MINISTÈRE
DE LA JUSTICE
Liberté
Égalité
Fraternité

Direction des affaires criminelles et des grâces

Paris, le 13 avril 2026

Le garde des Sceaux, ministre de la Justice

A

Pour attribution

Mesdames et Messieurs les procureurs généraux près les cours d'appel
Monsieur le procureur de la République près le tribunal supérieur d'appel
Mesdames et Messieurs les procureurs de la République près les tribunaux judiciaires

Pour information

Mesdames et Messieurs les premiers présidents des cours d'appel
Monsieur le président du tribunal supérieur d'appel
Mesdames et Messieurs les présidents des tribunaux judiciaires

N° NOR : NOR n°JUSD2605231C

N° CIRCULAIRE : 2026-5/CAB-20/02/2026

N/REF : DP 2026/0013/H34

TITRE : Circulaire relative à l'accès aux données détenues par les fournisseurs de services ou de messageries électroniques.

Dans un contexte de démocratisation des outils numériques et de développement des solutions de chiffrement commercialisées au grand public, l'accès à la preuve numérique constitue un enjeu majeur pour l'efficacité des procédures pénales, alors que 85% des enquêtes font désormais intervenir des données numériques[1].

Cet enjeu est d'autant plus prioritaire que les organisations criminelles ont adopté des modes opératoires toujours plus élaborés et se sont emparées de ces nouveaux moyens de communication pour dissimuler leurs échanges et organiser leurs actions criminelles.
Dans le prolongement de la circulaire du 5 mars 2025 de renforcement de la coordination judiciaire en matière de lutte contre la criminalité organisée, et de celle du 27 décembre 2025 relative à la lutte contre la criminalité organisée, je vous demande de mobiliser tous les moyens

[1] Selon une étude de l'Union européenne du 11 janvier 2024.

à votre disposition afin d'obtenir **la coopération des fournisseurs de services ou de messageries électroniques**, y compris s'ils sont établis en dehors du territoire national, et de **recueillir les preuves numériques** nécessaires aux enquêtes pénales dont vous avez la charge, que ce soit aux niveaux national, inter-régional ou territorial.

Il conviendra ainsi de les solliciter systématiquement à chaque fois que les nécessités de l'enquête l'exigent.

Dans le cadre de la coopération policière, des **réquisitions judiciaires** pourront ainsi être **directement adressées aux fournisseurs de services ou de messageries électroniques, y compris s'ils sont établis en dehors du territoire national**, afin d'obtenir la communication des données électroniques nécessaires à l'identification des utilisateurs ou à leur localisation[2].

Lorsque l'enquête judiciaire impose d'accéder à des données de contenu, vous pourrez mobiliser les **différentes techniques spéciales d'enquête prévues par le code de procédure pénale**[3] afin d'accéder aux communications et aux données stockées ou archivées dans les serveurs de ces fournisseurs. Vous pourrez également solliciter directement ces derniers afin que ces éléments de preuve vous soient remis volontairement. Ces demandes peuvent être facilitées par l'utilisation des plateformes dédiées[4].

En l'absence de remise volontaire des données par les fournisseurs, le bureau de l'entraide pénale internationale de la DACG pourra être utilement contacté pour s'assurer des canaux conventionnels et signaler la sensibilité ou l'urgence de la demande. Par ailleurs, les acteurs permettant de faciliter l'exécution des demandes d'entraide pénale internationale pourront utilement être mobilisés (magistrats de liaison, attachés de sécurité intérieure, réseau judiciaire européen, EUROJUST, EUROPOL), notamment dans le cadre des enquêtes les plus sensibles.

L'Office anti-cybercriminalité (OFAC) de la police nationale et l'Unité nationale cyber (UNC) de la gendarmerie nationale, ainsi que leurs antennes respectives, pourront également être sollicités afin de préciser, selon les fournisseurs de services ou de messageries électroniques requis, toutes les informations utiles à l'obtention de ces données, et en particulier :

- Les **points de contacts** (adresses courriels ; numéros de téléphone) pouvant recevoir ces demandes ;
- Les **filiales de ces sociétés** ;
- Les données accessibles par le biais d'une simple **réquisition judiciaire** ou celles nécessitant une **demande d'entraide pénale internationale** (DEPI), une **commission rogatoire internationale** (CRI) ou une **décision d'enquête européenne** (DEE), ainsi que des **modèles de réquisition judiciaire** conformes aux recommandations des fournisseurs de services ou de messageries électroniques requis.

---

[2] Vous veillerez, dans cette perspective, à la qualité des réquisitions adressées, au besoin en prenant l'attache des services d'enquête spécialisés en lien avec ces opérateurs.

[3] Selon les situations, il pourra être envisagé de recourir aux techniques **d'interception des correspondances émises par la voie des communications électroniques** (articles 100 à 100-8 et 706-95 CPP), **d'accès à distance aux correspondances stockées par la voie des communications électroniques accessibles au moyen d'un identifiant informatique** (articles 706-95-1 à 706-95-3 CPP) ou de **captation des données informatiques** (article 706-102-1 à 706-102-5 CPP).

[4] Plusieurs plateformes sont spécialisées dans **l'échange volontaire d'informations**, par exemple la **plateforme privée KODEX**. Cette dernière est un intermédiaire entre les autorités publiques, qui peuvent adresser gratuitement leurs demandes de communication volontaire de données, et les fournisseurs de service. Elle permet de solliciter la communication volontaire de tout type de données détenues par de nombreuses sociétés, telles que *Discord*, *LinkedIn*, *Grindr*, *Binance*, *Coinbase*, *Strava*, *Airbnb*, *Vodafone Global* ou encore *OpenAI*.

En cas de risque de dissipation des données, et lorsque les conventions le permettent[5], le gel des données pourra être sollicité préalablement à l'émission d'une DEPI. A cette fin, l'OFAC constitue le point de contact national pour ces demandes.

En raison de l'enjeu attaché à l'obtention de ces données, **l'absence de réponse d'un fournisseur ou le chiffrement des données** ne doit en effet pas constituer un obstacle à l'envoi de ces demandes dès lors qu'elles sont justifiées par les nécessités de la procédure judiciaire. Cette démarche doit, au contraire, vous permettre de distinguer les fournisseurs de services qui coopèrent de ceux qui, par leur absence systématique de réponse, adopteraient un positionnement pouvant s'apparenter à une volonté délibérée de se soustraire aux demandes de l'autorité judiciaire, voire de faciliter la commission d'infractions ou l'impunité de leurs auteurs.

Sans préjudice des poursuites judiciaires qui pourraient être diligentées sur le fondement des articles 60-1 et 77-1-1 du code de procédure pénale, **le recensement des refus ou des carences systématiques des fournisseurs de services** fréquemment utilisés par les réseaux criminels pourra opportunément faire l'objet d'une remontée d'information aux parquets disposant d'une compétence nationale spécialisée[6] afin de leur permettre, dans le cadre d'une stratégie concertée, d'initier des enquêtes à l'encontre de ces acteurs problématiques, à chaque fois qu'il pourra être démontré que leurs agissements facilitent sciemment la poursuite d'un objectif criminel[7].

Je vous saurais gré de bien vouloir également tenir la direction des affaires criminelles et des grâces informées, sous le timbre du bureau de la police judiciaire, de la mise en œuvre de la présente circulaire, et des difficultés rencontrées avec les opérateurs requis, d'une part dans le cadre de vos remontées d'information sur les affaires individuelles, d'autre part dans un rapport qui lui sera transmis pour le 1er juillet 2026.

Gerald DARMANIN

[5] Notamment la convention du conseil de l'Europe sur la cybercriminalité du 23 novembre 2001 dite de Budapest, et prochainement la Convention des Nations Unies contre la cybercriminalité

[6] Parquet national anti-criminalité organisée (PNACO) et section cyber du parquet de Paris.

[7] Outre les infractions de droit commun résultant de l'absence de réponse aux réquisitions découlant des articles 60-1 et 77-1-1 du CPP, les infractions de refus de communiquer, sur demande des autorités habilitées, les informations ou documents nécessaires pour la réalisation et l'exploitation des interceptions autorisées par la loi ou bien le refus de remettre une convention secrète de déchiffrement d'un moyen de cryptologie susceptible d'avoir été utilisé pour préparer, faciliter ou commettre un crime ou un délit, pour quiconque ayant connaissance de la convention secrète, sur les réquisitions de ces autorités, pourront être mobilisées dans le cadre des poursuites envisagées à l'encontre des personnes physiques ou morales en charge des fournisseurs de services concernés. La complicité des délits/crimes principaux, objets de la réquisition initiale, ou bien l'association de malfaiteurs en vue de préparer la commission de ces délits/crimes pourra être également utilement retenue à l'encontre des administrateurs des fournisseurs de service concernés ou bien de la personne morale. Enfin, l'infraction d'administration d'une plateforme en ligne pour permettre une transaction illicite en bande organisée pourra être également étudiée comme motivant les poursuites si les critères légaux sont réunis en fonction du cas d'espèce.