

N°8316

CHAMBRE DES DÉPUTÉS

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

* * *

RAPPORT DE LA COMMISSION DE LA JUSTICE

(25.01.2024)

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. Antécédents

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'État

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 proposé 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,
M. Laurent MOSAR

Le Rapporteur,
M. Alex DONNERSBACH