ASSEMBLÉE NATIONALE

28 octobre 2022

D’ORIENTATION ET DE PROGRAMMATION DU MINISTÈRE DE L’INTÉRIEUR - (N° 343)

Tombé

AMENDEMENT

N º CL438

présenté par
M. Pradal, M. Lemaire, Mme Moutchou, Mme Poussier-Winsback, M. Albertini, M. Alfandari, Mme Bellamy, M. Benoit, Mme Carel, M. Christophe, M. Favennec-Bécot , M. Gernigon, Mme Félicie Gérard, M. Jolivet, M. Kervran, Mme Kochert, M. Lamirault, M. Larsonneur, Mme Le Hénanff, Mme Magnier, M. Marcangeli, M. Mesnier, M. Patrier-Leitus, M. Plassard, M. Portarrieu, Mme Rauch, M. Thiébaut, M. Valletoux, M. Villiers, Mme Violland et les membres du groupe Horizons et apparentés

---

ARTICLE ADDITIONNEL

APRÈS L'ARTICLE 4, insérer l'article suivant:

Le chapitre III du titre II du livre III du code pénal est ainsi modifié :

1° L’article 323-1 est complété par un alinéa ainsi rédigé :

« Lorsque les infractions prévues aux deux premiers alinéas ont été commises à l’encontre d’un système de traitement automatisé de données à caractère personnel mis en œuvre par l’État et ont eu pour objet ou pour effet la mise en danger de la vie d’autrui, la peine est portée à sept ans d’emprisonnement et à 300 000 € d’amende. » ;

2° L’article 323-2 est complété par un alinéa ainsi rédigé :

« Lorsque cette infraction a été commise l’encontre d’un système de traitement automatisé de données à caractère personnel mis en œuvre par l’État et ont eu pour objet ou pour effet la mise en danger de la vie d’autrui, la peine est portée à dix ans d’emprisonnement et à 300 000 € d’amende. » ;

3° L’article 323-3 est complété par un alinéa ainsi rédigé :

« Lorsque cette infraction a été commise à l’encontre d’un système de traitement automatisé de données à caractère personnel mis en œuvre par l’État et ont eu pour objet ou pour effet la mise en danger de la vie d’autrui, la peine est portée à dix ans d’emprisonnement et à 300 000 € d’amende. »

EXPOSÉ SOMMAIRE

Le présent amendement vise à aggraver les sanctions encourues en cas de cyber-attaque dirigée vers les établissements publics et qui auraient pour objet ou pour effet la mise en danger de la vie d'autrui. Cela permettrait non seulement de sanctionner plus durement les auteurs de cyberattaques qui s'attaquent consciemment à des hôpitaux mettant ainsi en danger de la vie des patients ; mais également tout autre système d'information de l'Etat dont la perturbation conduirait à mettre en danger la vie de nos concitoyens. Tel est le cas du Data center du Ministère des Armées ou encore les réseaux du Ministère de l'Intérieur.

Les nouvelles menaces auxquelles sont confrontées les établissements publics et en particulier les hôpitaux sont intolérables. Les données de santé entre autres, ont une grande valeur sur le marché de la donnée, ce qui conduit malheureusement à faire des hôpitaux des cibles de choix. Or, s'il convient d'accompagner ces établissements dans la sécurisation de leurs systèmes, il est également nécessaire de renforcer la dissuasion lorsque la vie des patients peut être directement impactée.

L'exemple récent de la cyber-attaque dont l'hôpital de Corbeil-Essonnes a été victime, alors que la crise sanitaire perdure, en est une preuve flagrante : pendant deux mois, le système informatique a été paralysé. Il a fallu, dans ces 110 000 mètres carrés de salles, de chambres et de couloirs, se passer d’outils, de logiciels et de dossiers numériques, et revenir à l’« époque d’avant », comme dit le personnel. Celle du stylo et du papier. Les temps de prise en charge au sein des urgences pédiatriques ont été rallongés et une régulation des patients a du être mise en place. C'est absolument intolérable.

Si s'attaquer à un système d'information de l'Etat constitue déjà une circonstance aggravante prévue par notre code pénal, il nous semble plus que nécessaire que la mise en danger de la vie d'autrui conduise à une aggravation de peine, il en va de la sécurité et de la santé de nos concitoyens.