	Projet de loi		
	Résilience des infrastructures critiques et renforcement de la cybersécurité (PROCÉDURE ACCÉLÉRÉE)	N°	1 rect. quinquies
Direction de la Séance	(n°S 394, 393)	**12 mars 2025**	

a m e n d e m e n t

présenté par

MM. CADIC et CANÉVET, Mme MORIN-DESAILLY, MM. HAYE et Loïc HERVÉ, Mmes LOISIER, HOUSSEAU, FLORENNES, SOLLOGOUB, JACQUEMET, de LA PROVÔTÉ, SAINT-PÉ, PATRU, EVREN, PERROT et BILLON, M. KERN, Mme GACQUERRE, M. MILON, Mme JOSEPH, MM. MELLOULI et MICHALLET, Mme BRIANTE GUILLEMONT et MM. CHASSEING et DOSSUS

Article additionnel après l'article 16

Après l'article 16

Insérer un article additionnel ainsi rédigé :

Il ne peut être imposé aux fournisseurs de services de chiffrement, y compris aux prestataires de services de confiance qualifiés, l'intégration de dispositifs techniques visant à affaiblir volontairement la sécurité des systèmes d'information et des communications électroniques tels que des clés de déchiffrement maîtresses, ou tout autre mécanisme permettant un accès non consenti aux données protégées.

Objet

La sécurité des systèmes d'information est un enjeu stratégique pour la protection des données personnelles, la confidentialité des communications, le secret des affaires, la protection des Droits et Libertés fondamentales et la souveraineté numérique. Le chiffrement joue un rôle central dans cet écosystème en garantissant l'intégrité et la confidentialité des échanges numériques, qu'il s'agisse de transactions financières, de communications privées ou de données sensibles des entreprises et administrations.

Or, certaines initiatives législatives et réglementaires, tant au niveau national qu'international, ont cherché à imposer aux fournisseurs de services de chiffrement des obligations visant à insérer des dispositifs techniques permettant un accès aux données protégées par des tiers, notamment par les autorités publiques. Ces dispositifs, communément appelés « portes dérobées » (backdoors), « clés de déchiffrement maîtresses » ou autres mécanismes d'affaiblissement volontaire de la sécurité, présentent des risques considérables pour la sécurité informatique et la protection des droits fondamentaux.

D'une part, ces dispositifs créent des vulnérabilités exploitables non seulement par les autorités prévues, mais également par des acteurs malveillants, qu'il s'agisse de cybercriminels, d'États hostiles ou d'entités privées cherchant à compromettre la sécurité des systèmes d'information. Il est démontré que toute faiblesse introduite dans un système de chiffrement réduit sa fiabilité de manière globale et incontrôlable. Ainsi, l'obligation d'intégrer de telles failles irait à l'encontre des principes

de sécurité informatique et de cybersécurité reconnus au niveau international et imposé par la Directive NIS2.

D'autre part, l'introduction de ces obligations remettrait en cause des droits fondamentaux tels que le droit à la vie privée et à la protection des données personnelles, garantis par des textes fondamentaux comme le Règlement général sur la protection des données (RGPD) ou l'article 8 de la Convention européenne des droits de l'homme. L'accès non consenti aux communications et aux données privées, sans garanties suffisantes, constituerait une atteinte disproportionnée à ces droits.

Enfin, sur le plan économique et stratégique, fragiliser la sécurité des solutions de chiffrement françaises et européennes nuirait à leur compétitivité face aux acteurs internationaux qui, eux, ne seraient pas nécessairement soumis aux mêmes contraintes. Cela risquerait d'entraîner un déplacement des utilisateurs et entreprises vers des solutions étrangères considérées comme plus sûres, affaiblissant ainsi notre souveraineté numérique.

Cet amendement vise donc à inscrire dans la loi un principe clair de sécurité numérique