HEXATRUST
CLOUD CONFIDENCE & CYBERSECURITY

PROPOSITION DE LOI VISANT À SORTIR LA FRANCE DU PIÈGE DU NARCOTRAFIC
POSITION PAPER – ARTICLE 8 TER
CHIFFREMENT DES APPLICATIONS DE MESSAGERIES CHIFFRÉES

Déposée par les sénateurs Étienne BLANC (LR) et Jérôme DURAIN (PS), **la proposition de loi visant à sortir la France du piège du narcotrafic a été adoptée par le Sénat le 4 février dernier**. Au cours de l'examen en séance publique, un amendement cosigné par 80 sénateurs LR, UC et RDPI, a été adopté pour créer l'article 8 ter.

Contre l'avis de la Commission et du rapporteur, arguant de l'absence de toute étude d'impact, mais avec le soutien du Gouvernement, l'**article prévoit "*pour les plateformes une obligation de mettre en œuvre les mesures techniques nécessaires afin de permettre aux services de renseignement d'accéder au contenu intelligible des correspondances et données qui y transitent*.** *Cet accès serait limité aux seules correspondances et données ayant fait l'objet d'une autorisation spécifique de mise en œuvre des techniques de recueil de renseignement, après avis de la CNCTR*". Il s'agit, en somme, de rendre possible les *back doors*, permettant un accès aux contenus des conversations.

Un tel dispositif, s'il venait à être définitivement mis en place entraînerait un double recul : un **recul des libertés individuelles** et un recul des **capacités de protection dans l'espace numérique**. Hexatrust entend alerter le législateur sur sur **la remise en cause profonde de la sécurité des échanges électroniques qu'impliquerait** cette proposition, véritable boîte de pandore en matière de cybersécurité.

Une atteinte au droit à la vie privée et aux libertés fondamentales

Pour Hexatrust et ses membres, il semble urgent de revenir sur l'introduction potentielle de *backdoors* qui reviendrait **à remettre en cause les engagements français et européens en matière de protection des libertés personnelles dans l'espace numérique**.

Interrogée sur l'amendement adopté par le Sénat avec le soutien du gouvernement, la CNIL, tout en précisant n'avoir pas été consulté sur cette disposition, a rappelé que le Comité européen de la protection des données (EDPB) estimait "***que les technologies de chiffrement contribuent de manière fondamentale au respect de la vie privée et de la confidentialité des communications,*** *à la liberté d'expression, ainsi qu'à l'innovation et à la croissance de l'économie numérique. Dès lors, aucune disposition ne devrait pouvoir être interprétée comme interdisant ou affaiblissant le chiffrement*".

Alors que l'accès aux métadonnées des échanges est suffisant pour prouver l'existence de liens entre deux individus ou deux structures dans le cadre d'une enquête judiciaire, Hexatrust estime que la facilitation des enquêtes n'est **pas un argument suffisant pour remettre en cause le droit à la confidentialité des correspondances privées** garanties par la Convention Européenne des Droits de l'Homme.

Une remise en cause de la sécurité des communication dans l'espace numérique

Qu'ils s'agissent de solutions destinées au grand public ou au contraire à un usage professionnel, qu'elles soient européennes ou extra-européennes, les applications de messagerie proposent largement le chiffrage de bout-en-bout des conservations. Dans ce contexte, la clef de chiffrement n'est uniquement détenue que par les interlocuteurs et l'application n'a accès qu'aux métadonnées liées aux conversations - qui échange avec qui, quand, etc.

L'introduction des backdoors aurait pour conséquence de créer volontairement une faille en laissant à un agent tiers, qu'il s'agisse de l'entreprise proposant le service ou d'un tiers de confiance, **la possibilité d'accéder après déchiffrement au contenu des échanges**.

De fait, le chiffrement de bout-en-bout ne serait donc plus que théorique et viendrait remettre en cause l'intérêt de ces solutions au profit de solutions "classiques" de messagerie au sens où le niveau de protection cyber serait moindre. Cette alerte avait déjà été formulée en 2016 par Guillaume POUPARD, alors DG de l'ANSSI. Pour lui, "l'affaiblissement des mécanismes cryptographiques ou bien l'introduction volontaire de mécanismes de contournement sont systématiquement susceptibles d'être exploités par des attaquants aux profils variés".

De même les autorités européennes de protection des données comme le Comité européen de la protection des données (EDPB) et le Contrôleur européen de la protection des données (CEPD) ont rappelé qu'imposer la création de backdoor **risquerait de conduire à l'abandon du chiffrement de bout-en-bout, avec pour conséquence**. Il en résulterait **une dégradation substantielle de la confidentialité et de la sécurité des échanges par voie électronique**. A titre d'exemple, l'approche Zero Trust en cybersécurité, aujourd'hui largement reconnue comme un des plus performantes pour garantir la sécurité des entités dans l'espace numérique, verrait une partie de son concept rendu inapplicable en cas d'abandon du chiffrement de bout-en-bout.

Le dispositif serait donc **une remise en cause globale de la sécurité de la communication numérique l'ensemble des acteurs publics et privés français, et de celles de nos concitoyens**.

Une risque pour la sécurité nationale ainsi que du secret des affaires

Conséquence de cet affaiblissement, la mesure portée par les sénateurs fait peser **une forte menace sur la sécurité nationale et le secret des affaires**. Car, une *backdoors*, si elle est

utilisable par les institutions désignées par la loi pour accéder aux conversations, **peut également être accessible par un acteur malveillant**. Il est en effet techniquement impossible d'assurer que ce dispositif ne bénéficie qu'aux personnes autorisées. L'ensemble des experts s'accordent même sur le fait que les mécanismes de contournement des technologies de cryptologie sont systématiquement exploités par des attaquants. Le chiffrement intégral reste donc l'unique moyen permettant d'assurer **la sécurisation des échanges sensibles.**

Ainsi, alors que la Suède s'interroge elle aussi sur le même mécanisme, l'armée suédoise a interpellé le Gouvernement en s'opposant à cette proposition[1], rappelant que quelle que soit la solution utilisée par les forces armées suédoises, l'introduction d'un super-administrateur doté des clés de chiffrement et ayant la possibilité d'accéder au contenu des conversations grâce à celles-ci viendrait à créer une faille.

L'exemple étasunien Clipper chip est également la preuve que ces mécanismes ne sont jamais sans danger. En effet, ce programme de la NSA, qui visait à équiper les appareils électroniques destinés au grand public d'une puce de sécurité dont les services secrets auraient la clef de chiffrement, a été arrêté après la découverte d'une faille importante de cybersécurité.

Si la crainte se pose sur les **échanges sensibles concernant l'État**, il en va de même pour les échanges professionnels qui doivent être couverts **par le secret des affaires**. Dans le contexte géopolitique actuel, peut-on réellement se permettre d'intégrer des failles connues de tous, y compris des cyberdélinquants étatiques ou privés, et faciliter l'espionnage industriel ?

[1] Communication des Forces armées suédoises, consulté le 28.02.2025, disponible ici.