Chiffrement : l'Assemblée troque une loi contre une promesse

Le 10 novembre 2026, soixante-neuf députés suppriment du projet de loi Résilience l'article 16 bis, seule disposition qui interdisait d'imposer aux fournisseurs de chiffrement des dispositifs affaiblissant volontairement leur sécurité. En contrepartie, le Gouvernement s'engage à ne pas réintroduire de portes dérobées jusqu'à la fin de la session parlementaire, le ministre de l'Intérieur allant jusqu'à parler d'une proscription définitive. Lue avec Douglass North et Barry Weingast, l'opération remplace un engagement crédible (une règle que l'exécutif ne peut pas défaire seul) par un engagement révocable, daté, dont l'auteur a toutes les chances de disparaître avant l'échéance.

Par Alexandre Berge · 13 novembre 2026 · 19 min de lecture · Chronique

Une interdiction inscrite dans la loi, retirée contre une parole datée

L'article 16 bis n'appartenait pas au projet initial. Le Sénat l'a ajouté le 12 mars 2025, en adoptant un amendement d'Olivier Cadic et de plusieurs de ses collègues, contre l'avis défavorable de sa commission comme du Gouvernement. Le texte adopté interdit d'imposer aux fournisseurs de services de chiffrement, prestataires de services de confiance qualifiés compris, l'intégration de « dispositifs techniques visant à affaiblir volontairement la sécurité » des systèmes d'information et des communications électroniques, qu'il s'agisse de clés de déchiffrement maîtresses ou de tout autre mécanisme d'accès non consenti aux données protégées.

La disposition répondait à un épisode précis. Entendu par la commission spéciale de l'Assemblée le 15 juillet 2025, le directeur général de l'ANSSI, Vincent Strubel, rappelait qu'elle « visait à répondre à l'article 8 ter de la proposition de loi « narcotrafic » », lequel avait été supprimé au cours de la navette. Le 16 bis fonctionnait donc comme un verrou posé après une tentative avortée, afin d'interdire par la loi ce que le véhicule législatif suivant aurait pu réintroduire.

Les services ont combattu ce verrou dès les premières auditions. Le 9 juillet 2025, devant la même commission, la directrice générale de la sécurité intérieure exposait que le chiffrement rend les interceptions classiques obsolètes, et le représentant du groupement interministériel de contrôle, Pascal Chauve, estimait que « ce texte érige, en fait, le chiffrement en totem ». La

commission spéciale a pourtant conservé l'article en septembre 2025, en adoptant un amendement de son président, Philippe Latombe, et en rejetant une réécriture du rapporteur général Éric Bothorel, datée du 8 septembre, qui aurait seulement proclamé la protection des systèmes d'information par le chiffrement « d'intérêt général majeur », assortie d'une évaluation des enjeux de l'accès aux contenus chiffrés.

Le Gouvernement a déposé le 3 octobre 2026 son amendement n° 358, qui supprime l'article. L'exposé sommaire avance quatre motifs : un risque pour la sécurité nationale, une atteinte aux techniques d'enquête et de renseignement (interceptions, géolocalisation, recueil des données de connexion), un périmètre étendu à tout fournisseur de chiffrement et non aux seules messageries, enfin la qualification de l'article en « cavalier dépourvu de lien direct ou indirect avec le projet de loi ». Dans l'hémicycle, le 10 novembre, le ministre de l'Intérieur Laurent Nuñez a résumé la position en jugeant la rédaction bien trop large et sujette à interprétation.

Ces critiques de rédaction sont sérieuses, et cette chronique ne les conteste pas. La question qu'elle pose est ailleurs : ce que l'Assemblée a mis à la place. La veille du vote, la ministre déléguée chargée de l'intelligence artificielle et du numérique, Anne Le Hénanff, annonçait que le Gouvernement « s'engagera à ne pas réintroduire ni soutenir une réintroduction » d'un mécanisme de portes dérobées, selon le Journal du Net. Next, reprenant Le Monde, précise le terme de cet engagement : « jusqu'à la fin de la session parlementaire ». C'est ainsi que l'hémicycle a compris l'accord. Dès la discussion générale du 9 novembre, la députée écologiste Sabrina Sebaihi relevait qu'« une liberté garantie jusqu'au 30 juin n'est pas une liberté : c'est un sursis ». Le lendemain, Emeric Salmon (Rassemblement national) puis Philippe Latombe ont rappelé que l'engagement valait jusqu'à la fin de la session parlementaire.

Le ministre de l'Intérieur a donné une autre portée à la parole gouvernementale. Selon le compte rendu de la séance du 10 novembre, il a rappelé l'engagement de ne pas reprendre l'article 8 ter et de ne soutenir aucun amendement créant un dispositif similaire, affirmé que les portes dérobées sont « définitivement proscrites » et réitéré l'engagement du Gouvernement de ne pas y revenir. L'article a été supprimé dans la même séance, après une quarantaine de minutes de débat selon Next. Le vote solennel sur l'ensemble du texte est fixé au 17 novembre. **Le même jour, un ministre déclare donc définitivement proscrites des portes dérobées dont la seule interdiction écrite vient d'être retirée.**

> **Un scrutin à 107 votants**
>
> Le scrutin public n° 9794 du 10 novembre 2026 porte sur l'amendement n° 358 du Gouvernement et les amendements identiques de suppression (n° 5, 200, 300 et 397). Il réunit 107 votants pour 577 sièges, 106 suffrages exprimés, 69 voix pour la suppression, 37 contre et 1 abstention. La suppression est portée par le Rassemblement national (17 voix), Ensemble pour la République (17), Les Démocrates (9), la Droite républicaine (8), Horizons

> et Indépendants (8), le groupe Socialistes et apparentés (5), le groupe LIOT (3) et deux non-inscrits. Les 37 voix contraires viennent de La France insoumise (26), du groupe Écologiste et social (10) et d'un député Ensemble pour la République. Une règle adoptée par le Sénat et conservée par la commission spéciale a donc été retirée par un scrutin réunissant moins d'un cinquième des députés.

Un engagement n'est crédible que s'il coûte à rompre

Le cas oppose deux objets que le débat public a traités comme équivalents : une interdiction législative et une promesse ministérielle portant sur le même contenu. La littérature d'économie institutionnelle a précisément construit un outil pour les distinguer.

Dans « Constitutions and Commitment », publié en 1989 dans le *Journal of Economic History*, Douglass North et Barry Weingast étudient l'Angleterre du XVIIe siècle. Sous les Stuarts, la Couronne emprunte sous la contrainte et rembourse quand elle le veut. L'emprunt de 100 000 livres levé en 1617, censé être remboursé au bout d'un an, voit son principal honoré seulement en 1628. En 1672, le « Stop of the Exchequer » répudie partiellement une dette de plus d'un million de livres. Après la Glorieuse Révolution de 1688, le pouvoir n'appartient plus au roi seul mais au roi en son Parlement, les juges ne sont plus révocables au gré de la Couronne, le Parlement contrôle et vote la dépense, et la menace de destitution, deux fois mise à exécution dans le siècle, devient crédible. La dette publique passe d'environ un million de livres en 1688 à près de dix-sept millions en 1697, et les taux auxquels l'État emprunte baissent durablement au cours des décennies suivantes.

La thèse tient en une distinction. Un souverain peut rendre ses engagements crédibles de deux manières, soit en se constituant une réputation de comportement responsable, soit en se soumettant à des règles qui lui interdisent de s'en affranchir, « a set of rules that do not permit leeway » (un ensemble de règles qui ne laissent aucune latitude). Les auteurs notent avoir très rarement observé la première voie, parce que la pression des nécessités finit par pousser les gouvernants à rompre leurs engagements. Une règle que le souverain peut réviser seul ne produit pas les mêmes effets que la même règle soustraite à sa révision, même si son contenu est identique.

> **L'engagement crédible (North et Weingast, 1989)**
>
> Pour Douglass North et Barry Weingast, un gouvernant n'obtient la confiance de ceux dont il dépend (prêteurs, investisseurs, opérateurs) que si sa promesse de respecter une règle est crédible, c'est-à-dire si la rompre lui coûte davantage qu'elle ne lui rapporte. La réputation fournit une garantie fragile, car elle cède dès que la pression devient forte. La garantie robuste vient des institutions qui retirent au gouvernant la faculté de modifier seul la règle : veto d'une assemblée, juge indépendant, procédure publique. Le critère n'est pas la sincérité de celui qui promet, mais le prix de la défection.

Appliquée au 16 bis, la grille est sans ambiguïté. L'article relevait de la seconde voie. Pour lever l'interdiction, un gouvernement devait obtenir le vote des deux assemblées, en séance publique, sous le regard d'une opposition et, le cas échéant, sous le contrôle du Conseil constitutionnel. Le coût de la défection était la procédure législative elle-même, celle que l'Assemblée vient d'emprunter dans l'autre sens. La promesse ministérielle relève de la première voie. Elle n'est opposable devant aucun juge, ne prévoit aucune sanction, ne désigne aucune instance chargée d'en constater la violation. Son seul gage est la réputation de ceux qui l'ont prononcée. L'adverbe « définitivement » employé par le ministre de l'Intérieur ne modifie pas ce diagnostic. Il prête à la parole la durée de la règle sans lui en donner la force : une proscription déclarée définitive à la tribune reste révocable par la tribune suivante.

Ce qui manque à l'analyse publique du vote, c'est l'identification de ceux pour qui la crédibilité importe. Dans le schéma de North et Weingast, ce sont les détenteurs de capitaux. Ici, ce sont les fournisseurs de services de chiffrement et les prestataires de confiance qualifiés que l'article visait nommément, dont les choix d'architecture, de qualification et d'implantation se décident sur des horizons de plusieurs années. Une interdiction législative leur offrait un environnement stable. Un engagement de quelques mois ne leur offre qu'un sursis. La chronique du 7 novembre consacrée à l'achat public mobilisait l'autocontrainte de Jon Elster, par laquelle un acteur se lie lui-même. Le 16 bis relevait d'un autre registre : ce n'est pas l'exécutif qui s'était lié, c'est le Parlement qui l'avait lié, et c'est précisément ce qui rendait la règle crédible.

La promesse expire en juin 2027, son auteur sans doute avant elle

La durée annoncée par la ministre déléguée, et rappelée en séance par les députés qui ont porté l'accord, mérite d'être prise au mot. L'article 28 de la Constitution dispose que la session ordinaire commence le premier jour ouvrable d'octobre et prend fin le dernier jour ouvrable de juin. Pour la session ouverte en octobre 2026, l'échéance tombe le mercredi 30 juin 2027. L'engagement couvre donc un peu moins de huit mois à compter du vote.

Or ce calendrier en croise un autre. Le Conseil des ministres du 1er juillet 2026 a fixé l'élection présidentielle au 18 avril et au 2 mai 2027. Selon un usage constant de la Ve République, le Gouvernement en fonction remet sa démission au président nouvellement élu. Un gouvernement formé en mai 2027 ne sera tenu par aucune parole de son prédécesseur, puisque aucune procédure ne transmet une promesse ministérielle d'une équipe à l'autre. Sauf continuité politique, l'auteur de l'engagement aura donc cessé d'exister quelques semaines avant son terme. La version sans échéance du ministre de l'Intérieur n'échappe pas à cette limite : un engagement dit définitif, pris par un ministre, n'oblige pas davantage son successeur.

Il en résulte une asymétrie. La période effectivement couverte par la promesse correspond pour l'essentiel aux mois qui précèdent une élection présidentielle, pendant lesquels l'exécutif

n'aurait guère eu les moyens de faire adopter un texte aussi disputé qu'un accès légal aux contenus chiffrés. L'engagement porte sur le moment où il ne coûte rien. La rédaction laisse en outre ouverte la question des sessions extraordinaires que l'article 29 de la Constitution permet de convoquer en juillet, et dont rien n'indique qu'elles soient couvertes.

Au regard de la grille de North et Weingast, une promesse dont le terme coïncide avec l'horizon électoral de celui qui la fait constitue la forme la plus pure de l'engagement réputationnel. La réputation n'oblige qu'aussi longtemps que celui qui la porte a intérêt à la conserver. **Une interdiction permanente devient ainsi un engagement politique dont la durée de vie est inférieure à celle du gouvernement qui l'a contracté.**

Le canal européen reste hors du champ de la promesse

L'angle mort le plus net ne tient pas à la durée de l'engagement, mais à son périmètre. Tels que les consigne le compte rendu du 10 novembre, les termes de l'engagement portent sur la reprise de l'article 8 ter et sur le soutien à un amendement créant un dispositif similaire, autrement dit sur la seule procédure législative nationale. Ils ne disent rien de la position que la France défend au Conseil de l'Union européenne.

C'est pourtant là que se trouve le dossier. Le 4 mai 2026, la délégation parlementaire au renseignement, présidée par la sénatrice Muriel Jourda, a publié une communication jugeant un accès ciblé des services de renseignement et de la justice aux contenus chiffrés à la fois légitime et nécessaire, et qu'elle ne tient pas pour techniquement exclu. La délégation y estime que « l'échelle européenne paraît la plus adaptée » pour obtenir l'intégration d'outils permettant cet accès, invite le Gouvernement à poursuivre les démarches engagées avec ses partenaires, qualifie la rédaction du 16 bis de risque majeur pour la politique publique du renseignement et annonce son rapport annuel pour le début de l'année 2027.

Du côté de Bruxelles, la Commission a présenté le 24 juin 2025 une feuille de route sur l'accès légal et effectif aux données par les autorités répressives. Elle y annonce pour 2026 une feuille de route technologique sur le chiffrement, destinée à identifier et évaluer les solutions permettant cet accès, et le soutien à des capacités de déchiffrement de nouvelle génération pour Europol à partir de 2030. Un document de la présidence du Conseil daté du 23 janvier 2026 précise que le groupe d'experts informel chargé de ce travail, composé de quinze membres, s'est réuni pour la première fois en décembre 2025, que ses résultats sont attendus au quatrième trimestre 2026, et que la nouvelle plateforme d'Europol n'est pas attendue avant 2030.

La séquence se lit alors autrement. Les services ont déplacé leur demande vers l'échelon européen, la délégation parlementaire a validé ce déplacement, et la promesse gouvernementale a été dessinée autour du seul échelon qu'ils ont quitté. Le 16 bis n'aurait pas lié le droit de l'Union, qui prime sur la loi nationale. Mais il fixait dans la loi une position française qu'un gouvernement défendant l'inverse à Bruxelles aurait dû contredire

publiquement. Une règle crée un coût d'incohérence. Une promesse limitée à la procédure nationale n'en crée aucun.

Ni l'exposé sommaire de l'amendement n° 358, ni le compte rendu de la discussion de l'article 16 bis, où l'Union européenne n'apparaît qu'à propos de la transposition des directives, ni les quatre articles de presse consultés le 13 novembre 2026 ne mentionnent ce calendrier européen. Le discours institutionnel a présenté la suppression comme un renoncement aux portes dérobées. Il s'agit plus exactement d'un renoncement à les introduire par la seule voie où un verrou existait.

En 1999, l'État avait fait le chemin inverse, de l'annonce à la loi

Le droit français du chiffrement offre un précédent d'une proximité structurelle rare, parce qu'il porte sur le même objet, oppose les mêmes logiques de sécurité des systèmes et de capacité d'interception, et décrit une conversion entre promesse et règle. Simplement, elle allait dans l'autre sens.

Jusqu'à la fin des années 1990, la cryptologie relève en France d'un régime restrictif. La loi n° 96-659 du 26 juillet 1996 de réglementation des télécommunications assouplit l'autorisation à condition que les clés soient confiées à des tiers de confiance agréés, dispositif mis en œuvre par les décrets du 24 février 1998. Le 19 janvier 1999, à l'issue du comité interministériel pour la société de l'information, le Premier ministre Lionel Jospin annonce la libéralisation de l'usage de la cryptologie. Les décrets n° 99-199 et n° 99-200 du 17 mars 1999 relèvent de 40 à 128 bits le seuil des moyens dont l'utilisation est libre. Le Gouvernement ne tient pas ces décrets pour un aboutissement. Répondant en octobre 1999 au sénateur Jean-Pierre Raffarin, il présente ce relèvement comme une mesure prise « dans l'attente des dispositions législatives correspondantes ».

Ces dispositions viennent avec la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique, qui abroge le régime des tiers de confiance. Le I de son article 30 dispose : « L'utilisation des moyens de cryptologie est libre. » La phrase est toujours en vigueur. Il aura fallu plus de cinq ans pour convertir une annonce gouvernementale en règle de droit, et l'exécutif de l'époque considérait lui-même que sa décision restait incomplète tant qu'elle n'avait pas pris cette forme. La logique est celle de North et Weingast : pour être crue par les acteurs du marché, la libéralisation devait échapper à la révision par simple décret.

Le cas de 2026 inverse la trajectoire, à une vitesse sans commune mesure. Ce qui avait demandé cinq ans pour passer de l'annonce à la loi repasse de la loi à l'annonce en une séance. L'article 8 ter de la proposition de loi sur le narcotrafic, inséré puis supprimé en 2025, montre par ailleurs que la question de l'accès aux contenus chiffrés revient dans le premier véhicule législatif disponible dès que le verrou disparaît. La liberté d'utilisation posée en 2004 protège l'usager, pas le fournisseur contre une obligation de conception, et c'est précisément ce vide que le 16 bis comblait.

Une interdiction devenue sursis

Le titre de cette chronique oppose une loi et une promesse. La grille de North et Weingast permet de dire en quoi elles diffèrent, alors même que leur contenu se recouvre : la première faisait payer la défection au prix d'une procédure publique devant deux assemblées, la seconde ne la fait payer qu'au prix d'une réputation dont la valeur décroît à mesure que s'approche l'élection de 2027. Le mot de sursis, employé dès le 9 novembre dans l'hémicycle, en donne la mesure. La tension posée en ouverture, entre un Gouvernement qui renonce aux portes dérobées et la suppression de la seule règle qui les interdisait, se résout ainsi : le renoncement est réel, mais il a changé de nature, d'un *engagement crédible* vers un engagement révocable.

Cette lecture conduit à une hypothèse vérifiable. Si l'engagement gouvernemental n'est que réputationnel, la question d'un accès aux contenus chiffrés reviendra avant le 30 juin 2028 par l'un des canaux qu'il ne couvre pas, le droit de l'Union ou l'initiative d'un gouvernement issu de l'élection de 2027.

Quatre indicateurs permettront à tout lecteur de trancher sans information interne. Le premier est le texte issu de la commission mixte paritaire qui devrait suivre le vote solennel du 17 novembre 2026, selon que l'article 16 bis y sera absent, rétabli ou réécrit, par exemple dans les termes d'intérêt général que proposait la réécriture de septembre 2025. Le deuxième est le rapport annuel de la délégation parlementaire au renseignement attendu au début de 2027, selon qu'il recommande ou non une initiative législative. Le troisième est la publication de la feuille de route technologique de la Commission sur le chiffrement, attendue d'ici la fin de 2026, et la position que la France y prendra au Conseil. Le quatrième est le dépôt, à l'Assemblée nationale ou au Sénat, entre le 1er juillet 2027 et le 30 juin 2028, d'un projet ou d'une proposition de loi organisant un accès aux contenus chiffrés.

Si aucun de ces canaux ne s'est ouvert au 30 juin 2028, l'hypothèse sera infirmée, et la réputation aura tenu là où North et Weingast la jugeaient fragile. Dans le cas contraire, le vote du 10 novembre 2026 se lira comme le moment où le Parlement a cédé la seule garantie qui ne dépendait pas de la bonne volonté de celui qu'elle encadrait.

Note méthodologique

L'article s'appuie principalement sur le scrutin n° 9794, les comptes rendus des séances des 9 et 10 novembre 2026, l'amendement n° 358, le texte adopté par le Sénat le 12 mars 2025, les comptes rendus de la commission spéciale, la communication de la délégation parlementaire au renseignement et les documents européens cités. Sur la durée de l'engagement, le Journal du Net, Next (citant Le Monde) et LCP rapportent la formule de la ministre déléguée, « la fin de la session parlementaire », que reprennent en séance Emeric Salmon et Philippe Latombe. INCYBER évoque, dans ses propres termes, la « fin de l'actuelle mandature », et le ministre de

l'Intérieur, selon le compte rendu, ne fixe aucun terme. L'auteur retient la formule datée, attribuée au Gouvernement par plusieurs sources concordantes, dont il déduit l'échéance du 30 juin 2027 (article 28 de la Constitution), et discute la version sans terme dans le texte. L'absence de mention du calendrier européen est constatée dans l'exposé sommaire de l'amendement n° 358, dans le compte rendu de la discussion de l'article 16 bis et dans les quatre articles de presse cités, consultés le 13 novembre 2026. La lecture selon laquelle l'auteur de la promesse disparaîtra avant son terme, fondée sur l'usage de la démission du Gouvernement après l'élection présidentielle, est un choix d'interprétation de l'auteur.

Recherche de sources, croisement des données et structuration du raisonnement s'appuient sur une assistance par intelligence artificielle. Le choix de l'angle et du cadre théorique, la vérification des sources, les arbitrages et l'établissement du texte final relèvent de l'auteur.

Sources

Sources primaires parlementaires et gouvernementales

Assemblée nationale, « Scrutin public n° 9794 sur l'amendement n° 358 du Gouvernement et les amendements identiques de suppression de l'article 16 bis du projet de loi relatif à la résilience des infrastructures critiques et au renforcement de la cybersécurité (première lecture) », 10 novembre 2026. https://www.assemblee-nationale.fr/dyn/17/scrutins/9794

Assemblée nationale, compte rendu intégral de la première séance du lundi 9 novembre 2026. https://www.assemblee-nationale.fr/dyn/17/comptes-rendus/seance/session-ordinaire-de-2026-2027/premiere-seance-du-lundi-09-novembre-2026

Assemblée nationale, compte rendu intégral de la première séance du mardi 10 novembre 2026. https://www.assemblee-nationale.fr/dyn/17/comptes-rendus/seance/session-ordinaire-de-2026-2027/premiere-seance-du-mardi-10-novembre-2026

Gouvernement, amendement n° 358 à l'article 16 bis, projet de loi relatif à la résilience des infrastructures critiques et au renforcement de la cybersécurité (n° 1779), 3 octobre 2026. https://www.assemblee-nationale.fr/dyn/17/amendements/1779/AN/358.pdf

Sénat, Projet de loi relatif à la résilience des infrastructures critiques et au renforcement de la cybersécurité, texte adopté n° 78 (2024-2025), 12 mars 2025. https://www.senat.fr/leg/tas24-078.html

Sénat, amendement n° 1 rect. quinquies présenté par MM. Cadic et Canévet, Mme Morin-Desailly et plusieurs de leurs collègues, 12 mars 2025. https://www.senat.fr/amendements/2024-2025/394/Amdt_1.html

Assemblée nationale, commission spéciale chargée d'examiner le projet de loi relatif à la résilience des infrastructures critiques et au renforcement de la cybersécurité, compte rendu n° 13, 9 juillet 2025. https://www.assemblee-nationale.fr/dyn/17/comptes-rendus/cscyber/

l17cscyber2425013_compte-rendu.pdf

Assemblée nationale, même commission, compte rendu n° 15 (audition de Vincent Strubel, directeur général de l'ANSSI), 15 juillet 2025. https://www.assemblee-nationale.fr/dyn/17/comptes-rendus/cscyber/l17cscyber2425015_compte-rendu.pdf

Assemblée nationale, amendement n° CS358 présenté par M. Latombe, 5 septembre 2025. https://www.assemblee-nationale.fr/dyn/17/amendements/1112/CSCYBER/358.pdf

Assemblée nationale, amendement n° CS494 présenté par M. Bothorel, rapporteur général, 8 septembre 2025. https://www.assemblee-nationale.fr/dyn/17/amendements/1112/CSCYBER/494.pdf

Délégation parlementaire au renseignement, Communication sur les messageries chiffrées et la technique algorithmique, 4 mai 2026. https://www.senat.fr/fileadmin/Office_et_delegations/Renseignement/Communication_DPR_mai2026.pdf

Assemblée nationale, « Fiche de synthèse n° 39 : Sessions et séances », page consultée le 13 novembre 2026. https://www.assemblee-nationale.fr/dyn/contenu/telechargement/629092/file/Fiche%2039%20-%20Sessions%20et%20s%C3%A9ances.pdf

Service-public.gouv.fr (DILA), « Les dates de l'élection présidentielle de 2027 sont annoncées », 2 juillet 2026. https://www.service-public.gouv.fr/particuliers/actualites/A15053

Sources européennes

Commission européenne, DG Migration et affaires intérieures, « Commission presents Roadmap for effective and lawful access to data for law enforcement », 24 juin 2025. https://home-affairs.ec.europa.eu/news/commission-presents-roadmap-effective-and-lawful-access-data-law-enforcement-2025-06-24_en

Conseil de l'Union européenne, Présidence, « Access to data for effective law enforcement: Overview of activities during the Cyprus Presidency », document 5424/26, 23 janvier 2026. https://data.consilium.europa.eu/doc/document/ST-5424-2026-INIT/en/pdf

Parallèle historique

Loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique, article 30, Légifrance, version consultée le 13 novembre 2026. https://www.legifrance.gouv.fr/loda/id/JORFTEXT000000801164

Sénat, question écrite n° 17791 de M. Jean-Pierre Raffarin, publiée au JO Sénat du 8 juillet 1999, réponse publiée au JO Sénat du 21 octobre 1999. https://www.senat.fr/questions/base/1999/qSEQ990717791.html

ANSSI, « Crypto, le webdoc. Chapitre III : Sécurité, secret et légalité », page consultée le 13 novembre 2026. https://cyber.gouv.fr/crypto-le-webdoc/chapitre-iii-sécurité-secret-et-

légalité/

Cadre théorique

Douglass C. North et Barry R. Weingast, « Constitutions and Commitment: The Evolution of Institutions Governing Public Choice in Seventeenth-Century England », *The Journal of Economic History*, vol. 49, n° 4, décembre 1989, p. 803-832. https://doi.org/10.1017/S0022050700009451

Chronique ElegArtech citée

« SI public : la seule rigueur que l'État ne choisit pas », 7 novembre 2026. https://elegartech.fr/articles/si-public-la-seule-rigueur-que-l-etat-ne-choisit-pas

Presse spécialisée

Alexandre Mathiot, « Loi résilience : le gouvernement renonce aux portes dérobées dans les messageries chiffrées », Journal du Net, 9 novembre 2026. https://www.journaldunet.com/business/action-publique/1557749-le-gouvernement-renonce-aux-portes-derobees-dans-les-messageries-chiffrees/

Next, « « Ouf ! Enfin ! » : NIS2 arrive à l'Assemblée, le chiffrement déjà au cœur des débats », 9 novembre 2026, mis à jour le 10 novembre 2026. https://next.ink/266473/ouf-enfin-nis2-arrive-a-lassemblee-le-chiffrement-deja-au-coeur-des-debats/

Raphaël Marchal, « Loi sur la cybersécurité : la mesure décriée sur les messageries chiffrées supprimée par les députés », LCP, 10 novembre 2026. https://lcp.fr/actualites/loi-sur-la-cybersecurite-la-mesure-decriee-sur-les-messageries-chiffrees-supprimee-par

La Rédaction d'INCYBER News, « Loi Résilience : suppression de l'article 16 bis controversé », INCYBER, 11 novembre 2026. https://incyber.org/article/loi-resilience-suppression-article-16-bis-controverse/