ASSEMBLÉE NATIONALE

28 octobre 2022

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

Tombé

AMENDEMENT

N º CL286

présenté par
M. Bothorel

ARTICLE 4

I. – À l’alinéa 4, supprimer les mots :

« le paiement d’une rançon par l’assuré dans le cadre d’une extorsion prévue à l’article 312-1 du code pénal, lorsqu’elle est commise au moyen d’ ».

II. – En conséquence, au même alinéa 4, substituer aux mots :

« même code »

les mots :

« code pénal ».

III. – En conséquence, audit alinéa 4, substituer au mot :

« pré-plainte »

le mot :

« plainte ».

IV. – En conséquence, à la fin du même alinéa 4, substituer aux mots :

« dans les 24 heures suivant l’attaque et avant tout paiement de cette rançon »

les mots :

« au plus tard quarante-huit heures après la constatation de l’atteinte ».

EXPOSÉ SOMMAIRE

Cet article traduit une double objectif légitime de la part du Gouvernement. D'abord, conforter et protéger le marché français de l'assurance en ouvrant explicitement par la loi la couverture assurantielle des risques cyber, évitant ainsi que les entreprises se couvrent hors de France. Ensuite, améliorer la visibilité sur la cybercriminalité en conditionnant le bénéfice de la couverture assurantielle à une déclaration aux autorités.

Toutefois, la rédaction en l'état aurait des conséquences graves pour les entreprises et pour la sécurité nationale, puisqu'elle conforte le modèle de rentabilité des cyberattaques en prévoyant leur financement (paiement de la rançon). Les cibles françaises deviendraient alors un choix privilégié pour les cyberattaquants.

L'abaissement du délai de 48 à 24h voté par le Sénat ajoute une contrainte formelle bureaucratique et un risque de fuite informationnelle à la situation de crise engendrée par une cyberattaque, qui rend de facto inutilisable l'informatique de l'entreprise. Le délai de 48h semble plus réaliste pour permettre à l'entreprise attaquée de parer aux premiers effets et d'effectuer les démarches obligatoires (notamment en cas de perte de données personnelles, de données de santé, etc.).

Au-delà, en introduisant dans la loi l'idée selon laquelle une rançon peut être payée, c'est toute la doctrine de la France (« la France ne paye pas de rançon ») qui est remise en cause. Le paiement de rançons deviendrait pour notre pays une question de modalités et plus une question de principe : ce signal serait compris de tous, y compris des groupes terroristes, mettant ainsi potentiellement en danger nos compatriotes qui vivent à l'étranger. La France devra également assumer le financement potentiel du crime organisé, du terrorisme ou de l'action offensive de gouvernements étrangers hostiles.

Par conséquent, le présent amendement propose une nouvelle rédaction de l'article 4 qui supprime la référence au paiement de la rançon et reste ainsi fidèle à la doctrine de la France. Les assureurs disposeront d'une marge de manœuvre supplémentaire puisque l'article ainsi rédigé couvre l'ensemble des conséquences de l'atteinte aux systèmes d'information, notamment la perte d'exploitation. L'assureur pourra donc imposer plus facilement au souscripteur certaines mesures de sécurité informatique. Enfin, la couverture assurantielle pour les attaques n'incluant pas de demande de rançon serait également soumise à déclaration aux autorités, ce qui permet aux services de l'État concernés d'avoir une visibilité supérieure par rapport à la rédaction initiale.