

Portes dérobées dans les messageries chiffrées : l'AFCDP alerte sur les risques.**La proposition incluse dans le projet de loi de lutte contre le narcotrafic présente des risques et mérite un examen approfondi**

L'AFCDP, qui représente les Délégués à la Protection des Données (DPD/DPO), exprime sa vive préoccupation concernant la « *Proposition de loi visant à sortir la France du piège du narcotrafic* » adoptée par le Sénat et en cours de discussion à l'Assemblée nationale¹, en raison de ses dispositions visant à imposer aux opérateurs de communications électroniques, notamment aux messageries chiffrées, la mise en place d'accès pour les services de police.

Une menace pour la protection des données personnelles

En tant que garants de la conformité au Règlement Général sur la Protection des Données (RGPD) et à la Loi Informatique et Libertés, les DPD/DPO de l'AFCDP alertent sur les contradictions majeures entre cette proposition et les obligations légales de sécurisation des données qui incombent à tous les responsables de traitement.

Cette mesure, bien que placée sous le contrôle de la Commission nationale de contrôle des techniques de renseignement, comporte de facto la mise en œuvre de « portes dérobées » dans des systèmes conçus pour garantir la confidentialité des échanges.

L'AFCDP rejoint en cela les inquiétudes exprimées par Guillaume Poupard, ancien directeur général de l'ANSSI, qui a qualifié cette approche de « dangereuse » malgré son apparente séduction.

Une disposition contraire aux recommandations des autorités européennes et nationales

La position de l'AFCDP s'inscrit dans la droite ligne des analyses des autorités compétentes en matière de protection des données et de cybersécurité. Ainsi l'ANSSI avait, dès 2016, produit une analyse toujours d'actualité soulignant l'importance cruciale de la généralisation du chiffrement face à la banalisation des attaques informatiques.

De son côté, la CNIL rappelle la position commune du Comité Européen de la Protection des Données (CEPD/EDPB) et du Contrôleur Européen de la Protection des Données (CEPD/EDPS) de juillet 2022 qui, dans le cadre de la lutte contre les abus sexuels sur les enfants, estimaient qu'« *il devrait y avoir un meilleur équilibre entre la nécessité sociétale de disposer de canaux de communication sûrs et privés et de lutter contre leurs abus. Il convient d'indiquer clairement dans la proposition qu'aucune disposition du règlement proposé ne devrait être interprétée comme interdisant ou affaiblissant le chiffrement.* »

¹ https://www.assemblee-nationale.fr/dyn/17/dossiers/_DLR5L17N50169

Cette expertise technique et juridique semble aujourd'hui ignorée au profit d'une solution qui, sous couvert de sécurité publique, risque paradoxalement d'affaiblir la sécurité globale des systèmes d'information et la protection des données personnelles.

Des conséquences graves pour la sécurité numérique

Cette proposition législative présente plusieurs risques majeurs.

Elle constitue une **Violation potentielle du RGPD**, puisque son article 32 impose la mise en œuvre de « mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque ». L'affaiblissement délibéré du chiffrement va directement à l'encontre de cette obligation.

Elle s'oppose à la **jurisprudence européenne**, la Cour de Justice de l'Union Européenne ayant rappelé à plusieurs reprises l'importance d'une protection robuste des communications électroniques.

Elle présente des **risques pour les données dont le traitement nécessite un haut niveau de sécurité**, dans la mesure où des secteurs entiers (santé, finance, industrie) reposent sur des communications sécurisées pour protéger des données critiques.

Elle constitue enfin **un précédent dangereux**, risquant d'ouvrir la voie à d'autres exceptions au principe de confidentialité des communications, fragilisant l'ensemble de l'écosystème numérique.

L'AFCDP souhaite une inflexion de la proposition de loi

L'AFCDP considère que la lutte contre la criminalité organisée, bien que légitime, ne peut justifier une mesure qui compromet structurellement la sécurité des systèmes d'information, crée un précédent dangereux d'affaiblissement des protections techniques, place les entreprises et organismes dans une situation d'insécurité juridique face à leurs obligations légales de protection des données, ignore les recommandations techniques formulées par l'autorité nationale en matière de cybersécurité et va à l'encontre des positions adoptées par les autorités européennes de protection des données.

L'AFCDP appelle le législateur à :

- engager une concertation approfondie avec les experts en cybersécurité et en protection des données ;
- prendre en compte l'analyse technique de l'ANSSI de 2016 sur l'importance du chiffrement ;
- respecter la position commune du CEPD/EDPB et du CEPD/EDPS sur la préservation du chiffrement ;
- explorer des solutions alternatives qui ne compromettraient pas l'intégrité des systèmes de protection ;
- concilier les impératifs de sécurité publique avec les obligations légales de protection des données personnelles.

À propos de l'AFCDP - www.afcdp.net

L'AFCDP, créée dès 2004, regroupe plus de 6 000 professionnels de la conformité au RGPD et à la Loi Informatique & Libertés – dont les Délégués à la Protection des Données (DPD ou DPO, pour *Data Protection Officer*).

Si l'AFCDP est l'association représentative des DPD, elle rassemble largement. Au-delà des professionnels de la protection des données et des DPD désignés auprès de la CNIL, elle regroupe toutes les personnes intéressées par la protection des données à caractère personnel. La richesse de l'association réside – entre autres – dans la diversité des profils des adhérents : DPD, délégués à la protection des données, juristes et avocats, spécialistes des ressources humaines, informaticiens, professionnels du marketing et du e-commerce, RSSI et experts en sécurité, qualitiens, archivistes et Record Manager, déontologues, consultants, universitaires et étudiants.

Contact Presse : Maëlle Garrido, NASKAS RP, Relations Presse, 06 12 70 77 30, maelle@naskas-rp.com