européen de lutte contre la cybercriminalité et l'Agence européenne chargée de la sécurité des réseaux et de l'information (ENISA).

(2) Les systèmes d'information représentent un élément essentiel de l'interaction politique, sociale et économique au sein de l'Union. La société est très dépendante de ce type de systèmes et ce phénomène va croissant. Le bon fonctionnement et la sécurité de ces systèmes au sein de l'Union sont fondamentaux pour le développement du marché intérieur et d'une économie compétitive et innovante. Le fait de garantir un niveau de protection approprié des systèmes d'information devrait faire partie d'un cadre global de mesures de prévention efficaces accompagnant les réponses pénales à la cybercriminalité.

(3) Les attaques contre les systèmes d'information, et en particulier celles liées à la criminalité organisée, constituent une menace croissante au sein de l'Union et à l'échelle mondiale, et l'éventualité d'attaques terroristes ou politiques contre les systèmes d'information qui font partie de l'infrastructure critique des États membres et de l'Union suscite de plus en plus d'inquiétude. Cette situation menace la réalisation d'une société de l'information plus sûre et d'un espace de liberté, de sécurité et de justice, et appelle donc une réaction au niveau de l'Union ainsi qu'une amélioration de la coopération et de la coordination au niveau international.

([1]) JO C 218 du 23.7.2011, p. 130.

([2]) Position du Parlement européen du 4 juillet 2013 (non encore parue au Journal officiel) et décision du Conseil du 22 juillet 2013.

(4) Il existe plusieurs infrastructures critiques dans l'Union, dont l'arrêt ou la destruction aurait un impact transfrontalier significatif. Compte tenu de la nécessité de renforcer la capacité de protection des infrastructures critiques au sein de l'Union, il est devenu manifeste que les mesures de lutte contre les cyberattaques devraient s'accompagner de sanctions pénales sévères, reflétant la gravité de ces attaques. Une infrastructure critique pourrait s'entendre comme un point, un système ou une partie de celui-ci, situé dans des États membres, qui est indispensable au maintien des fonctions vitales de la société, de la santé, de la sûreté, de la sécurité et du bien-être économique ou social des citoyens, comme les centrales électriques, les réseaux de transport et les réseaux publics, et dont l'arrêt ou la destruction aurait un impact significatif dans un État membre du fait de la défaillance de ces fonctions.

(5) On constate une tendance à la perpétration d'attaques à grande échelle de plus en plus dangereuses et récurrentes contre des systèmes d'information qui peuvent souvent être critiques pour les États membres ou pour certaines fonctions du secteur public ou privé. Parallèlement, des méthodes de plus en plus sophistiquées sont mises au point, telles que la création et l'utilisation de «réseaux zombies», qui impliquent une infraction pénale en plusieurs stades, chaque stade pouvant à lui seul menacer gravement les intérêts publics. La présente directive vise, entre autres, à mettre en place des sanctions pénales en ce qui concerne la création de réseaux zombies, c'est-à-dire l'acte d'établir un contrôle à distance d'un nombre important d'ordinateurs en les contaminant au moyen de logiciels malveillants dans le cadre de cyberattaques ciblées. Une fois créé, le réseau d'ordinateurs contaminés qui constitue le réseau zombie peut être activé à l'insu des utilisateurs des ordinateurs dans le but de lancer une cyberattaque à grande échelle, qui est en général à même de causer un grave préjudice, comme indiqué dans la présente directive. Les États membres peuvent déterminer, en fonction de leur droit national et de leur pratique nationale, ce qui constitue un préjudice grave, comme le fait d'arrêter des services de réseau présentant un intérêt public important, ou de causer des coûts financiers majeurs ou la perte de données à caractère personnel ou d'informations sensibles.

(6) Des cyberattaques à grande échelle sont susceptibles de provoquer des dommages économiques notables, tant du fait de l'interruption des systèmes d'information et des communications qu'en raison de la perte ou de l'altération d'informations confidentielles importantes d'un point de vue commercial ou d'autres données. Il y a lieu en particulier de veiller à sensibiliser les petites et moyennes entreprises innovantes aux menaces liées à ces attaques et à leur vulnérabilité à cet égard, en raison de leur dépendance accrue à l'égard du bon fonctionnement et de la disponibilité des systèmes d'information et de leurs ressources limitées en matière de sécurité de l'information.

(7) Des définitions communes dans ce domaine sont importantes pour garantir une approche cohérente des États membres quant à l'application de la présente directive.

(8) Il est nécessaire d'adopter une approche commune en ce qui concerne les éléments constitutifs des infractions pénales en instituant des infractions communes d'accès illégal à un système d'information, d'atteinte illégale à l'intégrité d'un système, d'atteinte illégale à l'intégrité des données et d'interception illégale.

(9) L'interception comprend, sans que cette liste soit limitative, l'écoute, le contrôle ou la surveillance du contenu des communications et l'obtention du contenu des données, soit directement, au moyen de l'accès aux systèmes d'information et de leur utilisation, soit indirectement, au moyen de l'utilisation de dispositifs d'écoute électroniques ou de dispositifs d'écoute par des moyens techniques.

(10) Les États membres devraient prévoir des sanctions en ce qui concerne les attaques contre les systèmes d'information. Ces sanctions devraient être effectives, proportionnées et dissuasives et devraient comprendre des peines d'emprisonnement et/ou des amendes.

(11) La présente directive prévoit des sanctions pénales, au moins dans les cas où les faits ne sont pas mineurs. Les États membres peuvent déterminer, en fonction du droit national et de la pratique nationale, ce qui constitue un fait mineur. On peut considérer qu'un fait est mineur, par exemple, lorsque les dommages causés par l'infraction et/ou le risque pour les intérêts publics ou privés, tels que le risque pour l'intégrité d'un système informatique ou de données informatiques, ou pour l'intégrité, les droits ou les autres intérêts d'une personne, sont peu importants ou de nature telle qu'il n'est pas nécessaire d'appliquer une sanction pénale dans les limites du seuil légal ou que la responsabilité pénale soit engagée.

(12) La détection et la notification des menaces et des risques liés aux cyberattaques, ainsi que de la vulnérabilité des systèmes d'information à cet égard, sont des éléments pertinents pour prévenir les cyberattaques et y répondre de manière efficace, et pour améliorer la sécurité des systèmes d'information. Prévoir des mesures incitant à notifier les failles en matière de sécurité pourrait y contribuer. Les États membres devraient s'efforcer de prévoir les possibilités de détecter et de notifier de manière légale des failles en matière de sécurité.

(13) Il y a lieu de prévoir des sanctions plus sévères lorsque l'attaque contre un système d'information est commise par une organisation criminelle, telle que définie dans la décision-cadre 2008/841/JAI du Conseil du 24 octobre 2008 relative à la lutte contre la criminalité organisée ([1]), lorsqu'une cyberattaque est menée à grande échelle, affectant ainsi un grand nombre de systèmes d'information, y compris lorsque l'attaque a pour objectif de créer un réseau zombie, ou lorsqu'une cyberattaque cause un préjudice grave, y compris lorsqu'elle est menée via un réseau zombie. Il y a également lieu de prévoir des sanctions plus sévères lorsqu'une attaque est menée contre une infrastructure critique des États membres ou de l'Union.

([1]) JO L 300 du 11.11.2008, p. 42.

(14) La mise en place de mesures efficaces contre l'usurpation d'identité et d'autres infractions liées à l'identité constitue un autre élément important d'une approche intégrée contre la cybercriminalité. La nécessité de mener une action au niveau de l'Union contre ce type de comportement criminel pourrait également être envisagée dans le cadre de l'évaluation de la nécessité de disposer d'un instrument horizontal global au niveau de l'Union.

(15) Dans ses conclusions des 27 et 28 novembre 2008, le Conseil a indiqué qu'il convenait que les États membres et la Commission définissent une nouvelle stratégie, en prenant en considération le contenu de la convention du Conseil de l'Europe de 2001 sur la cybercriminalité. Cette convention est le cadre juridique de référence pour la lutte contre la cybercriminalité, y compris les attaques contre les systèmes d'information. La présente directive s'en inspire. Il faudrait se donner pour priorité d'achever, le plus rapidement possible, le processus de ratification de cette convention par tous les États membres.

(16) Compte tenu des différentes façons dont les attaques peuvent être menées et de l'évolution rapide des équipements et des logiciels, la présente directive fait référence à des outils qui peuvent être utilisés pour commettre les infractions prévues dans la présente directive. Ces outils pourraient comprendre des logiciels malveillants, notamment ceux qui sont capables de créer des réseaux zombies, utilisés pour lancer des cyberattaques. Même si cet outil est adapté ou particulièrement adapté pour commettre l'une des infractions prévues dans la présente directive, il se peut qu'il ait été produit à des fins légitimes. Dès lors qu'il faut éviter d'ériger en infractions la production et la commercialisation de ces outils à des fins légitimes, par exemple pour tester la fiabilité de produits relevant des technologies de l'information ou la sécurité des systèmes d'information, il faut, pour qu'il y ait infraction, outre une intention générale, une intention spécifique d'utiliser ces outils afin de commettre l'une ou plusieurs des infractions prévues dans la présente directive.

(17) La présente directive n'impose pas de responsabilité pénale lorsque les critères objectifs constitutifs des infractions mentionnées dans la présente directive sont remplis, mais que les actes sont commis sans intention délictueuse, par exemple lorsqu'une personne ne sait pas que l'accès n'était pas autorisé ou dans le cas d'interventions obligatoires visant à tester ou à protéger un système d'information, par exemple lorsqu'une personne est chargée par une entreprise ou un vendeur de tester la résistance de son système de sécurité. Dans le cadre de la présente directive, les obligations contractuelles ou les conventions visant à limiter l'accès à des systèmes d'information par des conditions d'utilisation ou des conditions générales, ainsi que les conflits du travail concernant l'accès aux systèmes d'information d'un employeur et leur utilisation à des fins privées ne devraient pas engager de responsabilité pénale lorsque l'accès effectué dans ces conditions serait réputé non autorisé et constituerait donc la seule motivation des poursuites pénales. La présente directive est sans préjudice du droit d'accès à l'information tel que déterminé par le droit national et le droit de l'Union, et ne peut pas non plus servir pour justifier un accès illicite ou arbitraire à l'information.

(18) Les cyberattaques seraient susceptibles d'être facilitées par diverses circonstances, comme lorsque l'auteur a accès, dans le cadre de son activité professionnelle, aux systèmes de sécurité internes des systèmes d'information affectés. Dans le cadre du droit national, de telles circonstances devraient être prises en considération au cours des poursuites pénales, le cas échéant.

(19) Les États membres devraient prévoir des circonstances aggravantes, dans leur droit national, conformément aux règles applicables établies en la matière par leur système juridique. Ils devraient veiller à ce que les juges puissent tenir compte de ces circonstances aggravantes lorsqu'ils prononcent une condamnation à l'encontre des auteurs d'infractions. Il relève de l'appréciation du juge d'évaluer ces circonstances avec les autres faits du cas considéré.

(20) La présente directive ne régit pas les conditions devant être remplies afin d'exercer une compétence à l'égard d'une des infractions qui y sont visées, telles qu'une déclaration de la victime sur le lieu de l'infraction, une dénonciation émanant de l'État du lieu où l'infraction a été commise, ou le fait que l'auteur de l'infraction n'ait pas fait l'objet de poursuites là où l'infraction a été commise.

(21) Dans le cadre de la présente directive, les États et les entités publiques restent pleinement tenus de garantir le respect des droits de l'homme et des libertés fondamentales, conformément aux obligations internationales existantes.

(22) La présente directive renforce l'importance des réseaux, tels que le réseau de points de contact du G8 ou celui du Conseil de l'Europe, disponibles vingt-quatre heures sur vingt-quatre et sept jours sur sept. Ces points de contact devraient donc pouvoir fournir une assistance effective, par exemple faciliter l'échange d'informations disponibles pertinentes et la fourniture de conseils techniques ou d'informations juridiques aux fins des enquêtes ou des procédures portant sur des infractions pénales concernant des systèmes d'information et des données connexes impliquant l'État membre demandeur. Afin de garantir le bon fonctionnement des réseaux, chaque point de contact devrait être en mesure d'entrer rapidement en communication avec le point de contact d'un autre État membre, selon une procédure accélérée en s'appuyant, entre autres, sur un personnel formé et équipé. Compte tenu de la rapidité avec laquelle des cyberattaques à grande échelle peuvent être menées, il conviendrait que les États membres soient en mesure de répondre promptement aux demandes urgentes émanant de ce réseau de points de contact. Dans pareils cas, il serait souhaitable que la demande d'informations s'accompagne d'un contact téléphonique afin de s'assurer que la demande est traitée rapidement par l'État membre auquel elle est adressée et qu'une réponse est apportée dans un délai de huit heures.

(23) La coopération entre les pouvoirs publics, d'un côté, et le secteur privé et la société civile, de l'autre, est essentielle pour prévenir les attaques contre les systèmes d'information et lutter contre celles-ci. Il est nécessaire de favoriser et d'améliorer la coopération entre les prestataires de services, les producteurs, les organismes chargés de l'application de la loi et les autorités judiciaires, tout en respectant pleinement l'état de droit. Cette coopération pourrait comprendre l'appui des prestataires de services pour aider à préserver des preuves éventuelles, fournir des éléments permettant d'identifier les auteurs d'infractions et, en dernier recours, fermer, totalement ou en partie, conformément au droit national et à la pratique nationale, les systèmes d'information ou les fonctions qui ont été compromis ou utilisés à des fins illégales. Les États membres devraient également envisager de mettre en place des réseaux de coopération et de partenariat avec les prestataires de service et les producteurs pour permettre l'échange d'informations relatives aux infractions relevant du champ d'application de la présente directive.

(24) Il est nécessaire de recueillir des données comparables sur les infractions prévues dans la présente directive. Des données pertinentes devraient être mises à la disposition des agences et organes spécialisés compétents de l'Union, comme Europol et ENISA, en fonction de leurs missions et de leurs besoins en information, afin d'avoir une vision plus complète du problème de la cybercriminalité et du niveau de sécurité des réseaux et de l'information au niveau de l'Union et de permettre ainsi de formuler une réponse plus efficace. Les États membres devraient transmettre à Europol et à son Centre européen de lutte contre la cybercriminalité des informations sur le mode opératoire des auteurs d'infractions, afin que ces agences puissent établir des évaluations de la menace et des analyses stratégiques en matière de cybercriminalité, conformément à la décision 2009/371/JAI du Conseil du 6 avril 2009 portant création de l'Office européen de police (Europol) ([1]). La communication d'informations peut aider à mieux comprendre les menaces actuelles et futures et contribuer ainsi à ce que des décisions plus appropriées et mieux ciblées soient prises pour combattre et prévenir les attaques contre les systèmes d'information.

(25) La Commission devrait présenter un rapport sur l'application de la présente directive et faire les propositions législatives nécessaires, susceptibles de mener à un élargissement de son champ d'application, en prenant en compte les évolutions dans le domaine de la cybercriminalité. Au nombre de ces évolutions pourraient figurer les progrès technologiques, par exemple ceux permettant une exécution des lois plus efficace dans le domaine des attaques contre les systèmes d'information ou facilitant la prévention ou limitant l'impact de telles attaques. À cette fin, la Commission devrait prendre en considération les analyses et les rapports disponibles établis par les acteurs compétents, en particulier Europol et ENISA.

(26) Afin de lutter efficacement contre la cybercriminalité, il est nécessaire de renforcer la résistance des systèmes d'information en prenant des mesures appropriées pour les protéger de manière plus efficace contre les cyberattaques. Les États membres devraient prendre les mesures nécessaires pour protéger leurs infrastructures critiques contre les cyberattaques, et examiner à cette occasion la protection de leurs systèmes d'information et des données qu'ils contiennent. Le fait que les personnes morales assurent un niveau adéquat de protection et de sécurité des systèmes d'information, par exemple lors de la fourniture de services de communications électroniques accessibles au public, conformément à la législation de l'Union en vigueur en matière de vie privée et de

([1]) JO L 121 du 15.5.2009, p. 37.

protection des communications électroniques et des données, est un élément essentiel d'une approche globale visant à lutter efficacement contre la cybercriminalité. Il convient de garantir des niveaux de protection appropriés contre les menaces et les vulnérabilités pouvant être raisonnablement identifiées en l'état des connaissances dans certains secteurs et compte tenu des situations spécifiques de traitement des données. Les coûts et charges liés à cette protection devraient être proportionnels au préjudice éventuel qu'une cyberattaque pourrait causer à ceux concernés. Les États membres sont encouragés à prévoir, dans le cadre de leur droit national, des mesures pertinentes permettant d'engager la responsabilité des personnes morales, lorsque celles-ci n'ont de toute évidence pas assuré un niveau de protection suffisant contre les cyberattaques.

(27) L'existence de lacunes et de différences importantes dans les législations et les procédures pénales des États membres en matière d'attaques contre les systèmes d'information risque d'entraver la lutte contre la criminalité organisée et le terrorisme, et de compliquer la coopération policière et judiciaire dans ce domaine. Les systèmes d'information modernes ayant un caractère transnational et ne connaissant pas de frontières, les attaques lancées contre eux ont une dimension transfrontière qui met en lumière la nécessité de prendre d'urgence des mesures complémentaires pour rapprocher le droit pénal dans ce domaine. Par ailleurs, il convient de faciliter la coordination des poursuites judiciaires dans les affaires relatives à des attaques contre des systèmes d'information par la mise en œuvre et l'application appropriées de la décision-cadre 2009/948/JAI du Conseil du 30 novembre 2009 relative à la prévention et au règlement des conflits en matière d'exercice de la compétence dans le cadre des procédures pénales ([1]). Les États membres, en coopération avec l'Union, devraient également chercher à améliorer la coopération internationale en matière de sécurité des systèmes d'information, des réseaux informatiques et des données informatiques. Il convient de prendre dûment en considération la sécurité du transfert et du stockage des données dans tout accord international impliquant l'échange de données.

(28) Il est essentiel d'améliorer la coopération entre les services compétents chargés de l'application de la loi et les autorités judiciaires à travers l'Union pour pouvoir lutter efficacement contre la cybercriminalité. Dans ce contexte, il convient d'encourager l'intensification des efforts visant à offrir une formation adaptée aux autorités compétentes, de manière qu'elles comprennent mieux la cybercriminalité et son impact et à favoriser la coopération et l'échange de bonnes pratiques, par exemple via les agences et organes spécialisés compétents de l'Union. Cette formation devrait notamment viser à mieux faire connaître les différents systèmes juridiques nationaux, les éventuels défis juridiques et techniques qui se présentent dans les enquêtes pénales et la répartition des compétences entre les autorités nationales compétentes.

(29) La présente directive respecte les droits de l'homme et les libertés fondamentales et est conforme aux principes consacrés en particulier par la Charte des droits fondamentaux de l'Union européenne et la convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales, notamment la protection des données à caractère personnel, le droit au respect de la vie privée, la liberté d'expression et d'information, le droit à un procès équitable, la présomption d'innocence et les droits de la défense, ainsi que les principes de légalité et de proportionnalité des infractions et sanctions pénales. La présente directive tend en particulier à garantir le plein respect de ces droits et principes et doit être mise en œuvre en conséquence.

(30) La protection des données à caractère personnel est un droit fondamental en vertu de l'article 16, paragraphe 1, du traité sur le fonctionnement de l'Union européenne, et de l'article 8 de la Charte des droits fondamentaux de l'Union européenne. Par conséquent, tout traitement de données à caractère personnel effectué dans le cadre de la mise en œuvre de la présente directive devrait être conforme au droit de l'Union en matière de protection des données.

(31) Conformément à l'article 3 du protocole sur la position du Royaume-Uni et de l'Irlande à l'égard de l'espace de liberté, de sécurité et de justice, annexé au traité sur l'Union européenne et au traité sur le fonctionnement de l'Union européenne, ces États membres ont notifié leur souhait de participer à l'adoption et à l'application de la présente directive.

(32) Conformément aux articles 1er et 2 du protocole sur la position du Danemark annexé au traité sur l'Union européenne et au traité sur le fonctionnement de l'Union européenne, le Danemark ne participe pas à l'adoption de la présente directive et n'est pas lié par celle-ci ni soumis à son application.

(33) Étant donné que les objectifs de la présente directive, à savoir rendre les attaques contre des systèmes d'information, dans tous les États membres, passibles de sanctions pénales effectives, proportionnées et dissuasives, et améliorer et favoriser la coopération judiciaire, entre les autorités judiciaires et les autres autorités compétentes, ne peuvent être atteints de manière suffisante par les États membres et peuvent donc, en raison de leurs dimensions ou de leurs effets, être mieux atteints au niveau de l'Union, celle-ci peut prendre des mesures conformément au principe de subsidiarité consacré à l'article 5 du traité sur l'Union européenne. Conformément au principe de proportionnalité tel qu'énoncé audit article, la présente directive n'excède pas ce qui est nécessaire pour atteindre ces objectifs.

(34) La présente directive vise à modifier et à étendre les dispositions de la décision-cadre 2005/222/JAI du Conseil du 24 février 2005 relative aux attaques visant les systèmes d'information ([2]). Puisque les modifications à faire sont significatives par leur nombre comme par leur nature, il convient, pour plus de clarté, de remplacer entièrement la décision-cadre 2005/222/JAI à l'égard des États membres qui participent à l'adoption de la présente directive,

([1]) JO L 328 du 15.12.2009, p. 42.

([2]) JO L 69 du 16.3.2005, p. 67.

ONT ADOPTÉ LA PRÉSENTE DIRECTIVE:

Article premier

Objet

La présente directive fixe des règles minimales concernant la définition des infractions pénales et les sanctions en matière d'attaques contre les systèmes d'information. Elle vise également à faciliter la prévention de ces infractions et à améliorer la coopération entre les autorités judiciaires et les autres autorités compétentes.

Article 2

Définitions

Aux fins de la présente directive, on entend par:

a) «système d'information»: un dispositif isolé ou un ensemble de dispositifs interconnectés ou apparentés, qui assure ou dont un ou plusieurs éléments assurent, en exécution d'un programme, un traitement automatisé de données informatiques, ainsi que les données informatiques stockées, traitées, récupérées ou transmises par ce dispositif ou cet ensemble de dispositifs en vue du fonctionnement, de l'utilisation, de la protection et de la maintenance de celui-ci;

b) «données informatiques»: une représentation de faits, d'informations ou de concepts sous une forme qui se prête à un traitement informatique, y compris un programme de nature à faire en sorte qu'un système d'information exécute une fonction;

c) «personne morale»: une entité à laquelle le droit en vigueur reconnaît le statut de personne morale, à l'exception des États ou des entités publiques agissant dans l'exercice de prérogatives de puissance publique, ou des organisations internationales relevant du droit public;

d) «sans droit»: un comportement visé dans la présente directive, y compris un accès, une atteinte à l'intégrité ou une interception, qui n'est pas autorisé par le propriétaire du système ou d'une partie du système ou un autre titulaire de droits sur celui-ci ou une partie de celui-ci, ou n'est pas permis par le droit national.

Article 3

Accès illégal à des systèmes d'information

Les États membres prennent les mesures nécessaires pour ériger en infraction pénale punissable l'accès sans droit, lorsqu'il est intentionnel, à tout ou partie d'un système d'information, lorsque l'acte est commis en violation d'une mesure de sécurité, au moins lorsqu'il ne s'agit pas de cas mineurs.

Article 4

Atteinte illégale à l'intégrité d'un système

Les États membres prennent les mesures nécessaires pour ériger en infraction pénale punissable le fait de provoquer une perturbation grave ou une interruption du fonctionnement d'un système d'information, en introduisant, en transmettant, en endommageant, en effaçant, en détériorant, en altérant, en supprimant ou en rendant inaccessibles des données informatiques lorsque l'acte est commis de manière intentionnelle et sans droit, au moins lorsqu'il ne s'agit pas de cas mineurs.

Article 5

Atteinte illégale à l'intégrité des données

Les États membres prennent les mesures nécessaires pour ériger en infraction pénale punissable le fait d'effacer, d'endommager, de détériorer, d'altérer, de supprimer ou de rendre inaccessibles des données informatiques d'un système d'information lorsque l'acte est commis de manière intentionnelle et sans droit, au moins lorsqu'il ne s'agit pas de cas mineurs.

Article 6

Interception illégale

Les États membres prennent les mesures nécessaires pour ériger en infraction pénale punissable l'interception, effectuée par des moyens techniques, de transmissions non publiques de données informatiques à destination, en provenance ou à l'intérieur d'un système d'information, y compris les émissions électromagnétiques provenant d'un système d'information transportant de telles données informatiques, lorsque l'acte est commis de manière intentionnelle et sans droit, au moins lorsqu'il ne s'agit pas de cas mineurs.

Article 7

Outils utilisés pour commettre les infractions

Les États membres prennent les mesures nécessaires pour ériger en infraction pénale punissable la production, la vente, l'obtention pour utilisation, l'importation, la diffusion ou d'autres formes de mise à disposition intentionnelles d'un des outils suivants lorsque l'acte est commis sans droit et dans l'intention de l'utiliser pour commettre l'une des infractions visées aux articles 3 à 6, au moins lorsqu'il ne s'agit pas de cas mineurs:

a) un programme informatique, principalement conçu ou adapté pour permettre la commission de l'une des infractions visées aux articles 3 à 6;

b) un mot de passe, un code d'accès ou des données informatiques similaires permettant d'accéder à tout ou partie d'un système d'information.

Article 8

Incitation, participation et complicité, et tentative

1. Les États membres veillent à ériger en infraction pénale punissable le fait d'inciter à commettre l'une des infractions visées aux articles 3 à 7, d'y participer ou de s'en rendre complice.

2. Les États membres veillent à ériger en infraction pénale punissable la tentative de commettre une infraction visée aux articles 4 et 5.

Article 9

Sanctions

1. Les États membres prennent les mesures nécessaires pour faire en sorte que les infractions visées aux articles 3 à 8 soient passibles de sanctions pénales effectives, proportionnées et dissuasives.

2. Les États membres prennent les mesures nécessaires pour faire en sorte que les infractions visées aux articles 3 à 7 soient passibles d'une peine d'emprisonnement maximale d'au moins deux ans, au moins lorsqu'il ne s'agit pas de cas mineurs.

3. Les États membres prennent les mesures nécessaires pour faire en sorte que les infractions visées aux articles 4 et 5 soient

passibles d'une peine d'emprisonnement maximale d'au moins trois ans lorsqu'elles sont commises de manière intentionnelle et qu'un nombre important de systèmes d'information est atteint au moyen d'un des outils visés à l'article 7.

4. Les États membres prennent les mesures nécessaires pour faire en sorte que les infractions visées aux articles 4 et 5 soient passibles d'une peine d'emprisonnement maximale d'au moins cinq ans dans les cas où:

a) elles sont commises dans le cadre d'une organisation criminelle telle que définie dans la décision-cadre 2008/841/JAI, indépendamment de la sanction qui y est prévue; ou

b) elles causent un préjudice grave; ou

c) elles sont commises contre un système d'information d'une infrastructure critique.

5. Les États membres prennent les mesures nécessaires pour que, lorsque les infractions visées aux articles 4 et 5 sont commises par l'utilisation abusive des données à caractère personnel d'une autre personne, en vue de gagner la confiance d'une tierce partie, causant ainsi un préjudice au propriétaire légitime de l'identité, ces éléments puissent, conformément au droit national, être considérés comme des circonstances aggravantes, à moins que ces circonstances ne soient déjà couvertes par une autre infraction punissable en vertu du droit national.

Article 10

Responsabilité des personnes morales

1. Les États membres prennent les mesures nécessaires pour que les personnes morales puissent être tenues pour responsables des infractions visées aux articles 3 à 8, lorsqu'elles sont commises pour leur compte par toute personne agissant soit individuellement, soit en tant que membre d'un organe de la personne morale en cause, et qui exerce un pouvoir de direction en son sein fondé sur:

a) un pouvoir de représentation de la personne morale;

b) une autorité pour prendre des décisions au nom de la personne morale;

c) une autorité pour exercer un contrôle au sein de la personne morale.

2. Les États membres prennent les mesures nécessaires pour s'assurer que les personnes morales puissent être tenues pour responsables lorsque l'absence de surveillance ou de contrôle de la part d'une personne visée au paragraphe 1 a rendu possible la commission de l'une des infractions visées aux articles 3 à 8 pour le compte de ladite personne morale, par une personne soumise à son autorité.

3. La responsabilité des personnes morales au titre des paragraphes 1 et 2 n'exclut pas les poursuites pénales contre les personnes physiques auteurs, instigatrices ou complices de l'une des infractions visées aux articles 3 à 8.

Article 11

Sanctions à l'encontre des personnes morales

1. Les États membres prennent les mesures nécessaires pour qu'une personne morale déclarée responsable au titre de l'article 10, paragraphe 1, soit passible de sanctions effectives, proportionnées et dissuasives, qui incluent des amendes pénales ou non pénales, et éventuellement d'autres sanctions, telles que:

a) l'exclusion du bénéfice d'un avantage ou d'une aide publics;

b) l'interdiction temporaire ou définitive d'exercer une activité commerciale;

c) le placement sous surveillance judiciaire;

d) une mesure judiciaire de dissolution;

e) la fermeture temporaire ou définitive d'établissements ayant servi à commettre l'infraction.

2. Les États membres prennent les mesures nécessaires pour qu'une personne morale déclarée responsable au titre de l'article 10, paragraphe 2, soit passible de sanctions ou d'autres mesures effectives, proportionnées et dissuasives.

Article 12

Compétence

1. Les États membres établissent leur compétence à l'égard des infractions visées aux articles 3 à 8, lorsque l'infraction a été commise:

a) en tout ou en partie sur leur territoire; ou

b) par un de leurs ressortissants, au moins dans les cas où l'acte constitue une infraction là où il a été commis.

2. Lorsqu'il établit sa compétence conformément au paragraphe 1, point a), un État membre veille à être compétent lorsque:

a) l'auteur de l'infraction a commis celle-ci alors qu'il était physiquement présent sur son territoire, que l'infraction vise un système d'information situé sur son territoire ou non; ou

b) l'infraction vise un système d'information situé sur son territoire, que l'auteur de l'infraction soit physiquement présent sur son territoire ou non lors de la commission de l'infraction.

3. Un État membre informe la Commission de sa décision d'établir sa compétence à l'égard des infractions visées aux articles 3 à 8 qui ont été commises en dehors de son territoire, notamment dans les cas suivants:

a) l'auteur de l'infraction réside habituellement sur son territoire; ou

b) l'infraction a été commise pour le compte d'une personne morale établie sur son territoire.

Article 13

Échange d'informations

1. Aux fins de l'échange d'informations relatives aux infractions visées aux articles 3 à 8, les États membres veillent à disposer d'un point de contact national opérationnel et à recourir au réseau existant de points de contact opérationnels, disponibles vingt-quatre heures sur vingt-quatre et sept jours sur sept. Les États membres veillent également à mettre en place des procédures afin que, en cas de demandes urgentes d'assistance, l'autorité compétente indique, dans un délai de huit heures à compter de la réception de la demande, au moins si la demande sera satisfaite, et la forme et le délai estimé pour cette réponse.

2. Les États membres communiquent à la Commission le point de contact visé au paragraphe 1 qu'ils ont désigné. La Commission transmet ces informations aux autres États membres et aux agences et organes spécialisés compétents de l'Union.

3. Les États membres prennent les mesures nécessaires pour faire en sorte que des canaux de communication appropriés soient mis à disposition afin de faciliter la notification sans retard indu aux autorités nationales compétentes des infractions visées aux articles 3 à 6.

Article 14

Suivi et statistiques

1. Les États membres veillent à mettre en place un système d'enregistrement, de production et de communication de statistiques sur les infractions visées aux articles 3 à 7.

2. Les statistiques visées au paragraphe 1 portent, au minimum, sur les données existantes concernant le nombre d'infractions visées aux articles 3 à 7 enregistrées par les États membres, ainsi que le nombre de personnes poursuivies et condamnées pour les infractions visées aux articles 3 à 7.

3. Les États membres transmettent à la Commission les données recueillies en vertu du présent article. La Commission veille à ce qu'un état consolidé des rapports statistiques soit publié et soumis aux agences et organes spécialisés compétents de l'Union.

Article 15

Remplacement de la décision-cadre 2005/222/JAI

La décision-cadre 2005/222/JAI est remplacée à l'égard des États membres qui participent à l'adoption de la présente directive, sans préjudice des obligations des États membres concernant le délai de transposition de la décision-cadre en droit national.

À l'égard des États membres participant à l'adoption de la présente directive, les références faites à la décision-cadre 2005/222/JAI s'entendent comme faites à la présente directive.

Article 16

Transposition

1. Les États membres mettent en vigueur les dispositions législatives, réglementaires et administratives nécessaires pour se conformer à la présente directive, au plus tard le 4 septembre 2015.

2. Les États membres communiquent à la Commission le texte des dispositions transposant dans leur droit national les obligations que leur impose la présente directive.

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

Article 17

Rapports

La Commission présente au Parlement européen et au Conseil, au plus tard le 4 septembre 2017, un rapport évaluant dans quelle mesure les États membres ont pris les dispositions nécessaires pour se conformer à la présente directive, accompagné, le cas échéant, de propositions législatives. La Commission tient également compte des évolutions techniques et juridiques dans le domaine de la cybercriminalité, en particulier au regard du champ d'application de la présente directive.

Article 18

Entrée en vigueur

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

Article 19

Destinataires

Les États membres sont destinataires de la présente directive conformément aux traités.

Fait à Bruxelles, le 12 août 2013.

Par le Parlement européen	*Par le Conseil*
Le président	*Le président*
M. SCHULZ	L. LINKEVIČIUS

Impression: CTIE – Division Imprimés et Fournitures de bureau

8316/01

Nº 8316[1]

CHAMBRE DES DEPUTES

PROJET DE LOI

portant modification du Code pénal aux fins de la transposition de la directive (UE) 2013/40 du Parlement et du Conseil du 12 août 2013 relative aux attaques visant les systèmes d'information et remplaçant la décision-cadre 2005/222/JAI du Conseil

* * *

AVIS DU CONSEIL D'ETAT

(24.10.2023)

En vertu de l'arrêté du 28 septembre 2023 du Premier ministre, ministre d'État, le Conseil d'État a été saisi pour avis du projet de loi sous rubrique, élaboré par la ministre de la Justice.

Le texte du projet de loi était accompagné d'un exposé des motifs, d'un commentaire de l'article unique, d'une fiche financière, d'une fiche d'évaluation d'impact, d'un « check de durabilité », de la directive 2013/40/UE qu'il s'agit de transposer et d'un texte coordonné, par extraits, du Code pénal qu'il s'agit de modifier.

Il ne ressort ni de la saisine du Conseil d'État, ni du dossier lui soumis que les chambres professionnelles et organes consultatifs le cas échéant légalement compétents ont été demandés en leur avis

*

CONSIDERATIONS GENERALES

Le projet de loi sous avis a pour objet de parfaire la transposition en droit national de la directive 2013/40/UE du Parlement européen et du Conseil du 12 août 2013 relative aux attaques contre les systèmes d'information et remplaçant la décision cadre 2005/222/JAI du Conseil.

Cette directive a fait l'objet d'une transposition par la loi du 18 juillet 2014 portant 1) approbation de la Convention du Conseil de l'Europe sur la cybercriminalité ouverte à la signature à Budapest le 23 novembre 2001, 2) approbation du Protocole additionnel à la Convention sur la cybercriminalité, relatif à l'incrimination d'actes de nature raciste et xénophobe commis par le biais de systèmes informatiques, fait à Strasbourg le 28 janvier 2003, 3) modification du Code pénal, 4) modification du Code d'instruction criminelle, 5) modification de la loi modifiée du 30 mai 2005 concernant la protection de la vie privée dans le secteur des communications électroniques.

Or, et ainsi que l'indiquent les auteurs du projet de loi sous avis dans leur exposé des motifs, « dans le cadre de l'évaluation de conformité de transposition en droit national de la directive 2013/40/UE, la Commission européenne a estimé que le Luxembourg n'a pas correctement transposé certaines dispositions de ladite directive ». La Commission européenne a considéré, en particulier, « que le Luxembourg n'avait pas correctement transposé dans sa législation nationale l'article 9, paragraphe 4 de la directive qui impose aux États membres de prendre les mesures nécessaires pour que les infractions d'atteinte à l'intégrité d'un système d'information et d'atteinte à l'intégrité des données, prévues aux articles 4 et 5 de la directive, soient passibles d'une peine d'emprisonnement maximale d'au moins cinq ans lorsqu'elles sont commises dans le cadre d'une organisation criminelle, qu'elles causent un préjudice grave ou qu'elles sont commises contre un système d'information d'une infrastructure critique ».

Le projet de loi sous avis entend dès lors répondre à cette critique en élargissant le champ d'application matériel de ces infractions.

*

EXAMEN DE L'ARTICLE UNIQUE

Sans observation.

*

OBSERVATIONS D'ORDRE LEGISTIQUE

Intitulé

Lorsqu'un acte est cité, il faut veiller à reproduire son intitulé tel que publié officiellement. Partant, le Conseil d'État suggère de reformuler l'intitulé de la loi en projet sous revue comme suit :

> « Projet de loi portant modification du Code pénal en vue de la transposition de la directive ~~(UE)~~ 2013/40/UE du Parlement et du Conseil du 12 août 2013 relative aux attaques visant les systèmes d'information et remplaçant la décision-cadre 2005/222/JAI du Conseil ».

Ainsi délibéré en séance plénière et adopté à l'unanimité des 18 votants, le 24 octobre 2023.

Le Secrétaire général, — *Le Président,*

Marc BESCH — Christophe SCHILTZ

Impression: CTIE – Division Imprimés et Fournitures de bureau

03

Chambre des Députés
GRAND-DUCHÉ DE LUXEMBOURG

CL/CSC P.V. JUST 03

Commission de la Justice

Procès-verbal de la réunion du 21 décembre 2023

Ordre du jour :

1. 8287 Projet de loi portant modification de la loi modifiée du 17 mars 2004 relative au mandat d'arrêt européen et aux procédures de remise entre Etats membres de l'Union européenne

   - Désignation d'un rapporteur
   - Présentation du projet de loi et examen des articles
   - Examen de l'avis du Conseil d'Etat
   - Echange de vues

2. 8316 Projet de loi portant modification du Code pénal aux fins de la transposition de la directive (UE) 2013/40 du Parlement et du Conseil du 12 août 2013 relative aux attaques visant les systèmes d'information et remplaçant la décision-cadre 2005/222/JAI du Conseil

   - Désignation d'un rapporteur
   - Présentation du projet de loi et examen des articles
   - Examen de l'avis du Conseil d'Etat
   - Echange de vues

3. 8053 Projet de loi modifiant
   1) La loi modifiée du 10 août 1915 sur les sociétés commerciales
   2) La loi modifiée du 19 décembre 2002 concernant le registre de commerce et des sociétés ainsi que la comptabilité et les comptes annuels des entreprises aux fins de transposer la Directive (UE) 2019/2121 du Parlement européen et du Conseil du 27 novembre 2019 modifiant la directive (UE) 2017/1132 en ce qui concerne les transformations, fusions et scissions transfrontalières

   - Désignation d'un rapporteur
   - Présentation du projet de loi et examen des articles

4. 7881 Projet de loi sur les échanges d'informations relatives aux ressortissants de pays tiers à l'Union européenne ainsi que le système européen d'information sur les casiers judiciaires (ECRIS) portant :
   1° transposition de la directive (UE) 2019/884 du Parlement européen et du Conseil du 17 avril 2019 modifiant la décision-cadre 2009/315/JAI du Conseil en ce qui concerne les échanges d'informations relatives aux ressortissants de pays tiers ainsi que le système européen d'information sur les casiers judiciaires (ECRIS), et remplaçant la décision 2009/316/JAI du Conseil ;
   2° mise en œuvre du règlement (UE) 2019/816 du Parlement européen et du

Conseil du 17 avril 2019 portant création d'un système centralisé permettant d'identifier les États membres détenant des informations relatives aux condamnations concernant des ressortissants de pays tiers et des apatrides, qui vise à compléter le système européen d'information sur les casiers judiciaires, et modifiant le règlement (UE) 2018/1726 ;
3° modification de la loi modifiée du 29 mars 2013 relative à l'organisation du casier judiciaire
- Rapporteur : M. Charles Margue

- Changement de rapporteur
- Examen de l'avis du Conseil d'Etat
- Continuation des travaux

5. 8326 Projet de loi portant sur l'information des représentants légaux des mineurs privés de liberté

- Désignation d'un rapporteur
- Présentation du projet de loi et examen des articles
- Echange de vues

6. Divers

*

Présents : Mme Simone Beissel, M. Dan Biancalana, Mme Liz Braz, M. Sven Clement (remplaçant M. Marc Goergen), M. Alex Donnersbach, M. Emile Eicher (remplaçant M. Charel Weiler), M. Gusty Graas (remplaçant M. Guy Arendt), Mme Carole Hartmann, M. Fernand Kartheiser, Mme Paulette Lenert, M. Laurent Mosar, M. Gérard Schockmel, Mme Sam Tanson, Mme Stéphanie Weydert, M. Laurent Zeimet

Mme Elisabeth Margue, Ministre de la Justice

Mme Mathilde Crouail, Mme Anne de Bourcy, M. Gil Goebbels, M. Daniel Ruppert, Mme Lisa Schuller, M. Laurent Thyes, Mme Barbara Ujlaki, Mme Michèle Wantz, du Ministère de la Justice

Mme Jenny Thines, du groupe parlementaire CSV

M. Christophe Li, de l'Administration parlementaire

Excusés : M. Guy Arendt, M. Marc Goergen, M. Charel Weiler

M. Marc Baum, observateur délégué

*

Présidence : M. Laurent Mosar, Président de la Commission

*

1. 8287 Projet de loi portant modification de la loi modifiée du 17 mars 2004 relative au mandat d'arrêt européen et aux procédures de remise entre Etats membres de l'Union européenne

Désignation d'un rapporteur

Les membres de la Commission de la Justice désignent Monsieur Charel Weiler (CSV) comme rapporteur du projet de loi sous rubrique.

Présentation du projet de loi et examen des articles

Dans l'objectif de se conformer aux conclusions de la Commission européenne dans le cadre de la procédure d'infraction INFR(2022)2018 ouverte à l'encontre du Grand-Duché de Luxembourg pour transposition incorrecte en droit national de certaines dispositions de la décision-cadre 2002/584/JAI du Conseil du 13 juin 2002 relative au mandat d'arrêt européen et aux procédures de remise entre États membres, modifiée par la décision-cadre 2009/299/JAI du Conseil du 26 février 2009 portant modification des décisions-cadres 2002/584/JAI, 2005/ 214/JAI, 2006/783/JAI, 2008/909/JAI et 2008/947/JAI, le projet de loi sous rubrique vise à insérer un nouvel alinéa 2 à l'article 12 de la loi modifiée du 17 mars 2004 relative au mandat d'arrêt européen et aux procédures de remise entre États membres de l'Union européenne.

Dans une lettre de mise en demeure du 19 mai 2022, la Commission européenne a demandé au Luxembourg de présenter ses observations quant à la transposition incorrecte de certaines dispositions de la décision-cadre 2002/584/JAI. Dans le courrier précité, la Commission européenne estimait que le Luxembourg avait manqué aux obligations qui lui incombent en vertu de l'article 15, paragraphe 1er, et l'article 17, paragraphes 2 et 4, de la décision-cadre 2002/584/JAI concernant les délais pour prendre une décision sur l'exécution du mandat d'arrêt européen ainsi qu'à ses obligations d'informer sans délai l'autorité judiciaire de l'État qui a émis le mandat d'arrêt européen.

En réponse aux observations formulées par le gouvernement luxembourgeois par lettre du 20 juin 2022, la Commission européenne a adressé un avis motivé au Grand-Duché de Luxembourg le 1er juin 2023, conformément à l'article 258 du Traité sur le fonctionnement de l'Union européenne. L'avis susmentionné constate que le Luxembourg a manqué aux obligations qui lui incombent en vertu de l'article 15, paragraphe 1er, et de l'article 17, paragraphe 4, de la décision-cadre 2002/584/JAI en transposant de manière incorrecte la possibilité de prolonger, dans certains cas, les délais pour statuer sur l'exécution d'un mandat d'arrêt européen ainsi que l'obligation ultérieure d'en informer immédiatement l'autorité judiciaire d'émission en indiquant les raisons ayant mené au retard.

Le constat de la transposition incorrecte de l'article 17, paragraphe 2, relatif aux délais d'adoption d'une décision sur l'exécution d'un mandat d'arrêt européen après le consentement de la personne recherchée à sa remise, a été retiré à la suite des observations formulées par le Luxembourg. Conformément à l'avis motivé susmentionné, le Luxembourg dispose d'un délai de deux mois à compter de la réception de l'avis pour prendre les mesures nécessaires afin de remédier aux manquements constatés par la Commission européenne. En cas de non-conformité à la décision-cadre dans le délai fixé, la Commission européenne pourrait saisir la Cour de justice de l'Union européenne d'un recours en manquement à l'encontre du Grand-Duché de Luxembourg.

Bien que la transposition de la décision-cadre par le Luxembourg en 2004 prévoie d'ores et déjà l'application de ces dispositions, la Commission européenne demande qu'elles soient consacrées textuellement et de manière explicite, afin de renforcer l'État de droit et les droits de la défense au Grand-Duché de Luxembourg. Le présent projet de loi vise donc à remédier aux manquements constatés.

Examen de l'avis du Conseil d'État

Quant au fond, le projet de loi n'appelle pas d'observations de la part du Conseil d'État.

Échange de vues

M. Fernand Kartheiser (ADR) souhaite savoir quelles raisons ont animé le législateur de l'époque à ne pas insérer une telle disposition dans la loi modifiée du 17 mars 2004 relative au mandat d'arrêt européen et aux procédures de remise entre États membres de l'Union européenne. Il se demande s'il s'agit d'un oubli de la part du législateur précédent ou, s'il s'agit d'un choix délibéré de celui-ci.

Le représentant du Ministère de la Justice explique que selon la lecture du texte de loi par les autorités judiciaires luxembourgeoises, ces dernières peuvent de toute façon informer l'autorité compétente de l'État d'émission des motifs du retard qui justifieraient l'obtention d'un tel délai additionnel, et ce, même en l'absence d'une disposition spécifique existante dans la loi précitée. Par conséquent, la réforme proposée vise uniquement à consacrer législativement une pratique existante et de se conformer aux critiques exprimées par la Commission européenne.

2. 8316 Projet de loi portant modification du Code pénal aux fins de la transposition de la directive (UE) 2013/40 du Parlement et du Conseil du 12 août 2013 relative aux attaques visant les systèmes d'information et remplaçant la décision-cadre 2005/222/JAI du Conseil

Désignation d'un rapporteur

Les membres de la Commission de la Justice désignent Monsieur Alex Donnersbach (CSV) comme rapporteur du projet de loi sous rubrique.

Présentation du projet de loi et examen des articles

Des systèmes d'information performants sont tout aussi indispensables à la liberté, à la sécurité et à la justice d'un État qu'à la lutte contre la cybercriminalité. Afin de garantir un niveau de protection adéquat des systèmes d'information des États membres de l'Union européenne, le Parlement européen et le Conseil ont adopté en date du 12 août 2013, la directive 2013/40/UE relative aux attaques contre les systèmes d'information et remplaçant la décision-cadre 2005/222/JAI du Conseil.

Au plan national, cette directive a été transposée par la loi du 18 juillet 2014 portant 1) approbation de la Convention du Conseil de l'Europe sur la cybercriminalité, ouverte à la signature à Budapest le 23 novembre 2001, 2) approbation du Protocole additionnel à la Convention sur la cybercriminalité, relatif à l'incrimination des actes de nature raciste et xénophobe commis par le biais de systèmes informatiques, fait à Strasbourg le 28 janvier 2003, 3) modification du Code pénal, 4) modification du Code d'instruction criminelle, 5) modification de la loi modifiée du 30 mai 2005 concernant la protection de la vie privée dans le secteur des communications électroniques.

La Commission européenne a toutefois constaté que le Luxembourg avait transposé de manière incorrecte l'article 9, paragraphe 4, de la directive, lequel impose aux États membres de prendre les mesures nécessaires pour que les infractions d'atteinte à l'intégrité d'un système d'information et à l'intégrité des données visées aux articles 4 et 5 de la directive soient passibles d'une peine maximale d'au moins cinq ans d'emprisonnement

lorsqu'elles sont commises dans le cadre d'une organisation criminelle, qu'elles causent un préjudice grave ou qu'elles sont commises contre un système d'information d'une infrastructure critique.

Il a donc été recommandé au Luxembourg d'élaborer une disposition légale permettant une application conforme et plus littérale du droit européen. De ce fait, ce projet de loi prévoit d'élargir le champ d'application matériel, tout en prévoyant une sanction efficace, proportionnée et dissuasive. *In fine*, il appartient à la Justice d'apprécier au cas par cas s'il s'agit ou non d'une circonstance aggravante.

Par l'ajout d'un alinéa 2 nouveau à l'article 509-4 du Code pénal, le législateur vise à se conformer à l'article 9, paragraphe 4, lettres b) et c) de la directive prémentionnée, en introduisant les attaques visant le système d'information d'une infrastructure critique et le préjudice grave comme circonstances aggravantes des infractions incriminées aux articles 4 et 5 de la directive. Toutefois, ces deux articles ne nécessitent aucune adaptation spécifique, vu que les libellés des articles 509-1 à 509-3 du Code pénal prévoient d'ores et déjà les infractions d'atteinte à l'intégrité d'un système informatique et à l'intégrité des données.

Par le biais de cette modification législative, l'auteur d'une atteinte à l'intégrité d'un système d'information ou à l'intégrité des données sera désormais puni d'un emprisonnement de quatre mois à cinq ans et d'une amende de 1 250 euros à 30 000 euros lorsque l'attaque est dirigée contre un système d'information d'une infrastructure critique telle que définie à l'article 2, point 4 de la loi du 23 juillet 2016 portant création d'un Haut-Commissariat à la protection nationale et modifiant a) la loi modifiée du 23 juillet 1952 concernant l'organisation militaire ; b) la loi du 8 décembre 1981 sur les réquisitions en cas de conflit armé, de crise internationale grave ou de catastrophe ; c) la loi modifiée du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel ; d) la loi modifiée du 25 juin 2009 sur les marchés publics ; e) la loi modifiée du 9 décembre 2005 déterminant les conditions et modalités de nomination de certains fonctionnaires occupant des fonctions dirigeantes dans les administrations et services de l'État ; f) la loi modifiée du 25 mars 2015 fixant le régime des traitements et les conditions et modalités d'avancement des fonctionnaires de l'État.

Il en va de même lorsque ces agissements ont causé un préjudice grave pour une personne physique ou morale.

À noter que la modification de l'article 509-4 du Code pénal s'inscrit dans le cadre du maximum des peines d'emprisonnement fixées à l'article 9, paragraphe 4, de la directive précitée, à savoir un maximum d'au moins cinq ans.

Le plafond de l'amende reflète la nécessité de punir les infractions d'atteinte à l'intégrité d'un système ou des données par une sanction effective, proportionnée et dissuasive, adaptée au but poursuivi par leur auteur et le préjudice subi par une personne.

Examen de l'avis du Conseil d'État

Le Conseil d'État n'a pas d'observations à formuler quant au fond du projet de loi sous rubrique. Il préconise toutefois une reformulation de l'intitulé de ce dernier.

Échange de vues

- M. Sven Clement (Piraten) renvoie à ses expériences professionnelles. Il signale que des experts informatiques sont capables de manipuler une demande informatique envoyée à un système informatique, permettant ainsi la révélation d'informations sensibles ou internes contenues dans ce système informatique, sans qu'une telle révélation ait été prévue lors de

la programmation de celui-ci. L'orateur se demande si cette pratique pourrait tomber dans le champ d'application de la loi en projet. L'orateur souligne l'importance de cette question, étant donné que des lanceurs d'alerte comme Edward Snowden disposaient d'un accès légitime au système informatique des autorités américaines, cependant ils ont réussi à obtenir accès à des informations confidentielles de ce système en faisant des manipulations informatiques, qui n'ont pas été prévues lors de la programmation de ce système informatique.

Le représentant du Ministère de la Justice explique que cette question est à examiner à la lumière de la loi du 29 juillet 2023[1]. Par le biais de cette récente réforme, le législateur a modifié l'article 509-1 du Code pénal et il a incriminé le fait d'effectuer un traitement des données à caractère personnel pour des finalités autres que celles pour lesquelles l'autorisation d'accès a été accordée, combien même l'auteur de l'infraction dispose d'une autorisation d'accès à tout ou partie de ce système de traitement ou de transmission automatisé.

❖ M. Fernand Kartheiser (ADR) souhaite connaître la position du Gouvernement sur la question de savoir si la directive concernée a été transposée correctement ou non.

Le représentant du Ministère de la Justice répond qu'à la lecture combinée des dispositions du Code pénal, des circonstances aggravantes ont été prévues pour certaines infractions prévues par ladite directive et permettent ainsi au juge du fond d'examiner l'existence éventuelle de ces dernières dans le chef du prévenu. Or, une disposition générale prévoyant une telle circonstance aggravante a fait défaut jusqu'à présent. Par le biais de cette modification législative, il est proposé de s'adapter à l'approche d'une transposition littérale, préconisée par la Commission européenne.

❖ M. Fernand Kartheiser (ADR) prend acte de ces explications. L'orateur donne à considérer que les directives instaurent une obligation de résultat, mais laissent les États membres libres quant aux moyens d'y parvenir. Ainsi, un État ne peut être obligé de transposer mot pour mot les dispositions issues du droit européen.

❖ M. Laurent Mosar (Président, CSV) renvoie à la *ratio legis* de ladite directive et signale que lors de la transposition de celle-ci, il incombe aux autorités nationales de transposer les dispositions y contenues dans un esprit fidèle à la volonté du législateur européen.

❖ Mme Simone Beissel (DP) souligne l'importance de la mise en place de sanctions dissuasives par le législateur en matière de lutte contre la cybercriminalité. L'oratrice signale que ce sujet constitue une préoccupation pour de nombreux pays européens.

3. 8053 Projet de loi modifiant
1) La loi modifiée du 10 août 1915 sur les sociétés commerciales
2) La loi modifiée du 19 décembre 2002 concernant le registre de commerce et des sociétés ainsi que la comptabilité et les comptes annuels des entreprises aux fins de transposer la Directive (UE) 2019/2121 du Parlement européen et du Conseil du 27 novembre 2019

[1] Loi du 29 juillet 2023 portant modification :
1° de la loi modifiée du 18 juillet 2018 sur la Police grand-ducale ;
2° de la loi modifiée du 18 juillet 2018 sur l'Inspection générale de la Police ;
3° de la loi du 1er août 2018 relative au traitement des données des dossiers passagers ;
4° de la loi modifiée du 5 juillet 2016 portant réorganisation du Service de renseignement de l'État ;
5° du Code pénal.
(Journal officiel du Grand-Duché de Luxembourg, Mémorial A561 du 1er septembre 2023).

modifiant la directive (UE) 2017/1132 en ce qui concerne les transformations, fusions et scissions transfrontalières

Désignation d'un rapporteur

Les membres de la Commission de la Justice désignent Mme Stéphanie Weydert (CSV), comme rapportrice du projet de loi sous rubrique.

Présentation du projet de loi et examen des articles

Il est renvoyé à la présentation[2] annexée au présent procès-verbal.

Échange de vues

❖ M. Laurent Mosar (Président, CSV) salue le fait que le projet de loi prévoit des dispositions spécifiques sur la protection des actionnaires minoritaires. De plus, l'orateur renvoie au champ d'application de la future loi, qui exclut les entités dans un État tiers. L'orateur donne à considérer que de nombreuses entreprises multinationales disposent d'entités dans un État membre de l'Union européenne, mais également dans des États tiers. Il souhaite savoir quelles implications cette exclusion aura pour les sociétés de droit luxembourgeois.

De plus, l'orateur signale que l'État luxembourgeois est actionnaire minoritaire dans plusieurs sociétés multinationales cotées en bourse. Il convient dès lors de se demander si les dispositions de la loi en projet ont vocation à s'appliquer à l'État.

Le représentant du Ministère de la Justice confirme que le projet de loi sous rubrique dispose d'un champ d'application déterminé et n'a pas vocation à s'appliquer aux sociétés et entités établies dans un État tiers. Par le biais de ce projet de loi, il est procédé à une transposition de la directive conformément à l'adage « la directive et rien que la directive ».

Il est par ailleurs confirmé que les règles issues de la loi en projet et visant les droits des actionnaires minoritaires, ont également vocation à s'appliquer à l'État luxembourgeois lorsque ce dernier est actionnaire minoritaire dans une société commerciale.

❖ Mme Stéphanie Weydert (Rapportrice, CSV) renvoie à son expérience professionnelle en tant que mandataire de justice et signale que des transformations, fusions et scissions transfrontalières de sociétés nécessitent une analyse détaillée au cas par cas, au vu des spécificités du droit luxembourgeois et des dispositions légales applicables à l'étranger.

L'oratrice salue d'une part la volonté du législateur de moderniser le cadre légal existant et de simplifier certaines dispositions de droit luxembourgeois. D'autre part, l'oratrice exprime sa crainte que le contrôle de légalité puisse, en fonction de la complexité de l'opération à effectuer et des informations à fournir au notaire, ralentir considérablement le projet entamé par une société.

❖ Mme Sam Tanson (déi gréng) donne à considérer que ce projet de loi n'a pas encore été avisé par le Conseil d'État.

En outre, le volet relatif au droit du travail dans le cadre des transformations, fusions et scissions transfrontalières a fait couler beaucoup d'encre parmi les experts en la matière. L'oratrice souhaite avoir des informations supplémentaires sur l'avancement de ce volet.

[2] *cf.* Annexe 1 et courrier électronique du portail interne de la Chambre des Députés du 21 décembre 2023.

Le représentant du Ministère de la Justice confirme que le projet de loi sous rubrique n'a pas encore fait l'objet d'un avis du Conseil d'État. Il est cependant probable que cet avis soit publié au début de l'année 2024.

À noter que le volet relatif au droit du travail fait l'objet d'un projet[3] de loi à part. Ce projet de loi a récemment été avisé par le Conseil d'État.

- M. Sven Clement (Piraten) tient à souligner l'importance de la lisibilité de la future loi. Une telle façon de procéder permet aux actionnaires, qui ne sont pas forcément des professionnels du droit, de mieux comprendre ce texte de loi et d'exercer les droits qui leurs sont conférés par la loi. Si l'orateur appuie l'approche adoptée par le Gouvernement à subdiviser ce texte du projet de loi en chapitres et en articles ayant chacun un intitulé, il donne également à considérer que le Conseil d'État s'est montré critique dans le passé face à cette démarche, en argumentant que seul le texte à valeur normative doit figurer dans la future loi.

- M. Alex Donnersbach (CSV) signale que la loi en projet confère de nouvelles missions aux notaires. L'orateur se pose la question de savoir si une réforme de la loi modifiée du 9 décembre 1976 relative à l'organisation du notariat est prévue.

  Mme Elisabeth Margue (Ministre de la Justice, CSV) indique qu'elle a récemment eu une entrevue avec les représentants de la Chambre des Notaires, lors de laquelle les défis auxquels les notaires font actuellement face ont été discutés. Il est à l'heure actuelle prématuré de discuter d'éventuelles réformes visant le notariat.

4. 7881 Projet de loi sur les échanges d'informations relatives aux ressortissants de pays tiers à l'Union européenne ainsi que le système européen d'information sur les casiers judiciaires (ECRIS) portant :
1° transposition de la directive (UE) 2019/884 du Parlement européen et du Conseil du 17 avril 2019 modifiant la décision-cadre 2009/315/JAI du Conseil en ce qui concerne les échanges d'informations relatives aux ressortissants de pays tiers ainsi que le système européen d'information sur les casiers judiciaires (ECRIS), et remplaçant la décision 2009/316/JAI du Conseil ;
2° mise en œuvre du règlement (UE) 2019/816 du Parlement européen et du Conseil du 17 avril 2019 portant création d'un système centralisé permettant d'identifier les États membres détenant des informations relatives aux condamnations concernant des ressortissants de pays tiers et des apatrides, qui vise à compléter le système européen d'information sur les casiers judiciaires, et modifiant le règlement (UE) 2018/1726 ;
3° modification de la loi modifiée du 29 mars 2013 relative à l'organisation du casier judiciaire

Changement de rapporteur

[3] *cf.* Projet de loi n°8225 modifiant le Code du travail aux fins de transposer la directive (UE) 2019/2121 du Parlement européen et du Conseil du 27 novembre 2019 modifiant la directive (UE) 2017/1132 en ce qui concerne les transformations, fusions et scissions transfrontalières.

La Commission de la Justice désigne son Président, M. Laurent Mosar (CSV), comme nouveau rapporteur du projet de loi sous rubrique.

Examen de l'avis du Conseil d'Etat

Dans son avis du 14 novembre 2023, le Conseil d'Etat constate que « *[…] le système projeté ne vise pas à créer une base de données européenne centralisée des casiers judiciaires de l'ensemble des États membres, mais permettra uniquement de déterminer quels États membres détiennent des informations sur le casier judiciaire du ressortissant d'un pays tiers ou d'un apatride. La demande d'information s'effectuera à travers l'ECRIS entre autorités centrales nationales compétentes.*

Le traitement des données à caractère personnel devra s'effectuer en conformité avec les dispositions de la loi du 1er août 2018 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel en matière pénale ainsi qu'en matière de sécurité nationale, transposant la directive (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, et abrogeant la décision-cadre 2008/977/JAI du Conseil, ci-après la « directive (UE) 2016/680 » ».

Quant à l'article 2 du projet de loi amendé, le Conseil d'État préconise la suppression des paragraphes 1er à 3. Selon l'avis de la Haute Corporation, ces dispositions sont superfétatoires. Quant au paragraphe 4, le Conseil d'État « *[…] conçoit l'utilité de fixer un délai de conservation des journaux dont la durée devrait correspondre à celle retenue pour l'accès à l'application JU-CHA, dont la durée est fixée par le projet de loi n° 7882. Un alignement des durées de conservation est de rigueur puisque le module casier judiciaire fait partie intégrante de l'application JU CHA* ».

Quant à lutte contre des consultations illégitimes, le Conseil d'État regarde d'un œil critique l'article 2, paragraphe 4 et s'oppose formellement à ce libellé. S'il constate que le texte proposé prévoit que « *[…] les journaux des opérations de consultation et de communication doivent permettre d'établir, entre autres, le motif de la consultation effectuée* », il estime également que « *[…] Le texte proposé sous le point 2° ne mentionne pas les motifs de la consultation et risque par conséquent d'être partiellement contraire au droit européen. Le Conseil d'État demande, sous peine d'opposition formelle pour violation du droit de l'Union européenne, soit de compléter la disposition sous examen, soit de reprendre la formulation de l'article 24 de la loi précitée du 1er août 2018.* ».

Quant à l'article 8 du projet de loi, le Conseil d'État renvoie aux dispositions légales existantes, et notamment à la loi du 1er août 2018[4] portant organisation de la Commission nationale pour la protection des données et du régime général sur la protection des données et rappelle que cette loi s'applique « *donc a priori également aux traitements de données relatifs à des ressortissants de pays tiers ou à des personnes apatrides. Le Conseil d'État*

[4] loi du 1er août 2018 portant organisation de la Commission nationale pour la protection des données et mise en œuvre du 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), portant modification du Code du travail et de la loi modifiée du 25 mars 2015 fixant le régime des traitements et les conditions et modalités d'avancement des fonctionnaires de l'État. (Journal officiel du Grand-Duché de Luxembourg, Mémorial A686 du 16 août 2018).

recommande de ne pas reprendre, dans le texte sous examen, les droits des personnes concernées, dans la mesure où ces droits découlent à suffisance de la loi du 1er août 2018 ».

De plus, le Conseil d'État s'oppose formellement au paragraphe 3 de l'article 8. Il estime que ce libellé est source d'insécurité juridique et il « *[…] s'interroge si la procédure visée est celle de l'article 45 de la loi précitée du 1er août 2018, qui traite du recours juridictionnel contre une décision de l'autorité de contrôle ou si le recours peut être porté directement devant la chambre du conseil de la Cour d'appel. Il demande, sous peine d'opposition formelle pour insécurité juridique, que ce point soit clarifié* ». Par ailleurs, le régime juridique applicable aux recours judiciaires suscite des observations critiques de la part du Conseil d'État. Il donne à considérer que « *[…] les contestations des inscriptions étant portées devant la chambre du conseil de la Cour d'appel. L'arrêt est susceptible d'un recours en cassation. Une telle voie de recours n'est pourtant pas prévue pour les personnes physiques, la loi précitée du 1er août 2018 ne la prévoyant pas. Le Conseil d'État note que les droits d'accès aux données conservées et les droits de rectification de ces mêmes données reconnus aux personnes physiques sont ainsi réglés différemment de ceux accordés aux personnes morales, ce qui risque d'être considérée comme contraire au principe constitutionnel de l'égalité devant la loi, tel que consacré par l'article 15 de la Constitution. Le Conseil d'État doit formuler une réserve de dispense du second vote constitutionnel dans l'attente d'explications des auteurs sur les raisons de cet agencement différent des droits d'accès et de rectification selon la nature de la personne concernée* ».

Quant à l'article 9, paragraphe 1er, du projet de loi portant sur l'obligation pour chaque État membre de créer un fichier de données dans le système ECRIS-TCN pour chaque ressortissant condamné d'un pays tiers, le Conseil d'État met en garde le législateur contre le risque d'une transposition incorrecte de la directive. Il donne à considérer que « *[…] En ce qui concerne l'article 12-1 nouveau, paragraphe 1er, alinéa 2, il convient de préciser que l'article 5, paragraphe 1er, lettre a), sous i), huitième tiret, du règlement (UE) 2019/816 exige l'inscription du « code de l'État membre de condamnation », à l'exception du cas où l'autorité n'en a pas connaissance. En outre, l'obligation de la mention selon laquelle « aux fins des règlements (CE) n° 767/2008 et (UE) 2018/1240, […] le ressortissant d'un pays tiers concerné a été condamné au cours des vingt-cinq dernières années pour une infraction terroriste ou au cours des quinze dernières années pour toute autre infraction pénale mentionnée dans la liste figurant dans l'annexe du règlement (UE) 2018/1240 si elle est passible, en droit national, d'une peine ou d'une mesure de sûreté privative de liberté d'une durée maximale d'au moins trois ans, y compris le code de l'État membre de condamnation » n'est pas prévue par la disposition sous examen. Aussi le Conseil d'État demande-t-il, sous peine d'opposition formelle pour contrariété avec le droit européen, de compléter la disposition sous examen* ».

Quant à l'article 9, paragraphe 2, du projet de loi, le Conseil d'État constate que « *[…] le procureur général d'État conserve une copie des données intégrées dans le système central ECRIS-TCN* », ce qui amène le Conseil d'État à soulever les interrogations suivantes : « *La collecte et la gestion de ces données ne peuvent-elle pas s'effectuer dans le système central ? Quel est le sort réservé aux « copies » anciennes si les données du système sont mises à jour ? La disposition pourrait utilement être précisée pour répondre à ces interrogations* ».

Continuation des travaux

- M. Laurent Mosar (Président-Rapporteur, CSV) salue le fait qu'une importance particulière dans la loi en projet est conférée au volet relatif à la protection des données. Quant à la disposition prévue à l'article 2 visant à prévenir des consultations illégitimes de fichiers contenant des données à caractère personnel, il y a lieu de modifier le libellé par voie d'amendement.

Le représentant du Ministère de la Justice confirme que le motif de la consultation effectuée peut être vérifié *a posteriori*.

5. 8326 Projet de loi portant sur l'information des représentants légaux des mineurs privés de liberté

Désignation d'un rapporteur

Les membres de la Commission de la Justice désignent M. Laurent Zeimet (CSV) comme rapporteur du projet de loi sous rubrique.

Présentation du projet de loi

Le projet de loi sous rubrique vise à parachever la transposition de la directive 2013/48/UE du Parlement européen et du Conseil du 22 octobre 2013 relative au droit d'accès à un avocat dans le cadre des procédures pénales et des procédures relatives au mandat d'arrêt européen, au droit d'informer un tiers dès la privation de liberté et au droit des personnes privées de liberté de communiquer avec des tiers et avec les autorités consulaires (ci-après « la Directive »).

En effet, la Directive a déjà fait l'objet d'une transposition par le Grand-Duché de Luxembourg par le biais de la loi du 8 mars 2017[5] renforçant les garanties procédurales en matière pénale.

Néanmoins, dans le cadre d'une procédure d'infraction initiée par la Commission européenne en 2017 contre le Luxembourg, la Commission a soulevé que le Luxembourg avait transposé de manière incorrecte les articles 5, paragraphes 2 et 4, et 10, paragraphe 3, de la Directive.

Ces articles prévoient l'information d'office des représentants légaux en cas de privation de liberté de leur enfant mineur, tant dans le cadre de procédures pénales nationales que dans

[5] Loi du 8 mars 2017 renforçant les garanties procédurales en matière pénale portant :
- transposition de la directive 2010/64/UE du 20 octobre 2010 relative au droit à l'interprétation et à la traduction dans le cadre des procédures pénales ;
- transposition de la directive 2012/13/UE du 22 mai 2012 relative au droit à l'information dans le cadre des procédures pénales ;
- transposition de la directive 2013/48/UE du 22 octobre 2013 relative au droit d'accès à un avocat dans le cadre des procédures pénales et des procédures relatives au mandat d'arrêt européen, au droit d'informer un tiers dès la privation de liberté et au droit des personnes privées de liberté de communiquer avec des tiers et avec les autorités consulaires ;
- transposition de la directive 2012/29/UE du 25 octobre 2012 établissant des normes minimales concernant les droits, le soutien et la protection des victimes de la criminalité ;
- changement de l'intitulé du Code d'instruction criminelle en « Code de procédure pénale » ;
- modification :
  - du Code de procédure pénale ;
  - du Code pénal ;
  - de la loi du 7 juillet 1971 portant en matière répressive et administrative, institution d'experts, de traducteurs et d'interprètes assermentés ;
  - de la loi modifiée du 10 août 1991 sur la profession d'avocat ;
  - de la loi modifiée du 20 juin 2001 sur l'extradition ;
  - de la loi modifiée du 17 mars 2004 relative au mandat d'arrêt européen et aux procédures de remise entre Etats membres de l'Union européenne.

(Journal officiel du Grand-Duché de Luxembourg, Mémorial A346 du 30 mars 2017).

le cadre de procédures relatives au mandat d'arrêt européen ainsi que les exceptions à ce principe. Il est précisé que la notion de « procédure pénale » est interprétée de façon large par la Commission européenne et vise toute procédure pouvant « potentiellement donner lieu à des mesures privatives de liberté », si cette privation de liberté est « justifiée non seulement par des raisons thérapeutiques, mais également par des motifs de sûreté ; et (…) si cette procédure est appliquée à l'égard d'une personne soupçonnée ou accusée d'avoir commis un fait constitutif d'une infraction pénale. ». Dès lors, la Commission européenne estime que les procédures visées par la loi modifiée du 10 août 1992 sur la protection de la jeunesse sont des procédures pénales.

Tel que soulevé par la Commission européenne, la législation luxembourgeoise actuellement en vigueur (Code de procédure pénale, loi modifiée du 10 août 1992 sur la protection de la jeunesse et loi modifiée du 17 mars 2004 relative au mandat d'arrêt européen et aux procédures de remise entre États membres de l'Union européenne) ne prévoit pas l'information d'office des représentants légaux du mineur lorsque celui-ci est privé de liberté.

Il échet de noter que le projet de loi n°7991 portant introduction d'une procédure pénale pour mineurs, au sujet duquel la procédure législative se poursuit, prévoit une telle disposition dans le cadre de la réforme d'envergure du système actuel de la protection de la jeunesse.

Toutefois, il convient de remédier ponctuellement aux lacunes constatées par la Commission européenne par le biais du présent projet de loi, en attendant l'adoption du projet de loi n°7991 précité, ce afin de garantir la pleine conformité de la législation luxembourgeoise actuelle à la Directive.

Examen de l'article unique

L'article unique du projet de loi prévoit de manière générale une information des représentants légaux en cas de privation de liberté de leur enfant mineur ainsi que des motifs de celle-ci, en s'inspirant de l'article 5[6], paragraphes 2 et 4, de la Directive.

Paragraphe 1er

Cet article unique est subdivisé en deux paragraphes distincts. Le paragraphe 1er, alinéa 1er, énonce de façon générale les différentes hypothèses de privation de liberté d'un mineur, qui peut avoir lieu soit dans le cadre d'une procédure pénale, soit dans le cadre d'une procédure de protection de la jeunesse ou dans le cadre d'un mandat d'arrêt européen.

[6] « Art. 5 1. Les États membres veillent à ce que les suspects ou les personnes poursuivies qui sont privés de liberté aient le droit, s'ils le souhaitent, d'en informer sans retard indu au moins une personne qu'ils désignent, telle qu'un membre de leur famille ou un employeur.
2. Si le suspect ou la personne poursuivie est un enfant, les États membres veillent à ce que le titulaire de l'autorité parentale de l'enfant soit informé dans les meilleurs délais de la privation de liberté et des motifs de celle-ci, à moins que cela ne soit contraire à l'intérêt supérieur de l'enfant, auquel cas l'information est transmise à un autre adulte approprié. Aux fins du présent paragraphe, est considérée comme enfant une personne âgée de moins de dix-huit ans.
3. Les États membres peuvent déroger temporairement à l'application des droits prévus aux paragraphes 1 et 2 si cela est justifié, compte tenu des circonstances particulières du cas d'espèce, sur la base d'un des motifs impérieux suivants :
a) lorsqu'il existe une nécessité urgente de prévenir une atteinte grave à la vie, à la liberté ou à l'intégrité physique d'une personne ;
b) lorsqu'il existe une nécessité urgente d'éviter une situation susceptible de compromettre sérieusement une procédure pénale.
4. Lorsque les États membres dérogent temporairement à l'application du droit prévu au paragraphe 2, ils veillent à ce qu'une autorité compétente en matière de protection de l'enfance soit informée sans retard indu de la privation de liberté de l'enfant. ».

En l'état actuel de la législation, sont visées les mesures privatives de liberté suivantes :

- une mesure de placement prononcée en application de l'article 1er, alinéa 2, point 4. (placement dans un établissement de rééducation de l'État) et de l'article 6 (internement dans un établissement disciplinaire de l'État) de la loi modifiée du 10 août 1992 sur la protection de la jeunesse ;
- une rétention prévue à l'article 39 du Code de procédure pénale ;
- un mandat d'amener ou d'arrêt prévu à l'article 52-1 du Code de procédure pénale ;
- un mandat de dépôt prévu à l'article 94 du Code de procédure pénale ;
- une peine privative de liberté prononcée en application du Code pénal ;
- une arrestation prévue par la loi modifiée du 17 mars 2004 relative au mandat d'arrêt européen et aux procédures de remise entre États membres de l'Union européenne (visée par l'article 10, paragraphe 3, de la Directive qui prévoit que certains droits prévus par la Directive s'appliquent également *mutatis mutandis* à la procédure relative au mandat d'arrêt européen).

Concernant les mesures privatives de liberté visées dans la loi modifiée du 10 août 1992 sur la protection de la jeunesse, il convient de préciser que les mesures de placement autres que celles prévues par l'article 1er, alinéa 2, point 4. et l'article 6 de la loi précitée ne devraient pas tomber dans le champ d'application de la présente disposition, étant donné que les autres mesures de placement n'emportent pas une privation de liberté.

Concernant les différentes mesures privatives de liberté prévues par le Code de procédure pénale, il convient de préciser que celles-ci ne s'appliquent qu'au mineur âgé de plus de 16 ans au sujet duquel le juge de la jeunesse a accordé l'autorisation de procéder « suivant les formes et compétences ordinaires » en matière pénale, en application de l'article 32 de la loi modifiée du 10 août 1992 sur la protection de la jeunesse.

Les exceptions à cette information reprises aux points 1° à 4° sont des exceptions d'une part reprises de l'article 5, paragraphes 2 et 3, de la Directive en ce qui concerne les points 1°, 3° et 4°, et d'autre part ajoutées afin de couvrir l'hypothèse dans laquelle aucun représentant légal n'est joignable (point 2°).

Paragraphe 2

Le paragraphe 2 de l'article unique prévoit que lorsque l'information ne peut pas être transmise aux représentants légaux en raison des cas énumérés aux points 1° à 4° du paragraphe 1er, l'information est transmise d'une part à un représentant du choix du mineur, conformément à l'article 5, paragraphe 2 *in fine* de la Directive qui prévoit la transmission de l'information à un « autre adulte approprié ».

Il convient de préciser que la Directive prévoit la transmission de l'information à un « autre adulte approprié » dans le seul cas où les représentants légaux ne sont pas informés en raison du fait que cette information serait contraire à l'intérêt supérieur de l'enfant. Le paragraphe 2 de l'article unique de la présente loi en projet étend néanmoins cette information à toutes les situations où les représentants légaux ne sont pas informés de la privation de liberté du mineur, afin de garantir qu'une personne de confiance du mineur soit informée de la privation de liberté en toute situation.

D'autre part, l'information est transmise à l'Office national de l'enfance (ONE), conformément à l'article 5, paragraphe 4, de la Directive, qui prévoit la transmission de l'information à une « autorité compétente en matière de protection de l'enfance ».

Échange de vues

- M. Sven Clement (Piraten) renvoie aux avis consultatifs des autorités judiciaires. Dans leurs avis, certaines remarques quant à la terminologie employée sont soulevées. De plus, l'orateur juge pertinent les remarques y soulevées quant au paragraphe 2 de l'article unique. Il est d'avis que la communication de l'information visée au paragraphe 1er « à un représentant au choix du mineur », telle que proposée actuellement audit paragraphe 2 de l'article unique, risque de susciter des difficultés lors de l'application de la future loi.

  L'orateur esquisse le cas de figure d'un mineur arrêté en flagrant délit. Ce mineur bénéficie bien évidemment de la présomption d'innocence, cependant, il se peut que le constat soit dressé que ce mineur fréquente des personnes douteuses ayant des antécédents judiciaires. Dans ce cas de figure, il peut s'avérer contraire à l'intérêt supérieur de l'enfant de laisser le mineur désigner un représentant de son choix à laquelle cette information est communiquée.

  Le représentant du Ministère de la Justice donne à considérer que la terminologie sera revue dans le cadre de l'instruction parlementaire du projet de loi n°7991 prémentionné.

- Mme Carole Hartmann (DP) renvoie au projet de loi n°7991, dont l'instruction parlementaire est en cours. L'oratrice souligne l'importance que des fugues ne donnent plus lieu à un placement du mineur dans un lieu privatif de liberté.

- M. Dan Biancalana (LSAP) renvoie au rôle de l'Office national de l'enfance et aux observations soulevées par les autorités judiciaires y relatives. Il y a lieu d'examiner s'il s'avère plus opportun de mentionner expressément le Service central d'assistance sociale (SCAS) dans le texte de la future loi.

6. Divers

Les membres de la Commission de la Justice auront une entrevue au Conseil d'État en date du 24 janvier 2024.

Procès-verbal approuvé et certifié exact

Annexe 1 : Présentation intitulée « PL 8053 Transposition de la Directive 2019/2121 qui concerne les transformations, fusions et scissions transfrontalières dite « mobilité » », élaborée par le Ministère de la Justice.

PL 8053

Transposition de la Directive 2019/2121 qui concerne les transformations, fusions et scissions transfrontalières dite « mobilité »

Commission de la Justice

21 décembre 2023

LE GOUVERNEMENT
DU GRAND-DUCHÉ DE LUXEMBOURG
Ministère de la Justice

Présentation de la Directive Mobilité

LE GOUVERNEMENT
DU GRAND-DUCHÉ DE LUXEMBOURG

- Vise l'amélioration du marché intérieur par le biais :
  - De la mise à jour et amélioration du régime des fusions transfrontalières corrigeant certaines insuffisances certaines imperfections qui demeuraient dans le régime introduit à l'origine par la 10ème directive en 2005, principalement en ce qui concerne la protection des créanciers, des associés minoritaires et des travailleurs.
  - D'un nouveau cadre légal pour les scissions et les transformations transfrontalières

Objectifs de la Directive

- Un socle commun de règles applicables aux différentes opérations de mobilité transfrontalière ;
- Une information renforcée des parties prenantes ;
- Un droit de retrait bénéficiant aux associés opposés à l'opération projetée ;
- Un contrôle anti-abus et anti-fraude de l'opération.

Enjeux de la transposition

LE GOUVERNEMENT
DU GRAND-DUCHÉ DE LUXEMBOURG

- Directive que l'on peut considérer comme plus restrictive en matière de mobilité du point de vue national
- Directive plus favorable aux associés minoritaires que notre droit national
- Éviter tout retour en arrière par rapport à la situation actuelle dans laquelle toutes les opérations transfrontalières sont possibles pour toutes les sociétés dotées de la personnalité juridique et parfaitement réalisables en pratique.

Objectif du projet de loi (1/2)

- Adopter une position jugée plus conforme à la liberté d'établissement telle qu'interprétée par la Cour de justice de l'Union européenne.
  - Premier pilier : délimiter le champ d'application des nouveaux régimes issus de la Directive Mobilité et ne pas l'étendre à d'autres opérations transfrontalières telles que les transformations transfrontalières impliquant des États tiers ou en encore les scissions transfrontalières par absorption.
  - En d'autres termes, application du principe de transposition « toute la directive, rien que la directive »

Objectif du projet de loi (2/2)

- Second pilier: faire usage des options ainsi que de toute la latitude laissée aux États membres par le texte européen pour mettre en place un régime aussi favorable à la mobilité transfrontalière que possible
- Une attention particulière est à porter au:
  - **contrôle anti-abus** dont les notaires seront chargés lors du premier contrôle de légalité
  - **droit de retrait des associés minoritaires** opposés au projet de fusion, de scission ou de transformation transfrontalière.

Méthode 1/2

- Les nouvelles dispositions relatives aux fusions et aux scissions transfrontalières européennes ont été isolées au sein d'une section séparée du chapitre II et du chapitre III du titre X de la Loi de 1915
- Introduction de nouvelles notions de « fusion transfrontalière européenne » et de « scission transfrontalière européenne » pour en délimiter le champ d'application.

Méthode 2/2

- Il s'agira d'un régime spécial et dérogatoire au droit commun des fusions et scissions internes et transfrontalières
- Approche différente pour la procédure de transformation interne qui n'a pas été calquée sur le modèle européen des restructurations transfrontalières – elles s'apparentent davantage au « transfert de siège volontaire ». Cette procédure est transposée au sein d'un nouveau chapitre VI du titre X de la Loi de 1915 sous la notion de « transformation transfrontalière européenne ».

Rappel du nouveau processus

LE GOUVERNEMENT
DU GRAND-DUCHÉ DE LUXEMBOURG

1. Préparation et publication

- Projet commun
- Rapport de l'organe de gestion/administration
- Rapport d'expert
- Publication et information des stakeholders

2. Approbation

- Approbation de l'opération par l'assemblée générale

3. Premier contrôle

- 1er contrôle de légalité
- Certificat préalable

4. Deuxième contrôle et prise d'effet

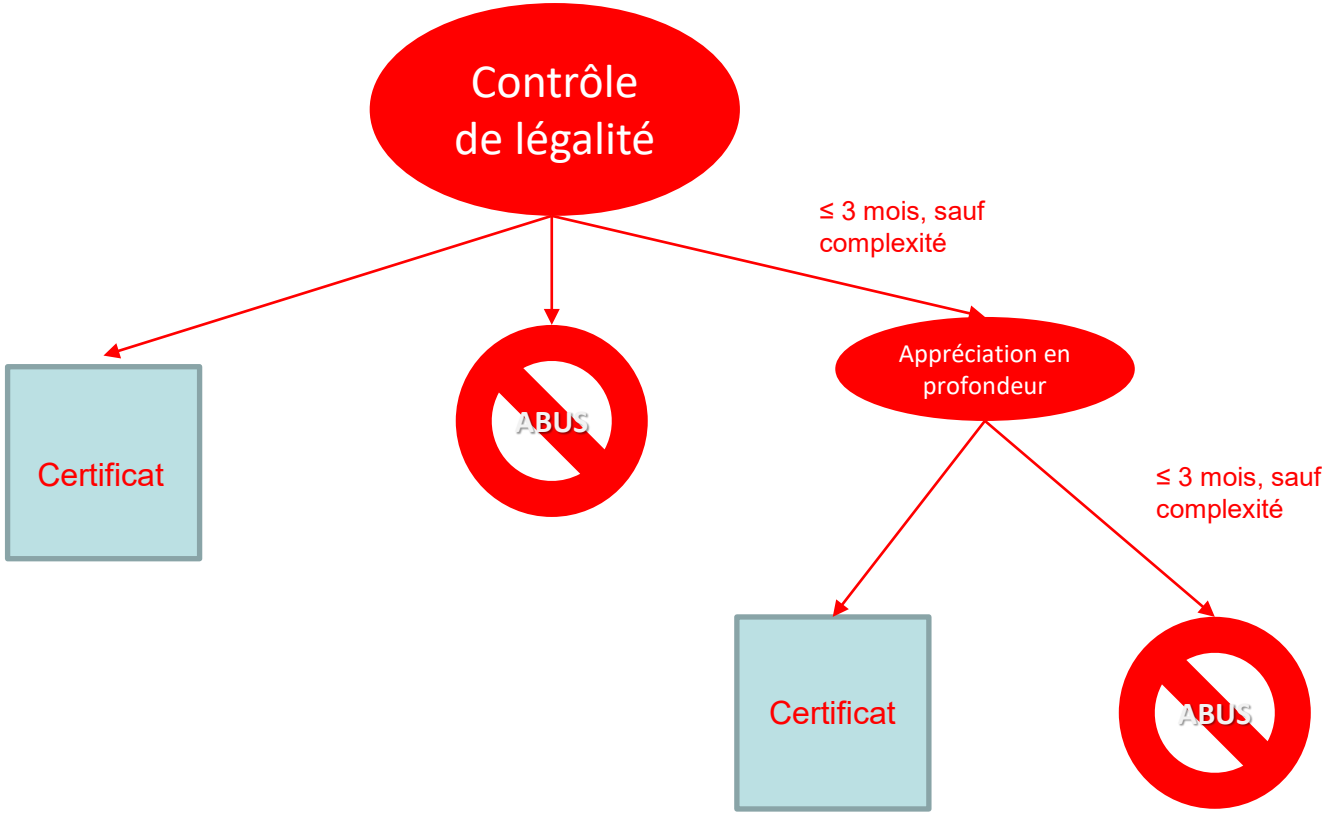
- 2ème contrôle de légalité
- Date de prise d'effet

Le contrôle anti-abus

- *Les Etats membres veillent à ce que l'autorité compétente ne délivre pas de certificat préalable à la fusion/scission/transformation s'il est déterminé, conformément au droit national, qu'une opération transfrontalière est réalisée à des fins abusives ou frauduleuses menant ou visant à se soustraire au droit de l'Union ou au droit national ou à le contourner, ou à des fins criminelles.*

Le contrôle anti-abus

LE GOUVERNEMENT
DU GRAND-DUCHÉ DE LUXEMBOURG



La protection des associés minoritaires

- Une exposition à certains risques pour les minoritaires:
  - une décision imposée par la majorité
  - la nature transfrontalière de l'opération
  - un rapport d'échange inadéquat
  - l'allocation asymétrique des actions des sociétés bénéficiaires (scissions)
- Un système de protection double:
  - Droit de retrait contre juste rémunération
  - Droit de contester le rapport d'échange

La protection des associés minoritaires

- Nécessité de voter contre l'opération transfrontalière
- Pas d'extension aux actions sans droit de vote
- Droit de retrait à exercer au plus tard lors de l'AG
- Délai de paiement de deux mois après la prise d'effet
- Droit de retrait à exercer sur toutes les actions de l'actionnaire sortant
- Exclusion des actions acquises préalablement à l'AG mais après publication du projet

8316/02

N° 8316²

CHAMBRE DES DEPUTES

PROJET DE LOI

portant modification du Code pénal en vue de la transposition de la directive 2013/40/UE du Parlement et du Conseil du 12 août 2013 relative aux attaques visant les systèmes d'information et remplaçant la décision-cadre 2005/222/JAI du Conseil

* * *

RAPPORT DE LA COMMISSION DE LA JUSTICE

(25.1.2024)

La Commission se compose de : M. Laurent MOSAR, Président ; M. Alex DONNERSBACH, Rapporteur ; M. Guy ARENDT, Mme Simone BEISSEL, M. Dan BIANCALANA, Mme Liz BRAZ, M. Marc GOERGEN, Mme Carole HARTMANN, M. Fernand KARTHEISER, Mme Paulette LENERT, M. Gérard SCHOCKMEL, Mme Sam TANSON, M. Charel WEILER, Mme Stéphanie WEYDERT et M. Laurent ZEIMET, Membres.

*

1. ANTECEDENTS

Le projet de loi n°8316 a été déposé par la Ministre de la Justice de l'époque, Madame Sam Tanson (déi gréng), en date du 28 septembre 2023.

Le texte du projet de loi était accompagné d'un exposé des motifs, d'un commentaire des articles, d'une fiche financière et d'évaluation d'impact, d'un check de durabilité ainsi que d'un texte coordonné par extrait du Code pénal. Au texte gouvernemental était également joint la directive 2013/40/UE du Parlement européen et du Conseil du 12 août 2013 relative aux attaques contre les systèmes d'information et remplaçant la décision-cadre 2005/222/JAI du Conseil.

En date du 24 novembre 2023, le présent projet de loi a été renvoyé à la Commission de la Justice.

Le projet de loi a été présenté aux membres de la Commission de la Justice le 21 décembre 2023 et M. Alex Donnersbach (CSV) a été nommé rapporteur au cours de cette même réunion.

Le Conseil d'État a rendu son avis en date du 24 octobre 2023. Il a été examiné par la Commission de la Justice le 21 décembre 2023.

L'adoption du rapport a eu lieu le 25 janvier 2024.

*

2. OBJET

Des systèmes d'information performants sont tout aussi indispensables à la liberté, à la sécurité et à la justice d'un État qu'à la lutte contre la cybercriminalité. Afin de garantir un niveau de protection adéquat des systèmes d'information des États membres de l'Union européenne, le Parlement européen et le Conseil ont adopté en date du 12 août 2013, la directive 2013/40/UE relative aux attaques contre les systèmes d'information et remplaçant la décision-cadre 2005/222/JAI du Conseil.

Au plan national, cette directive a été transposée par la loi du 18 juillet 2014 portant 1) approbation de la Convention du Conseil de l'Europe sur la cybercriminalité, ouverte à la signature à Budapest le 23 novembre 2001, 2) approbation du Protocole additionnel à la Convention sur la cybercriminalité,

relatif à l'incrimination des actes de nature raciste et xénophobe commis par le biais de systèmes informatiques, fait à Strasbourg le 28 janvier 2003, 3) modification du Code pénal, 4) modification du Code d'instruction criminelle, 5) modification de la loi modifiée du 30 mai 2005 concernant la protection de la vie privée dans le secteur des communications électroniques.

La Commission européenne a toutefois constaté que le Luxembourg avait transposé de manière incorrecte l'article 9, paragraphe 4, notamment le point b), de la directive, lequel impose aux États membres de prendre les mesures nécessaires pour que les infractions d'atteinte à l'intégrité d'un système d'information et à l'intégrité des données visées aux articles 4 et 5 de la directive soient passibles d'une peine maximale d'au moins cinq ans d'emprisonnement lorsqu'elles sont commises dans le cadre d'une organisation criminelle, qu'elles causent un préjudice grave ou qu'elles sont commises contre un système d'information d'une infrastructure critique.

Il a donc été recommandé au Luxembourg d'élaborer une disposition légale permettant une application conforme et plus littérale du droit européen. De ce fait, ce projet de loi prévoit ainsi d'inclure les circonstances aggravantes prévues par la directive, tout en y appliquant une sanction efficace, proportionnée et dissuasive. *In fine*, il appartient aux autorités judiciaires d'apprécier au cas par cas s'il s'agit ou non d'une circonstance aggravante.

*

3. AVIS DU CONSEIL D'ETAT

Le Conseil d'État n'a pas d'observation à formuler sur le contenu du projet de loi sous rubrique. Il propose toutefois de reformuler l'intitulé du projet de loi de manière à reproduire son intitulé tel que publié officiellement :

« Projet de loi portant modification du Code pénal en vue de la transposition de la directive ~~(UE)~~ 2013/40/UE du Parlement et du Conseil du 12 août 2013 relative aux attaques visant les systèmes d'information et remplaçant la décision-cadre 2005/222/JAI du Conseil »

*

4. COMMENTAIRE DES ARTICLES

Par l'ajout d'un alinéa 2 nouveau à l'article 509-4 du Code pénal, le législateur vise à se conformer à l'article 9, paragraphe 4, lettres b) et c) de la directive prémentionnée, en introduisant les attaques visant le système d'information d'une infrastructure critique et le préjudice grave comme circonstances aggravantes des infractions incriminées aux articles 4 et 5 de la directive. Toutefois, ces deux articles ne nécessitent aucune adaptation spécifique, vu que les libellés des articles 509-1 à 509-3 du Code pénal prévoient d'ores et déjà les infractions d'atteinte à l'intégrité d'un système informatique et à l'intégrité des données.

Par le biais de cette modification législative, l'auteur d'une atteinte à l'intégrité d'un système d'information ou à l'intégrité des données sera désormais puni d'un emprisonnement de quatre mois à cinq ans et d'une amende de 1 250 euros à 30 000 euros lorsque l'attaque est dirigée contre un système d'information d'une infrastructure critique telle que définie à l'article 2, point 4 de la loi du 23 juillet 2016 portant création d'un Haut-Commissariat à la protection nationale et modifiant a) la loi modifiée du 23 juillet 1952 concernant l'organisation militaire ; b) la loi du 8 décembre 1981 sur les réquisitions en cas de conflit armé, de crise internationale grave ou de catastrophe ; c) la loi modifiée du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel ; d) la loi modifiée du 25 juin 2009 sur les marchés publics ; e) la loi modifiée du 9 décembre 2005 déterminant les conditions et modalités de nomination de certains fonctionnaires occupant des fonctions dirigeantes dans les administrations et services de l'État ; f) la loi modifiée du 25 mars 2015 fixant le régime des traitements et les conditions et modalités d'avancement des fonctionnaires de l'État.

Il en va de même lorsque ces agissements ont causé un préjudice grave pour une personne physique ou morale.

À noter que la modification de l'article 509-4 du Code pénal s'inscrit dans le cadre du maximum des peines d'emprisonnement fixées à l'article 9, paragraphe 4, de la directive précitée, à savoir un maximum d'au moins cinq ans.

Le plafond de l'amende reflète la nécessité de punir les infractions d'atteinte à l'intégrité d'un système ou des données par une sanction effective, proportionnée et dissuasive, adaptée au but poursuivi par leur auteur et le préjudice subi par une personne.

*

5. TEXTE PROPOSE PAR LA COMMISSION

Compte tenu de ce qui précède et pour donner suite à la suggestion du Conseil d'État, la Commission de la Justice recommande à la Chambre des Députés d'adopter le projet de loi n°8316 dans la teneur suivante :

*

PROJET DE LOI

portant modification du Code pénal en vue de la transposition de la directive 2013/40/UE du Parlement et du Conseil du 12 août 2013 relative aux attaques visant les systèmes d'information et remplaçant la décision-cadre 2005/222/JAI du Conseil

À l'article 509-4 du Code pénal est ajouté un alinéa 2 qui prend la teneur suivante :

« *Sera puni des mêmes peines, celui qui aura commis les infractions visées aux articles 509-1 à 509-3 contre un système d'information d'une infrastructure critique ou qui, par la commission de ces infractions, aura causé un préjudice grave à un tel système d'information.* »

Luxembourg, le 25 janvier 2024

Le Président,
Laurent MOSAR

Le Rapporteur,
Alex DONNERSBACH

Impression: CTIE – Division Imprimés et Fournitures de bureau

07

Chambre des Députés
GRAND-DUCHÉ DE LUXEMBOURG

CL/CSC P.V. JUST 07

Commission de la Justice

Procès-verbal de la réunion du 25 janvier 2024

La réunion a eu lieu par visioconférence.

Ordre du jour :

1. Approbation du projet de procès-verbal de la réunion du 21 décembre 2023

2. 8287 Projet de loi portant modification de la loi modifiée du 17 mars 2004 relative au mandat d'arrêt européen et aux procédures de remise entre Etats membres de l'Union européenne
   - Rapporteur : Monsieur Charel Weiler

   - Présentation et adoption d'un projet de rapport

3. 8316 Projet de loi portant modification du Code pénal aux fins de la transposition de la directive (UE) 2013/40 du Parlement et du Conseil du 12 août 2013 relative aux attaques visant les systèmes d'information et remplaçant la décision-cadre 2005/222/JAI du Conseil
   - Rapporteur : Monsieur Alex Donnersbach

   - Présentation et adoption d'un projet de rapport

4. Divers

*

Présents : M. Guy Arendt, Mme Simone Beissel, M. Dan Biancalana, Mme Liz Braz, M. Sven Clement, M. Alex Donnersbach, Mme Carole Hartmann, M. Fernand Kartheiser, Mme Paulette Lenert, M. Laurent Mosar, Mme Sam Tanson, M. Charel Weiler, Mme Stéphanie Weydert, M. Laurent Zeimet

M. Gil Goebbels, Mme Barbara Ujlaki, du Ministère de la Justice

Mme Jenny Thines, du groupe parlementaire CSV

M. Christophe Li, de l'Administration parlementaire

Excusés : M. Gérard Schockmel

M. Marc Baum, observateur délégué

Mme Elisabeth Margue, Ministre de la Justice

*

Présidence : M. Laurent Mosar, Président de la Commission

*

1. Approbation du projet de procès-verbal de la réunion du 21 décembre 2023

Le projet de procès-verbal sous rubrique recueille l'accord unanime des membres de la Commission de la Justice.

*

2. 8287 Projet de loi portant modification de la loi modifiée du 17 mars 2004 relative au mandat d'arrêt européen et aux procédures de remise entre Etats membres de l'Union européenne

Présentation et adoption d'un projet de rapport

M. Charel Weiler (Rapporteur, CSV) présente les grandes lignes de son projet de rapport. Ce projet de rapport ne suscite aucune observation particulière de la part des membres de la Commission de la Justice.

Vote

M. Fernand Kartheiser (ADR) s'abstenant, les Députés des groupes et sensibilités politiques CSV, DP, LSAP, déi gréng et Piraten votent en faveur du projet de rapport.

Temps de parole

Pour les débats en séance publique de la Chambre des Députés, il est proposé de recourir au modèle de base.

*

3. 8316 Projet de loi portant modification du Code pénal aux fins de la transposition de la directive (UE) 2013/40 du Parlement et du Conseil du 12 août 2013 relative aux attaques visant les systèmes d'information et remplaçant la décision-cadre 2005/222/JAI du Conseil

Présentation et adoption d'un projet de rapport

M. Alex Donnersbach (Rapporteur, CSV) présente les grandes lignes de son projet de rapport. Ce projet de rapport ne suscite aucune observation particulière de la part des membres de la Commission de la Justice.

Vote

M. Fernand Kartheiser (ADR) s'abstenant, les Députés des groupes et sensibilités politiques CSV, DP, LSAP, déi gréng et Piraten votent en faveur du projet de rapport.

Temps de parole

Pour les débats en séance publique de la Chambre des Députés, il est proposé de recourir au modèle de base.

*

4. Divers

Aucun point divers n'est soulevé.

Procès-verbal approuvé et certifié exact

Bulletin de vote n°6 - Projet de loi N°8316

Bulletin de Vote (Vote Public)

Date: 30/01/2024 17:52:55
Scrutin: 6
Vote: PL 8316 - Directive 2013-40-UE
Description: Projet de loi N°8316

Président: M. Wiseler Claude
Secrétaire Général: M. Scheeck Laurent

	Oui	Abst	Non	Total
Présents:	52	0	0	52
Procurations:	8	0	0	8
Total:	60	0	0	60

Nom du député	Vote	(Procuration)	Nom du député	Vote	(Procuration)
CSV					
Adehm Diane	Oui		Arendt épouse Kemp Nancy	Oui	
Bauer Maurice	Oui		Boonen Jeff	Oui	
Donnersbach Alex	Oui		Eicher Emile	Oui	
Eischen Félix	Oui		Galles Paul	Oui	
Hansen Christophe	Oui		Hengel Max	Oui	
Kemp Françoise	Oui		Lies Marc	Oui	(Mosar Laurent)
Modert Octavie	Oui	(Adehm Diane)	Morgenthaler Nathalie	Oui	
Mosar Laurent	Oui		Spautz Marc	Oui	
Weiler Charel	Oui		Weydert Stéphanie	Oui	
Wiseler Claude	Oui		Wolter Michel	Oui	(Arendt épouse Kemp Nancy)
Zeimet Laurent	Oui				
DP					
Agostino Barbara	Oui		Arendt Guy	Oui	
Bauler André	Oui		Baum Gilles	Oui	
Beissel Simone	Oui		Cahen Corinne	Oui	
Emering Luc	Oui		Etgen Fernand	Oui	(Bauler André)
Goldschmidt Patrick	Oui		Graas Gusty	Oui	
Hartmann Carole	Oui		Minella Mandy	Oui	
Polfer Lydie	Oui	(Agostino Barbara)	Schockmel Gérard	Oui	
LSAP					
Biancalana Dan	Oui		Bofferding Taina	Oui	(Cruchten Yves)
Braz Liz	Oui		Closener Francine	Oui	(Biancalana Dan)
Cruchten Yves	Oui		Delcourt Claire	Oui	
Di Bartolomeo Mars	Oui		Engel Georges	Oui	
Fayot Franz	Oui		Haagen Claude	Oui	
Lenert Paulette	Oui				
ADR					
Engelen Jeff	Oui		Kartheiser Fernand	Oui	
Keup Fred	Oui		Schoos Alexandra	Oui	
Weidig Tom	Oui				
déi gréng					
Bausch François	Oui		Sehovic Meris	Oui	(Bausch François)
Tanson Sam	Oui		Welfring Joëlle	Oui	

Bulletin de Vote (Vote Public)

Date: 30/01/2024 17:52:55
Scrutin: 6
Vote: PL 8316 - Directive 2013-40-UE
Description: Projet de loi N°8316

Président: M. Wiseler Claude
Secrétaire Général: M. Scheeck Laurent

	Oui	Abst	Non	Total
Présents:	52	0	0	52
Procurations:	8	0	0	8
Total:	60	0	0	60

Nom du député	Vote	(Procuration)	Nom du député	Vote	(Procuration)
Piraten					
Clement Sven	Oui		Goergen Marc	Oui	
Polidori Ben	Oui				
DÉI LÉNK					
Baum Marc	Oui		Wagner David	Oui	

Le Président:

Le Secrétaire Général:

Texte voté - projet de loi N°8316

Chambre des Députés
GRAND-DUCHÉ DE LUXEMBOURG

N° 8316

PROJET DE LOI

portant modification du Code pénal en vue de la transposition de la directive 2013/40/UE du Parlement et du Conseil du 12 août 2013 relative aux attaques visant les systèmes d'information et remplaçant la décision-cadre 2005/222/JAI du Conseil

*

À l'article 509-4 du Code pénal est ajouté un alinéa 2 qui prend la teneur suivante :

« *Sera puni des mêmes peines, celui qui aura commis les infractions visées aux articles 509-1 à 509-3 contre un système d'information d'une infrastructure critique ou qui, par la commission de ces infractions, aura causé un préjudice grave à un tel système d'information.* »

Projet de loi adopté par la Chambre des Députés
en sa séance publique du 30 janvier 2024

Le Secrétaire général, Le Président,

s. Laurent Scheeck s. Claude Wiseler

8316/03

N° 8316[3]

CHAMBRE DES DEPUTES

PROJET DE LOI

portant modification du Code pénal en vue de la transposition de la directive 2013/40/UE du Parlement et du Conseil du 12 août 2013 relative aux attaques visant les systèmes d'information et remplaçant la décision-cadre 2005/222/JAI du Conseil

* * *

DISPENSE DU SECOND VOTE CONSTITUTIONNEL PAR LE CONSEIL D'ETAT

(6.2.2024)

Le Conseil d'État,

appelé par dépêche du Président de la Chambre des députés du 30 janvier 2024 à délibérer sur la question de dispense du second vote constitutionnel du

PROJET DE LOI

portant modification du Code pénal en vue de la transposition de la directive 2013/40/UE du Parlement et du Conseil du 12 août 2013 relative aux attaques visant les systèmes d'information et remplaçant la décision-cadre 2005/222/JAI du Conseil

qui a été adopté par la Chambre des députés dans sa séance du 30 janvier 2024 et dispensé du second vote constitutionnel ;

Vu ledit projet de loi et l'avis émis par le Conseil d'État en sa séance du 24 octobre 2023 ;

se déclare d'accord

avec la Chambre des députés pour dispenser le projet de loi en question du second vote prévu par l'article 78, paragraphe 4, de la Constitution.

Ainsi décidé en séance publique à l'unanimité des 17 votants, le 6 février 2024.

Pour le Président,
Le Vice-Président,
Patrick SANTER

Le Secrétaire général,
Marc BESCH

Impression: CTIE – Division Imprimés et Fournitures de bureau

Mémorial A N° 83 de 2024

JOURNAL OFFICIEL

DU GRAND-DUCHÉ DE LUXEMBOURG

MÉMORIAL A

N° 83 du 4 mars 2024

Loi du 28 février 2024 portant modification du Code pénal en vue de la transposition de la directive 2013/40/UE du Parlement et du Conseil du 12 août 2013 relative aux attaques visant les systèmes d'information et remplaçant la décision-cadre 2005/222/JAI du Conseil.

Nous Henri, Grand-Duc de Luxembourg, Duc de Nassau,

Vu la Directive 2013/40/UE du Parlement et du Conseil du 12 août 2013 relative aux attaques visant les systèmes d'information et remplaçant la décision-cadre 2005/222/JAI du Conseil ;

Le Conseil d'État entendu ;

Vu l'adoption par la Chambre des Députés ;

Vu la décision de la Chambre des Députés du 30 janvier 2024 et celle du Conseil d'État du 6 février 2024 portant qu'il n'y a pas lieu à second vote ;

Avons ordonné et ordonnons :

À l'article 509-4 du Code pénal est ajouté un alinéa 2 qui prend la teneur suivante :

« Sera puni des mêmes peines, celui qui aura commis les infractions visées aux articles 509-1 à 509-3 contre un système d'information d'une infrastructure critique ou qui, par la commission de ces infractions, aura causé un préjudice grave à un tel système d'information. »

Mandons et ordonnons que la présente loi soit insérée au Journal officiel du Grand-Duché de Luxembourg pour être exécutée et observée par tous ceux que la chose concerne.

La Ministre de la Justice,
Elisabeth Margue

Palais de Luxembourg, le 28 février 2024.
Henri

Doc. parl. 8316 ; sess. ord. 2022-2023 et législature 2023-2028 ; Dir. 2013/40/UE.

Résumé

Résumé du projet de loi n°8316

Des systèmes d'information performants sont tout aussi indispensables à la liberté, à la sécurité et à la justice d'un État qu'à la lutte contre la cybercriminalité. Afin de garantir un niveau de protection adéquat des systèmes d'information des États membres de l'Union européenne, le Parlement européen et le Conseil ont adopté en date du 12 août 2013, la directive 2013/40/UE relative aux attaques contre les systèmes d'information et remplaçant la décision-cadre 2005/222/JAI du Conseil.

Au plan national, cette directive a été transposée par la loi du 18 juillet 2014 portant 1) approbation de la Convention du Conseil de l'Europe sur la cybercriminalité, ouverte à la signature à Budapest le 23 novembre 2001, 2) approbation du Protocole additionnel à la Convention sur la cybercriminalité, relatif à l'incrimination des actes de nature raciste et xénophobe commis par le biais de systèmes informatiques, fait à Strasbourg le 28 janvier 2003, 3) modification du Code pénal, 4) modification du Code d'instruction criminelle, 5) modification de la loi modifiée du 30 mai 2005 concernant la protection de la vie privée dans le secteur des communications électroniques.

La Commission européenne a toutefois constaté que le Luxembourg avait transposé de manière incorrecte l'article 9, paragraphe 4, notamment le point b), de la directive, lequel impose aux États membres de prendre les mesures nécessaires pour que les infractions d'atteinte à l'intégrité d'un système d'information et à l'intégrité des données visées aux articles 4 et 5 de la directive soient passibles d'une peine maximale d'au moins cinq ans d'emprisonnement lorsqu'elles sont commises dans le cadre d'une organisation criminelle, qu'elles causent un préjudice grave ou qu'elles sont commises contre un système d'information d'une infrastructure critique.

Il a donc été recommandé au Luxembourg d'élaborer une disposition légale permettant une application conforme et plus littérale du droit européen. De ce fait, ce projet de loi prévoit ainsi d'inclure les circonstances aggravantes prévues par la directive, tout en y appliquant une sanction efficace, proportionnée et dissuasive. *In fine*, il appartient aux autorités judiciaires d'apprécier au cas par cas s'il s'agit ou non d'une circonstance aggravante.