

ASSEMBLÉE NATIONALE

14 mars 2025

SORTIR LA FRANCE DU PIÈGE DU NARCOTRAFIC - (N° 1043)

Commission	
Gouvernement	

Rejeté

AMENDEMENT

N° 846

présenté par
M. Midy

ARTICLE 8 TER

Rétablir cet article dans la rédaction suivante :

« I. – Le code de la sécurité intérieure est ainsi modifié :

« 1° Le premier et le second alinéas de l'article L. 871-1 sont remplacés par les dispositions suivantes :

« « I. – Les opérateurs et personnes mentionnés à l'article L. 851-1 qui fournissent des prestations de cryptologie assurant une fonction de confidentialité, sont tenus de permettre, dans un délai n'excédant pas 72 heures, aux seuls agents autorisés, d'accéder au contenu intelligible des seuls informations, documents, données ou renseignements dont la collecte a fait l'objet, conformément à l'article L. 821-4, d'une autorisation préalable de mise en œuvre de l'une des techniques de recueil de renseignement mentionnées aux articles L. 851-1, L. 851-2 et L. 852-1.

« « II. – Les dispositifs techniques des opérateurs et personnes mentionnés au I leur permettant de satisfaire à cette obligation sont autorisés par le Premier ministre, préalablement à leur mise en œuvre, dans les conditions définies pour l'application du 1° de l'article 226-3 du code pénal.

« « Ces dispositifs techniques préservent le secret des correspondances et assurent la protection des données à caractère personnel au titre du respect de la vie privée, conformément à l'article L. 801-1. Ils doivent exclure toute possibilité d'accès par une personne autre que les agents autorisés à mettre en œuvre les techniques de recueil de renseignement mentionnées au I. Ces dispositifs techniques ne peuvent porter atteinte à la prestation de cryptologie visant à assurer une fonction de confidentialité.

« « Les opérateurs et personnes mentionnés au I ne peuvent exciper d'arguments contractuels ou techniques pour faire obstacle à cette obligation.

« « Un décret en Conseil d'État définit les conditions d'application du présent article, notamment les conditions d'autorisation des dispositifs techniques par le Premier ministre et de prise en charge financière par l'État des mesures techniques mises en œuvre. »

« 2° L'article L. 871-3 est abrogé ;

« 3° L'article L. 871-4 est ainsi modifié :

« a) Au premier alinéa, les mots : « de communications électroniques mentionnés à l'article L. 34-1 du code des postes et des communications électroniques ainsi que les personnes mentionnées aux 1 et 2 du I de l'article 6 de la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique » sont remplacés par les mots : « et personnes mentionnées à l'article L. 851-1 » ;

« b) À la fin du second alinéa, les mots : « ces opérations » sont remplacés par les mots : « cette mise en œuvre ».

« 4° L'article L. 871-5 est abrogé.

« 5° L'article L. 871-6 est ainsi modifié :

« a) Après la première occurrence du mot : « Les », sont insérés les mots : « opérateurs et personnes mentionnés à l'article L. 851-1 procèdent aux » ;

« b) Les mots : « dans les locaux et installations des services ou organismes placés sous l'autorité ou la tutelle du ministre chargé des communications électroniques ou des exploitants de réseaux ou fournisseurs de services de communications électroniques ne peuvent être effectuées que sur » sont remplacés par le signe et le mot : « . Sur » ;

« c) La seconde occurrence du mot : « par » est remplacée par les mots : « , les opérateurs et personnes mentionnés à l'article L. 851-1 fournissent dans les meilleurs délais les informations, documents, données ou renseignements requis. Si l'ordre le prévoit, son exécution est confiée à » ;

« d) Les mots : « services, organismes, exploitants ou fournisseurs » sont remplacés par les mots : « opérateurs ou personnes » ;

« e) Sont ajoutés les mots : « et dans le respect du secret de la défense nationale » ;

« 6° À l'article L. 871-7, les mots : « à la mise en œuvre des techniques de recueil de renseignement mentionnées aux articles L. 851-1, L. 851-2 à L. 851-4, L. 851-6, L. 852-1 et L. 853-2 » sont remplacés par les mots : « aux obligations prévues par l'article L. 871-6 » ;

« 7° À l'article L. 881-1, les mots : « , 226-14 » sont supprimés ;

« 8° L'article L. 881-2 est ainsi modifié :

« a) Au premier alinéa, les mots : « au premier alinéa de l'article L. 871-1 et à l'article L. 871-4 » sont remplacés par les mots : « aux articles L. 871-1, L. 871-2, L. 871-4 et L. 871-6 » ;

« b) Le second alinéa est ainsi rédigé :

« Lorsque ces infractions sont commises à titre habituel, elles sont punies d'une amende de 1 500 000 euros. Pour les personnes morales, cette amende peut être portée à 2 % du chiffre d'affaires mondial moyen annuel hors taxes, calculé sur les trois derniers exercices annuels connus à la date des faits. ».

« II. – Le code des postes et des communications électroniques est ainsi modifié :

« 1° L'article L. 33-1 est ainsi modifié :

« a) Le e du I est ainsi modifié :

« – La première occurrence du mot : « et » est remplacée par le signe : « , » ;

« – Après la première occurrence du mot : « publique », sont insérés les mots : « et la protection des intérêts fondamentaux de la Nation » ;

« – Après la seconde occurrence des mots : « publique », sont insérés les mots : « ou de la protection des intérêts fondamentaux de la Nation » ;

« b) Le 1° du VII est ainsi modifié :

« – Après le mot : « Futuna », sont insérés les mots : « , dans les Terres australes et antarctiques françaises » ;

« – Sont ajoutés les mots : « et de la loi n° XXXX du xxx » ;

« 2° Le chapitre II du titre I^{er} du livre est complété par une section 10 ainsi rédigée :

« *Section 10*

« *Des prescriptions exigées par l'ordre public, la défense nationale, la sécurité publique ou la protection des intérêts fondamentaux de la Nation*

« *Art. L. 34-18. – I. – Aux fins de respecter les prescriptions mentionnées au e) du I de l'article L. 33-1, les opérateurs et les personnes mentionnées au 2 du I de l'article 6 de la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique mettent en place ou assurent la mise en œuvre des moyens nécessaires pour exécuter, s'il y a lieu, dans le respect du secret de la défense nationale, les techniques d'enquête numérique judiciaires autorisées en application des dispositions de la section 3 du chapitre I^{er} du titre III du livre I^{er} du code de procédure pénale et des sections 5 et 6 du chapitre II du titre XXV du livre IV du même code, ainsi que les techniques de recueil de renseignement et demandes formulées en application du livre VIII du code de la sécurité intérieure.*

« Ils se mettent à même de répondre aux réquisitions des agents autorisés et des autorités judiciaires compétentes, sans pouvoir exciper d'arguments contractuels ou techniques qui y feraient obstacle.

« II. – Ces moyens sont mis en place et mis en œuvre dans les conditions suivantes :

« – Ils sont validés au préalable par l'État ;

« – Ils sont mis en place sur le territoire national et mis en œuvre depuis le territoire national ;

« – Les données produites par les systèmes utilisés sont chiffrées par un moyen validé par l'État lorsque ces données doivent transiter par voie électronique en dehors du territoire national ;

« – Seuls des agents spécialement désignés et qualifiés des personnes mentionnées au I du présent article ou des agents désignés par l'autorité administrative peuvent mettre en place et assurer la mise en œuvre de ces moyens et accéder aux données qu'ils traitent.

« III. – Les garanties de la juste rémunération prévue au e) du I de l'article L. 33-1, sont définies par décret en Conseil d'État.

« IV. – À titre exceptionnel, le ministre chargé des communications électroniques peut, après avoir recueilli l'avis de l'Autorité de régulation des communications électroniques, des postes et de la distribution de la presse et de l'Agence nationale de la sécurité des systèmes d'information, autoriser un opérateur ou une personne mentionnée au 2 du I de l'article 6 de la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique à déroger aux obligations prévues au II du présent article lorsque les coûts à exposer pour satisfaire à ces conditions sont disproportionnés au regard du nombre de demandes adressées à cet opérateur ou à la personne mentionnée au 2 du I de l'article 6 de la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique.

« *Art. L. 34-19.* – Dans le cadre des attributions qui lui sont conférées par le présent livre, le ministre chargé des communications électroniques veille notamment à ce que les opérateurs prennent les mesures nécessaires pour assurer l'application, s'il y a lieu, dans le respect du secret de la défense nationale, des dispositions du livre VIII du code de la sécurité intérieure, de la section 3 du chapitre I^{er} du titre III du livre I^{er} du code de procédure pénale relatives aux interceptions de correspondances émises par la voie des télécommunications ordonnées par l'autorité judiciaire et des sections 5 et 6 du chapitre II du titre XXV du livre IV du même code.

« *Art. L. 34-20.* – En cas de méconnaissance des dispositions prévues à l'article L. 34-18, le Premier ministre peut mettre en demeure les personnes morales défailtantes mentionnées audit article de se mettre en conformité avec leurs obligations dans un délai qu'il fixe et qui ne peut être inférieur à quinze jours.

« En cas de méconnaissance des termes de cette mise en demeure, le Premier ministre peut fixer un nouveau délai en l'assortissant d'une astreinte dont le montant ne peut excéder 50 000 euros par jour de retard.

« S'il constate que la procédure mentionnée au précédent aliéna n'a pas abouti à la mise en conformité exigée, le Premier ministre peut :

« 1° Lorsque la personne en cause est un opérateur de communications électroniques, prendre une décision à effet immédiat de suspension totale ou partielle du droit d'établir un réseau de

communications électroniques ou de fournir un service de communications électroniques sur le territoire national pour une durée d'un mois au plus ;

« 2° Lorsque la personne en cause est l'une des personnes mentionnées au 2 du I de l'article 6 de la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique, prendre une décision à effet immédiat de suspension totale ou partielle de son activité sur le territoire national, pour une durée d'un mois au plus.

« La décision du Premier ministre est prise après que l'opérateur ou la personne mentionnée au 2 du I de l'article 6 de la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique a été mis en capacité de présenter des observations dans un délai minimal de quinze jours.

« Le Premier ministre peut renouveler les décisions mentionnées aux quatrième et cinquième alinéas si, aux termes du délai d'un mois, la personne concernée refuse de se mettre en conformité avec les dispositions prévues à l'article L. 34-18. Il peut l'assortir d'une astreinte dont le montant ne peut excéder 50 000 euros par jour de retard.

« En cas d'urgence, de circonstances exceptionnelles ou d'atteinte imminente à la sécurité nationale, le Premier ministre peut prendre les décisions mentionnées aux quatrième et cinquième alinéas sans qu'aient été préalablement prononcées les mises en demeure mentionnées aux premier et deuxième alinéa. Les conditions d'application du présent article sont déterminées par décret en Conseil d'État.

« *Art. L. 34-21.* – Les exigences essentielles définies au 12° de l'article L. 32 et le secret des correspondances mentionné à l'article L. 32-3 ne sont opposables ni aux juridictions compétentes pour ordonner des interceptions en application de l'article 100 du code de procédure pénale, ni au ministre chargé des communications électroniques dans l'exercice des prérogatives qui leur sont dévolues par le présent livre VIII du code de la sécurité intérieure.

« *Art. L. 34-22.* – Les dispositions de la présente section sont applicables en Polynésie française, dans les îles Wallis et Futuna, dans les Terres australes et antarctiques françaises et en Nouvelle-Calédonie. »

EXPOSÉ SOMMAIRE

En Commission, a été supprimé l'article 8 ter de la proposition de loi qui avait été introduit, au Sénat et qui récrivait l'article L. 871-1 du code de la sécurité intérieure, pour passer d'une logique d'exigence de déchiffrement généralisé des communications au bénéfice des autorités publiques à une exigence de fourniture des seuls contenus des correspondances que la loi autorise les services de renseignement à réquisitionner.

Ce faisant, l'article rééquilibrait les obligations des opérateurs de messageries tout en assurant la conventionalité du dispositif, notamment suite à l'arrêt CEDH, 13 février 2024, Podchasov c. Russie qui, tout en reconnaissant la légitimité des interceptions, en raison notamment des impératifs de protection de la sécurité nationale et de la sûreté publique ou de prévention des infractions pénales, interdisait une réglementation aboutissant à une atteinte généralisée au chiffrement au bénéfice des services de sécurité.

Les débats en Commission ont mis en évidence la crainte que ces dispositions n'aboutissent à une obligation d'affaiblir les technologies de chiffrement mises en œuvre par les opérateurs de messageries électroniques, qui sont une garantie de libertés publiques fondamentales.

A ce titre, les travaux réalisés pour parvenir à cet amendement se sont assurés que la rédaction proposée interdit sans ambiguïté toute solution technique qui reposerait sur la création d'une « porte dérobée » (ou « backdoor »), susceptible d'affaiblir le chiffrement.

Le présent amendement propose donc de rétablir partiellement l'article 8 ter, en opérant la modification permettant de ne cibler que les seules correspondances qui font l'objet d'une autorisation d'interception par les services de renseignement. Il ajoute des garanties claires quant au fait que la technologie mise en œuvre pour permettre ces interceptions préserve le secret des correspondances et assure la protection des données à caractère personnel au titre du respect de la vie privée, conformément à l'article L.801-1 du même code.

Pour ce faire, la solution retenue par les personnes physiques ou morales mentionnées devra respecter ces exigences afin d'être validée par l'autorité administrative compétente préalablement à son utilisation, après avis d'une commission constituée d'administrations expertes et d'une autorité administrative indépendante, la CNCTR (commission nationale de contrôle des techniques de renseignement[1]). Ces solutions feront en outre l'objet d'une compensation financière, dont les modalités seront définies dans le décret.

Le présent amendement explicite en outre dans la loi le fait que les dispositifs techniques mis en œuvre sont soumis à autorisation préalable du Premier ministre selon les modalités définies par l'article R.226-3 du code pénal soit après avis de la commission dite R.226-2[2], dans l'objectif de limiter l'atteinte portée au secret des correspondances et à la vie privée aux seules correspondances visées par l'autorisation légale. Cette commission est présidée par le directeur général de l'ANSSI.

L'amendement énonce explicitement les critères à respecter pour garantir le respect de ces libertés :

- les dispositifs techniques doivent exclure toute possibilité d'accès par une personne autre que les agents autorisés à mettre en œuvre les techniques de recueil de renseignement au contenu intelligible des informations, documents, données ou renseignements concernés ;
- ces dispositifs techniques ne peuvent porter atteinte à la prestation de cryptologie visant à assurer une fonction de confidentialité.

Ainsi, cette rédaction interdit sans ambiguïté toute solution technique qui reposerait sur la création d'une « porte dérobée » (ou « backdoor »), susceptible d'affaiblir le chiffrement, solution qui ne correspond d'ailleurs absolument pas aux attentes de l'Etat.

Les services experts de l'Etat en matière de technologies de l'information et de la communication, en matière d'interception et en matière de cybersécurité garantissent qu'il existe bien des solutions techniques qui présentent deux garanties :

1. elles ne portent aucunement atteinte au protocole de chiffrement de bout en bout, qui prémunit contre toute interception du flux d'information par un tiers non autorisé,
2. elles demeurent exécutées par les opérateurs de messageries eux-mêmes, qui agissent ainsi sur réquisition légale des services de renseignement : sur autorisation du Premier ministre, après avis de la CNCTR (et après saisine automatique du Conseil d'Etat en cas d'avis défavorable de la CNCTR, ce qui ne s'est jamais produit à ce jour).

Par ailleurs, la disposition réécrite par le présent amendement restreint très strictement la portée de l'obligation de transmission de contenu imposée aux seules trois techniques de recueil de renseignement suivantes : le recueil de données de connexion (article L. 851-1), l'accès aux données de connexion en temps réel (article L.851-2) et les interceptions de sécurité (article L. 852-1).

Pour assurer un meilleur respect de ces exigences de coopération modernisées, les dispositions proposées renforcent les sanctions pénales applicables aux personnes physiques et morales qui refuseraient de s'acquitter de leurs obligations en la matière. Elles portent à 1.500.000 euros le montant de l'amende encourue pour les personnes physiques commettant ces infractions de manière habituelle et d'une amende pouvant atteindre jusqu'à 2% du chiffre d'affaires mondial annuel hors taxes, les personnes morales se trouvant dans la même situation. Le montant de ces sanctions correspond à celui qui a été retenu, pour des infractions de nature équivalente en matière judiciaire, par l'Union européenne dans le règlement 2023/1543 (eEvidence).

A cet égard, l'interpellation récente du fondateur de plateforme Telegram montre que le levier répressif est susceptible de fournir des résultats opérationnels tangibles puisque la coopération de cette plateforme avec l'autorité judiciaire s'est depuis nettement améliorée.

Par ailleurs, sans modifier le droit applicable, dans l'attente de la transposition du paquet européen eEvidence, par souci de lisibilité et de cohérence légistique, le présent article prévoit le déplacement des dispositions applicables aux réquisitions de données émanant de l'autorité judiciaire dans le code de procédure pénale et dans le code des postes et des communications électroniques.

Dans le même temps, les évolutions envisagées du Code des poste et des communications électroniques (CPCE) consistent à créer une nouvelle section consacrée aux « prescriptions exigées par l'ordre public, la défense nationale, la sécurité publique ou la sauvegarde des intérêts fondamentaux de la Nation ».

Les dispositions de cette section reprennent une partie des dispositions règlementaires du CPCE (article D.98-7) actuellement applicables aux personnes exploitant un réseau de communications électroniques ou fournissant des services de communications électroniques et les personnes mentionnées au 2 du I de l'article 6 de la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique afin d'élever le niveau de norme applicable. Il s'agit d'inscrire dans la loi l'obligation pour les personnes précitées d'assurer la mise en place des moyens techniques requis préalablement à l'exécution des réponses aux réquisitions légales qui leur sont adressées.

Afin d'assurer le respect de ces nouvelles dispositions, le texte propose enfin de confier au Premier ministre, au titre de ses attributions spécifiques en matière de défense et de sécurité nationale et au terme d'une procédure contradictoire, la possibilité de sanctionner les personnes morales défailtantes. De nature progressive, ces sanctions peuvent aller jusqu'à l'obligation pour la personne morale défailtante de suspendre immédiatement son activité sur le territoire national. Cette décision serait, en tout état de cause, susceptible de recours devant le juge administratif.

La mise à jour du cadre légal est le préalable nécessaire pour instaurer un dialogue équilibré avec les opérateurs de messageries chiffrées. Les dispositions actuelles, par leur obsolescence et leur inconventionnalité, ne le permettent pas.

En tout état de cause, aucune autre dispositif légal ou technique ne permettrait de pallier l'absence de coopération des plateformes de messagerie chiffrée, dont l'utilisation tend à remplacer les communications téléphoniques classiques.

Cet état de fait représente d'ores et déjà un obstacle majeur pour la protection des intérêts fondamentaux de la Nation par les services de renseignement. En matière terroriste, plusieurs attaques mortelles récentes auraient pu être évitées si les plateformes avaient coopéré avec les services de renseignement. Dans le domaine du narcotrafic, les organisations concernées recourent désormais principalement aux solutions privées « grand public » pour la coordination de leurs activités clandestines. Les solutions ad hoc dédiées au crime organisé sont quant à elles de moins en moins investies.