Conseil de
l'Union européenne

Bruxelles, le 31 mai 2024
(OR. en)

10477/24

LIMITE

COSI 102
ENFOPOL 268
IXIM 145
CATS 48
COPEN 289
CYBER 177

NOTE

Origine:	la présidence
Destinataire:	Comité des représentants permanents/Conseil
Objet:	Accès aux données en vue d'une répression efficace: présentation des recommandations du groupe de haut niveau – *Échange de vues*

1. La sécurité intérieure à l'ère numérique

La transformation numérique de nos sociétés offre un énorme potentiel pour une vie meilleure, plus prospère et plus sûre. La maximisation des avantages de l'ère numérique pour les citoyens implique aussi de réduire au minimum les opportunités qu'elle offre à la grande criminalité organisée et au terrorisme.

En Europe, cette transformation numérique a donné naissance à une nouvelle dimension de l'espace de liberté, de sécurité et de justice sans frontières intérieures; un nouveau contexte dans lequel l'Union européenne promeut et protège les valeurs de respect de la dignité humaine, de liberté, de démocratie, d'égalité, d'État de droit et de respect des droits de l'homme. Garantir le droit des Européens à la sécurité et à la sûreté nécessite un renforcement de la sécurité intérieure européenne, notamment grâce au développement et à l'utilisation de nouvelles technologies sûres et centrées sur l'humain et à la mise en œuvre du principe de sécurité dès la conception. Il est essentiel de relever que la prévention et la détection de la grande criminalité organisée, ainsi que les enquêtes et les poursuites en la matière, requièrent la disponibilité de preuves électroniques et l'accès à celles-ci.

Aujourd'hui, toutes les enquêtes et poursuites menées avec succès dans des affaires de grande criminalité ou de criminalité organisée reposent sur des preuves électroniques. Paradoxalement, si la transformation numérique a conduit à la création, à la transmission et au stockage d'un volume de données toujours plus important, la disponibilité et l'accès aux preuves électroniques à des fins répressives et pénales sont apparus comme le principal défi pour protéger les citoyens de l'Union contre la menace que représentent le terrorisme et la grande criminalité organisée.

Bien que ce défi ne soit pas nouveau, il continue de gagner en importance chaque jour. Les services répressifs "perdent la vision", littéralement. Dès juin 2017, le Conseil européen appelait à "*relever les défis que posent les systèmes qui permettent aux terroristes de communiquer par des moyens auxquels les autorités compétentes ne peuvent avoir accès, y compris le chiffrement de bout en bout, tout en préservant les avantages que ces systèmes offrent en matière de protection de la vie privée, des données et des communications*" et estimait que "*l'accès effectif aux preuves électroniques est essentiel pour lutter contre les formes graves de criminalité et le terrorisme et que, sous réserve de garanties appropriées, la disponibilité des données devrait être assurée*"[1]. Dans son arrêt du 30 avril 2024, la Cour de justice a souligné, en ce qui concerne l'accès aux adresses IP dans le cadre d'infractions pénales commises en ligne, que le fait de "*[n]e pas permettre un tel accès comporterait [...] un réel risque d'impunité systémique [...] d'infractions pénales commises en ligne ou dont la commission ou la préparation est facilitée par les caractéristiques propres à Internet*"[2].

[1] Conclusions du Conseil européen des 22 et 23 juin 2017, point 2.
[2] Arrêt du 30 avril 2024, La Quadrature du Net, C- 470/21, EU:C:2024:370, point 119.

2. Le groupe de haut niveau sur l'accès aux données en vue d'une répression efficace

Afin de déterminer la voie à suivre, la présidence suédoise, en coopération avec les présidences espagnole et belge, a lancé, en juin 2023, un groupe de haut niveau (GHN) sur l'accès aux données en vue d'une répression efficace, institué par une décision de la Commission du 6 juin 2023, composé de représentants des États membres, de la Commission, d'organes et organismes compétents de l'UE et du coordinateur de l'UE pour la lutte contre le terrorisme. Examinant les défis auxquels les membres des services répressifs de l'Union sont confrontés dans leur travail quotidien, les experts ont recensé un ensemble de recommandations, figurant à l'annexe de la présente note, afin de relever les défis actuels et attendus dans le contexte des évolutions technologiques, ce qui permettra d'adopter une approche globale de l'UE pour garantir l'efficacité des enquêtes et des poursuites pénales en tant qu'élément essentiel de l'État de droit. Ces recommandations ne sont pas contraignantes, mais elles peuvent apporter une contribution significative aux choix politiques qui seront formés aux niveaux national et de l'UE dans les années à venir.

Le comité de coordination dans le domaine de la coopération policière et judiciaire en matière pénale (CATS), le 23 mai 2024, et le comité permanent de coopération opérationnelle en matière de sécurité intérieure (COSI), le 29 mai 2024, ont débattu des recommandations du GHN dans la perspective de l'échange de vues qui aura lieu au sein du Conseil. Les deux comités ont exprimé leur soutien au processus mené par le GHN et ont salué le travail accompli par les experts.

Le COSI a recensé les principales questions qui pourraient constituer des priorités pour la prochaine législature:

1. la mise en place de règles pour un accès effectif aux données à des fins répressives couvrant tous les fournisseurs de services de communications électroniques,

2. un cadre législatif harmonisé sur la conservation des données à des fins répressives au niveau de l'Union, et

3. des solutions solides du point de vue juridique et technique pour accéder à des données chiffrées, à des conditions spécifiques et dans des cas individuels, sans affaiblissement généralisé du chiffrement.

La législation et la jurisprudence existantes pourraient déjà être répertoriées. Le COSI a suggéré de lancer sans retard des activités dans les domaines du renforcement des capacités, de la normalisation et de la coopération avec l'industrie, en utilisant au mieux les structures existantes et en les renforçant, y compris le pôle d'innovation de l'UE pour la sécurité intérieure et les agences de l'UE. Le COSI s'est exprimé en faveur de l'élaboration, sur la base des priorités à définir par le Conseil, d'une feuille de route prévoyant un calendrier précis et couvrant les aspects financiers. Les délégations ont également souligné la nécessité d'assurer la coordination des activités.

3. Questions aux ministres

La présidence invite les ministres à répondre aux questions suivantes:

1. Quelles sont les trois questions qui devraient être traitées en tant que priorités politiques pour la prochaine législature?

2. Comment le Conseil et ses structures pourraient-ils soutenir la mise en œuvre rapide des priorités politiques de la manière la plus efficace possible?

4. Suggestion pour la suite des travaux

Le Conseil est invité à prendre note des recommandations du GHN sur l'accès aux données en vue d'une répression efficace, et à demander aux prochaines présidences et à la Commission de faire avancer d'urgence ces travaux importants.

ANNEXE

Recommandations du groupe de haut niveau sur l'accès aux données en vue d'une répression efficace

Les points de vue exposés reflètent exclusivement l'opinion des experts et ne sauraient être considérés comme représentatifs d'une prise de position formelle de la Commission européenne.

Introduction

L'Union européenne constitue un espace de liberté, de sécurité et de justice dans le respect des droits fondamentaux et des différents systèmes et traditions juridiques des États membres[3]. Elle œuvre pour assurer un niveau élevé de sécurité par des mesures de prévention de la grande criminalité organisée ainsi que de lutte contre celle-ci, y compris le renforcement de la coopération policière et judiciaire transfrontière[4], à l'exclusion de toute ingérence dans la sécurité nationale, qui reste de la compétence exclusive des États membres. Pour assurer une approche efficace de la lutte contre la criminalité et d'autres défis liés au maintien d'un niveau élevé de sécurité, les services répressifs doivent pouvoir accomplir leurs missions de manière effective et légale et dans le plein respect des droits fondamentaux, afin de prévenir et de détecter les infractions pénales, d'enquêter sur celles-ci et d'assurer leur poursuite, de servir la justice dans l'intérêt général, en particulier celui des victimes, et de préserver la sécurité publique.

3 Traité sur le fonctionnement de l'Union européenne (TFUE), article 67, paragraphe 1.
4 Ibid, paragraphe 3.

Ces dernières années, malgré la création, la transmission et le stockage de quantités toujours plus importantes de données, l'accès aux données à des fins répressives est apparu comme un défi majeur pour mener des enquêtes et des poursuites sur des infractions pénales et pour faire respecter le droit de manière effective. L'UE a mis en place des règles strictes pour faciliter l'accès transfrontière aux preuves électroniques (ci-après les "règles de l'UE en matière de preuves électroniques")[5]. Toutefois, le fait qu'il n'existe pas d'obligation de conservation des données a une incidence négative sur l'efficacité des règles en matière de preuves électroniques, étant donné qu'il n'y a aucune garantie que toutes les informations faisant l'objet d'injonctions européennes de conservation ou de production, y compris les données relatives au trafic, les données demandées à la seule fin d'identifier l'utilisateur et les données relatives aux abonnés, soient disponibles. En outre, les règles de l'UE en matière de preuves électroniques ne couvrent que les données en possession des fournisseurs de services et ne répondent pas au problème du chiffrement, avec pour conséquence qu'en l'absence de mesures opérationnelles autorisant un accès légal aux données, la législation risque de ne pas pouvoir être appliquée de manière efficace. Aux fins du présent document, on entend par "accès aux données" l'accès accordé aux services répressifs, soumis à autorisation judiciaire ex ante si nécessaire, aux fins d'enquêtes pénales et au cas par cas. En règle générale, dans les cas où une telle autorisation judiciaire est nécessaire en raison du caractère sensible des données en question, elle fait partie intégrante du cadre juridique et opérationnel applicable. L'accès aux données doit se faire dans le plein respect des droits fondamentaux, ainsi que de la jurisprudence de la Cour de justice de l'Union européenne (CJUE) et des arrêts de la Cour européenne des droits de l'homme sur ces questions, ainsi que des garanties procédurales applicables.

[5] *Voir Preuves électroniques - accès transfrontière aux preuves électroniques (Commission européenne) (en anglais seulement). Les nouvelles règles entreront en vigueur le 17 août 2023 et s'appliqueront à compter du 17 février 2026 pour la directive et du 17 août 2026 pour le règlement.*

Ce défi figure depuis longtemps à l'ordre du jour politique. Entre autres, le Conseil européen, le Conseil[6], le Parlement européen[7], la CJUE et les agences de l'UE ont mené des discussions et formulé des conclusions sur divers aspects juridiques et politiques de l'accès aux données de communications électroniques, y compris les données relatives au trafic et les données de localisation (métadonnées), et plus généralement aux preuves électroniques. Dans ses conclusions des 22 et 23 juin 2017[8], le Conseil européen appelait déjà à "relever les défis que posent les systèmes qui permettent aux terroristes de communiquer par des moyens auxquels les autorités compétentes ne peuvent avoir accès, y compris le chiffrement de bout en bout, tout en préservant les avantages que ces systèmes offrent en matière de protection de la vie privée, des données et des communications" et soulignait que "l'accès effectif aux preuves électroniques est essentiel pour lutter contre les formes graves de criminalité".

La stratégie de l'UE visant à lutter contre la criminalité organisée (2021-2025) souligne l'importance de l'accès aux données de communications électroniques pour lutter contre la criminalité organisée et de faire en sorte que les services répressifs et l'appareil judiciaire soient adaptés à l'ère numérique[9]. L'accès aux données revêt également une importance capitale pour toutes les priorités de l'EMPACT dans la lutte contre la grande criminalité organisée pour la période 2022-2025[10], et la stratégie de l'UE pour l'union de la sécurité a indiqué que la Commission étudierait des mesures visant à renforcer les capacités répressives dans le cadre des enquêtes numériques[11]. En 2023, la présidence suédoise du Conseil a présenté le document sur les besoins opérationnels des services répressifs en matière d'accès légal aux communications (Law Enforcement – Operational Needs for Lawful Access to Communications (LEON)"[12], qui dresse une liste complète des besoins opérationnels des services répressifs en ce qui concerne les réseaux et services de communication[13].

---

6 Doc. 10007/16, *Conclusions du Conseil sur l'amélioration de la justice pénale dans le cyberespace*.

7 JO C 346 du 27.9.2018, p. 29, *Résolution du Parlement européen du 3 octobre 2017 sur la lutte contre la cybercriminalité.*

8 Doc. EUCO 8/17.

9 *Communication de la Commission relative à la stratégie de l'UE visant à lutter contre la criminalité organisée (2021-2025)*, COM(2021)170, 14 avril 2021.

10 Doc. 8665/21.

11 *Communication de la Commission relative à la stratégie de l'UE pour l''union de la sécurité,* COM/2020/605 final, 24 juillet 2020.

12 LEON est le résultat de travaux menés par les services répressifs suédois en étroite coopération avec les représentants des services répressifs d'États membres de l'UE, d'Amérique du Nord et d'Australie. L'objectif est de recenser et de décrire les besoins des services répressifs en matière d'accès licite aux contenus de communications, aux données relatives au contenu et aux informations relatives aux abonnés.

13 *Communication from the Council Presidency on Law Enforcement Operational Needs for Lawful Access to Communications (LEON),* doc. 6050/23 du 16 février 2023.

Pour déterminer les éventuelles voies à suivre, la présidence suédoise, en coopération avec les présidences espagnole et belge prenant sa suite, a lancé le groupe de haut niveau (GHN) sur l'accès aux données en vue d'une répression efficace, composé de représentants de haut niveau des États membres, de la Commission, d'organes et organismes compétents de l'UE, et du coordinateur de l'UE pour la lutte contre le terrorisme, en juin 2023[14]. Coprésidé par la Commission et par la présidence tournante du Conseil de l'UE, le GHN a étudié les défis auxquels les membres des services répressifs de l'Union sont quotidiennement confrontés en matière d'accès aux données, et a établi des solutions et des recommandations potentielles pour les surmonter, dans le but de garantir la disponibilité d'outils répressifs efficaces pour lutter contre la criminalité et renforcer la sécurité publique à l'ère numérique, dans le plein respect des droits fondamentaux.

Tout au long de ses travaux, le GHN a mis en évidence par de nombreux éléments le manque persistant, voire croissant, d'accès effectif aux données, et en a fait état à plusieurs reprises. En outre, d'autres éléments l'illustrant sont encore en cours de collecte dans le cadre de consultations ciblées. Les données de communication générées, traitées ou stockées numériquement (métadonnées et données relatives au contenu) constituent un élément important des enquêtes pénales modernes[15]. Les criminels ayant de plus en plus recours aux services en ligne, les demandes de données adressées aux fournisseurs de services en ligne ont triplé entre 2017 et 2022[16].

---

14 *Commission decision setting up a high-level group on access to data for effective law enforcement* (Décision de la Commission instituant un groupe de haut niveau sur l'accès aux données en vue d'une répression efficace), C(2023) 3647, 6 juin 2023

15 Analyse d'impact accompagnant la proposition de règlement du Parlement européen et du Conseil relatif aux injonctions européennes de production et de conservation de preuves électroniques en matière pénale et la proposition de directive du Parlement européen et du Conseil établissant des règles harmonisées concernant la désignation de représentants légaux aux fins de la collecte de preuves en matière pénale [COM(2018) 225 final] - [COM(2018) 226 final] - [SWD(2018) 119 final].

16 Rapport SIRIUS pour 2023, https://www.eurojust.europa.eu/sites/default/files/assets/sirius-eueesr-2023.pdf, p. 69.

Le GHN maintient que les services répressifs sont confrontés à des défis opérationnels croissants lorsqu'ils cherchent à accéder légalement à des données générées, traitées ou stockées numériquement dans un format lisible. Quarante-sept pour cent des répondants à l'enquête annuelle la plus récente du projet SIRIUS sur l'accès transfrontière aux preuves électroniques ont indiqué que le manque de conservation des données était le principal problème auquel ils se heurtaient[17] et, dès 2018, on estimait qu'en 2019, plus de 22 % des messages échangés dans le monde seraient chiffrés de bout en bout et inaccessibles aux services répressifs[18]. Le GHN a constaté que l'absence de cadre juridique adéquat permettant de procéder à l'interception légale de services de télécommunications non traditionnels avait également des conséquences importantes sur l'action répressive: plus de 90 % des messages sont échangés via ce type de services "par contournement" (over-the-top ou OTT).

Face à ce constat, le groupe de haut niveau a formulé des recommandations stratégiques tournées vers l'avenir afin de relever les défis actuels et prévisibles compte tenu des évolutions technologiques, permettant ainsi une approche globale de l'UE pour garantir l'accès aux données en vue d'une répression efficace. Ces recommandations ont été formulées par les experts des groupes de travail du GHN, qui ont été sélectionnés par les États membres et par les organes et agences concernés de l'UE. Les experts comprenaient principalement des représentants des services répressifs et des autorités judiciaires, mais aussi des professionnels de la cybersécurité et des experts en protection des données.

Les recommandations qui suivent dans le présent rapport ont été formulées à partir des trois cas d'utilisation selon lesquels les groupes de travail ont été organisés. Les recommandations ont été regroupées par axe de travail et approuvées par le GHN lors de sa 4ème session plénière, le 21 mai 2024. Dans un deuxième temps, ces recommandations seront mises en œuvre et feront l'objet d'une évaluation de leur faisabilité juridique, technique et financière, en gardant à l'esprit que les ressources budgétaires et humaines disponibles au titre du budget de l'UE sont limitées, en vue de présenter un rapport final à l'automne 2024.

17 Ibid, p. 46.

18 https://www.csis.org/blogs/strategic-technologies-blog/scoping-law-enforcements-encrypted-messaging-problem.

Principales raisons sous-tendant les recommandations

Les contributions présentées ci-dessus, ainsi que les discussions approfondies tenues lors de trois réunions plénières du GHN, de neuf réunions de groupes d'experts et d'une réunion de consultation publique, et des contributions écrites, ont permis de recenser les principales sources de problèmes qui sous-tendent les défis exposés ci-avant et qui justifient les recommandations.

En ce qui concerne l'**accès aux données au repos dans l'appareil d'un utilisateur**, le GHN a identifié les principaux problèmes suivants: l'absence de coopération transfrontière entre services répressifs en ce qui concerne le partage d'outils de criminalistique numérique; l'insuffisance de la coopération entre les services répressifs et les prestataires, les fabricants et les fournisseurs de matériel et logiciels concernés, ce qui entrave la capacité d'accéder aux données en clair; la difficulté d'accéder légalement à l'appareil d'un utilisateur et, si l'accès est possible, d'extraire et de déchiffrer les données et métadonnées disponibles pour obtenir des informations intelligibles susceptibles d'être utiles aux enquêtes et d'être présentées à titre de preuves recevables devant les tribunaux.

Le GHN estime que le rythme des évolutions technologiques liées au **chiffrement** des informations sur les appareils est rapide, au point que les outils et techniques de déchiffrement existants deviennent inefficaces. Cela est particulièrement vrai dans les cas où des suspects et des groupes criminels organisés ont recours à des dispositifs et des réseaux de communication spécialement conçus. Le temps nécessaire pour déchiffrer les données extraites des dispositifs constitue également un problème important: les experts ont indiqué que cela peut prendre jusqu'à deux ans dans certains cas. Le degré de difficulté lié au déchiffrement des appareils sur mesure qui ont été conçus et commercialisés exclusivement à des fins criminelles est encore plus élevé et pose des défis supplémentaires aux services de criminalistique numérique dans l'ensemble des États membres.

Toutefois, il importe que les solutions techniques permettant aux autorités d'utiliser leurs pouvoirs d'enquête préservent tous les avantages du chiffrement pour des raisons de protection des données, de respect de la vie privée, de cybersécurité et de sécurité nationale. Ce principe de "sécurité par le chiffrement et sécurité malgré le chiffrement" était un principe central des discussions du GHN, et les futurs outils ou solutions techniques qui sont mis au point ne doivent pas conduire à compromettre ou à affaiblir les technologies de chiffrement pour la communication d'autres utilisateurs qui ne sont pas visés par la mesure d'accès licite.

Une question essentielle soulevée par le GHN est **le manque de mécanismes de coopération transfrontière entre services répressifs** en ce qui concerne le partage d'outils de criminalistique numérique entre les États membres, qui disposent souvent de solutions distinctes pour résoudre des problèmes techniques similaires. Bien qu'Europol héberge un répertoire interne d'outils auxquels les services répressifs nationaux peuvent recourir, il est probable que les États membres aient accès à d'autres outils et à des logiciels de déchiffrement sur mesure. Or ils s'abstiennent de les partager, soit en raison d'un manque de confiance et de communication entre les services de criminalistique numérique concernés, soit parce qu'ils ne sont pas autorisés à le faire par la loi, souvent pour des préoccupations de sécurité nationale.

Le GHN est convenu que des **réseaux** tels que le Réseau européen des instituts de police scientifique (ENFSI[19]) consacrés à la coordination et au partage des connaissances en matière de méthodes, d'outils et de bonnes pratiques en matière de criminalistique numérique sont essentiels pour les praticiens de la criminalistique numérique dans l'ensemble de l'UE. De tels réseaux existent déjà, mais pour améliorer la communication et la collaboration entre les services de criminalistique numérique des différents États membres, ils devraient être recensés et davantage soutenus afin de favoriser tant de meilleures connaissances qu'un meilleur partage des outils[20], en s'appuyant sur un système centralisé. Le GHN a également souligné que le coût d'outils de criminalistique numérique sur le marché constituait un obstacle important dans l'ensemble des États membres, et qu'il conviendrait de poursuivre la recherche et le développement d'outils au niveau de l'UE ainsi que de recourir à des mécanismes existants, tels que l'Association européenne pour le développement de technologies de lutte contre la cybercriminalité (EACTDA) et la plateforme Europol Tool Repository, pour assurer leur diffusion[21]. L'évaluation et la certification des outils disponibles sur le marché a constitué un autre point de discussion récurrent[22], et le GHN est largement tombé d'accord sur le fait qu'il serait justifié de mettre en place un mécanisme ou un système visant à garantir que ces outils respectent les normes en matière de responsabilité et de criminalistique au sein de l'Union. L'évaluation et la certification sont nécessaires pour garantir que les technologies satisfont aux exigences de fiabilité (par exemple, les exigences relatives à l'intégrité des données tout au long du processus de criminalistique numérique), que le fabricant soit établi au sein de l'UE ou en dehors de celle-ci.

---

19 https://enfsi.eu/
20 Voir la recommandation nº 1.
21 Voir les recommandations nos 3 et 4.
22 Voir la recommandation nº 5.

Parmi les problèmes relevés par le GHN figurait également un **déclin de la communication** entre les services répressifs et les prestataires et fournisseurs de matériel et de logiciels; en conséquence, les services répressifs éprouvent des difficultés à dialoguer avec l'industrie pour obtenir l'accès aux données sur les dispositifs saisis. Le GHN a conclu qu'un manque de connaissances portait préjudice aux interactions entre les services répressifs et les producteurs de matériel et de logiciels. Le déclin de la communication entre les services répressifs et l'industrie a également conduit à une baisse du nombre de protocoles mis en place pour permettre un accès légal aux données des appareils des utilisateurs. Le GHN a indiqué que le manque de participation des services répressifs aux organismes de normalisation affectait la possibilité de mettre au point les protocoles des produits et l'architecture technique de telle sorte que leurs préoccupations et exigences techniques soient prises en compte à un stade précoce de l'élaboration des futures normes technologiques[23].

L'une des dernières questions clés abordées par le GHN était que, en l'absence de coopération volontaire, **le fait qu'il n'existe pas d'obligation pour l'industrie** de coopérer dans le cadre de demandes des services répressifs visant à obtenir les données au repos dans l'appareil d'un utilisateur a une incidence négative sur la capacité de ces services à mener des enquêtes approfondies. Le groupe a constaté l'absence de toute vue d'ensemble des obligations existantes au niveau des États membres[24].

Pour ce qui est de l'**accès aux données au repos dans le système d'un fournisseur de services**, la première question essentielle à laquelle les services répressifs sont confrontées concerne les divergences entre les cadres juridiques nationaux régissant la conservation des données au sein des systèmes des fournisseurs et la durée de cette conservation.

[23] Voir la recommandation nº 12.
[24] Voir la recommandation nº 25.

Les experts ont notamment souligné qu'il n'existe actuellement aucune sorte d'**harmonisation de la législation sur la conservation des données** dans l'ensemble de l'UE et qu'il est complexe de satisfaire aux critères indiqués par la CJUE, qui limitent la conservation généralisée et indifférenciée des données relatives au trafic et des données de localisation dans des circonstances spécifiques à la lutte contre les menaces graves pour la sécurité, et n'autorisent que la conservation ciblée de ces données pour lutter contre la criminalité grave. En particulier, la notion de conservation ciblée des données s'avère très difficile à mettre en œuvre pour les États membres, en partie aussi parce que certains des critères ont été conçus sur la base de technologies qui ont évolué depuis que ces arrêts ont été rendus[25], et un manque de clarté demeure quant aux types de données auxquelles il est possible d'accéder pour des infractions dépourvues de gravité.

Le GHN a estimé qu'une approche harmonisée de la conservation des données au niveau de l'UE était indispensable à l'efficacité des enquêtes, en particulier dans les affaires transfrontières, et à l'admissibilité des preuves devant les tribunaux. Le groupe a également discuté de la manière dont l'absence d'obligations de conservation des données peut affecter l'efficacité des nouvelles règles en matière de preuves électroniques, étant donné que les données relatives au trafic faisant l'objet d'injonctions européennes de conservation ou de production pourraient ne pas être disponibles.

Le GHN est d'avis que toute solution aux défis actuels doit être neutre sur le plan technologique afin de couvrir les futures évolutions techniques, quelles qu'elles soient. L'accent a été mis sur la nécessité que de telles solutions créent des obligations pour tous les fournisseurs de services, y compris les OTT, qui devraient être tenus de répondre aux demandes des services répressifs et d'être plus transparents en ce qui concerne les données qu'ils collectent à des fins professionnelles. Un tel régime pourrait être mis en place au moyen **de mesures législatives ou non contraignantes**, avec une préférence pour les premières[26].

---

25 Par exemple, des technologies telles que les adresses IP dynamiques et la traduction d'adresse réseau de classe transporteur (NAT de classe transporteur ou CGN) n'avaient pas atteint leur plein développement au moment où ont été rendus les arrêts de la CJUE qui suggéraient la conservation des données sur la base d'un ciblage géographique (voir les arrêts de référence Digital Rights Ireland, de 2014, et Tele2 Sverige AB, de 2016).

26 Voir la recommandation nº 27.

À la lumière de la jurisprudence relative à la conservation des données, le GHN a examiné comment appliquer la **conservation ciblée** dans la pratique et a souligné les difficultés que posait la mise en œuvre des exigences de la Cour (c'est-à-dire la conservation ciblée sur la base de critères géographiques et de catégories de personnes). Les experts ont estimé que la mise en œuvre des exigences de la Cour posait des problèmes en ce qui concerne les droits fondamentaux (en raison d'une discrimination à l'encontre de catégories de personnes ou de la localisation), d'un point de vue opérationnel (le ciblage de la collecte de données réduisant considérablement la capacité d'accès aux informations essentielles pour les enquêtes), et du point de vue de la mise en œuvre technique pour les opérateurs. Compte tenu de ces considérations, de nombreux experts ont déclaré qu'un régime de l'UE devrait se concentrer non seulement sur la conservation, mais aussi sur l'accès. En particulier, certains experts étaient d'avis que les catégories d'infractions, en fonction desquelles des différences seraient établies dans les délais d'accès aux données conservées, devraient constituer le seul critère régissant les régimes de conservation des données, et que des solutions pour un accès très ciblé devraient être conçues sur la base d'autres critères[27]. Toutefois, d'autres experts ont exprimé des inquiétudes quant à la conformité de telles mesures à la jurisprudence de la CJUE, étant donné que cette dernière s'applique à la fois à la conservation des données et à l'accès aux données.

Parmi les problèmes recensés, les services répressifs rencontrent aussi des difficultés en ce qui concerne les **types de métadonnées conservées** par les fournisseurs de services. Lorsque des obligations légales existent, elles laissent parfois une certaine souplesse aux fournisseurs de services de communication en ce qui concerne les types de métadonnées à conserver; il en résulte une multitude de données disponibles qui constituent des indices d'une utilité variable pour les enquêtes. Le GHN a considéré que l'UE devrait exiger des niveaux minimaux de conservation (au moins des données nécessaires à l'identification d'un utilisateur), qui devraient être imposés aux opérateurs au niveau de l'Union[28]. Le GHN est également convenu que les fournisseurs de services proposant des services chiffrés doivent être tenus de trouver les moyens de fournir des données intelligibles en réponse aux demandes légales émanant des services répressifs et des autorités judiciaires[29].

---

27 Voir la recommandation nº 29.
28 Voir la recommandation nº 27, point v.
29 Voir la recommandation nº 27, point iii.

Le passage des fournisseurs de services de communication traditionnels à l'utilisation de **services par contournement** est un facteur essentiel à l'origine des difficultés auxquelles les services répressifs sont confrontés lorsqu'ils tentent d'accéder aux données stockées dans les systèmes des fournisseurs de services. Bien que les services par contournement relèvent du champ d'application du code des communications électroniques européen (CCEE), ils ne sont pas soumis à des systèmes d'octroi de licences comparables qui peuvent entraîner des obligations à cet égard. Les experts ont discuté de la nécessité impérieuse d'établir des règles obligeant les services par contournement à conserver des données même lorsque ces services sont installés dans des juridictions différentes. L'absence de telles règles entraîne un manque de clarté et une certaine insécurité juridique ayant pour conséquence une non-conformité de leur part. En outre, il arrive que certains services par contournement ne conservent absolument aucune donnée.

Le GHN s'est accordé sur la nécessité de **transparence** en ce qui concerne les données générées, traitées et stockées par les fournisseurs de services de communication, notamment, en particulier, les services par contournement et d'autres services qui proposent des "services de communication" (tels que les constructeurs automobiles)[30], et a discuté des instruments permettant d'assurer le respect des règles avant toute mise en service sur le marché de l'UE[31]. Les experts ont examiné l'opportunité de légiférer sur les données que les fournisseurs ont déjà en leur possession à des fins professionnelles[32].

Dans ce contexte, les experts sont convenus de la nécessité de mettre en place des **mécanismes de coopération** avec le secteur privé visant à accroître la transparence, et ont avancé plusieurs pistes à cet effet, notamment au moyen de protocoles d'accord[33] et par le renforcement et la pleine exploitation des structures existantes, comme par exemple la plateforme SIRIUS, le RJE[34] et/ou le RJEC[35].

---

30 Voir la recommandation nº 17.
31 Voir la recommandation nº 30.
32 Voir la recommandation nº 31.
33 Voir la recommandation nº 14.
34 Le réseau judiciaire européen est un réseau constitué de points de contact nationaux qui a pour objectif de faciliter la coopération judiciaire en matière pénale.
35 Voir la recommandation nº 13.

Le GHN a estimé qu'il était utile de renforcer la coopération, y compris en ce qui concerne la définition de formats normalisés pour la conservation des données[36]. En fait, s'il existe une norme élaborée sous les auspices de l'Institut européen des normes de télécommunications (ETSI) ayant trait aux métadonnées dans les télécommunications traditionnelles, celle-ci n'est pas appliquée de manière universelle dans tous les États membres, même pour ce qui est des fournisseurs de services de télécommunications, et il n'y a aucun accord sur un format normalisé pour les transmissions de données des services par contournement aux services répressifs. Cela complique encore l'analyse des données, pour autant que des données puissent être fournies.

Il convient de poursuivre la **normalisation** afin de veiller à ce que les données soient classées d'une manière harmonisée en vue de leur conservation et de l'accès à celles-ci, mais aussi de mettre en place des canaux sécurisés pour les échanges entre les autorités compétentes et les fournisseurs de services. Le GHN a examiné plusieurs possibilités à cet effet, et s'est notamment concentré sur une participation coordonnée accrue des représentants des services répressifs dans les organismes de normalisation concernés[37].

La plupart des États membres disposent de cadres nationaux spécifiques règlementant l'**accès en temps réel aux données de communication**; accès qui demeure un outil essentiel dans la lutte contre la criminalité, y compris la criminalité en ligne et la criminalité organisée, ainsi que le terrorisme.

Toutefois, lorsqu'il est question des fournisseurs de services non traditionnels, les services répressifs ne peuvent s'appuyer sur aucun cadre contraignant et harmonisé. En fait, si certains États membres ont mis en place des réglementations qui obligent les services par contournement à répondre aux demandes légales d'accès, on constate une **mise en œuvre inégale** entre les fournisseurs de services de communication et les services par contournement en ce qui concerne l'accès en temps réel aux données, les services par contournement ne mettant généralement pas en œuvre ces obligations pour des raisons juridiques et techniques.

---

36 Voir les recommandations n^{os} 15 et 16.

37 Voir la recommandation n^{o} 20.

Les experts se sont accordés sur le fait que l'un des principaux objectifs consisterait à **créer des conditions équitables entre les fournisseurs de services de communication[38] et les autres types de fournisseurs de services de communications électroniques** eu égard aux obligations exécutoires en matière d'interception légale; l'interception légale doit être prévue par la loi et autorisée par des juridictions ou des autorités administratives indépendantes conformément aux normes techniques et dans le plein respect de la protection des données et de la vie privée, ainsi que des mesures de cybersécurité et d'interopérabilité. Les experts ont précisé que, dans de nombreux cas, l'interception légale des services de communications électroniques devrait être la mesure privilégiée pour accéder aux données en temps réel. Ces règles en matière d'interception légale devraient être fondées sur des principes qui s'appliquent actuellement aux fournisseurs de services de communication traditionnels, par exemple pour ce qui est de la surveillance et de la coopération avec les fournisseurs de services de communication, mais aussi pour ce qui est de la capacité d'accéder à des données en clair lorsque les autorités judiciaires estiment que cela est nécessaire et proportionné[39].

Les différences qui existent entre les cadres juridiques nationaux des États membres de l'UE sur la question de l'interception de métadonnées ou de données relatives au contenu posent des difficultés aux services répressifs dans les affaires comportant des éléments transfrontières. Par exemple, les services répressifs peuvent éprouver des difficultés à intercepter en temps réel des communications entre deux citoyens de leur pays qui utilisent un service de communication hébergé dans un autre État membre de l'UE ayant des règles de procédure différentes pour l'interception en direct. Les experts ont discuté de l'opportunité de résoudre ces problèmes au niveau de l'UE, et ont détaillé les différentes mesures qui pourraient être mises en œuvre à cette fin, par exemple des mesures législatives[40]. L'incertitude juridique découlant des différences d'exigences entre les cadres juridiques nationaux en matière d'interception a constitué un sujet de discussion central entre les experts, qui ont insisté sur la nécessité de traiter des questions telles que l'application territoriale de certaines obligations, qui entraîne des conflits de lois et des retards ou des obstacles administratifs dans le cadre des enquêtes[41].

Outre les problèmes posés par le manque d'harmonisation au niveau des législations des États membres, les experts ont également discuté du fait que **le manque d'informations concernant la localisation précise des utilisateurs et des données complique souvent la détermination du lien territorial d'une infraction pénale**.

---

38 Fournisseurs de services de télécommunications traditionnels selon la définition de l'ETSI, c'est-à-dire des propriétaires d'infrastructures.

39 Voir la recommandation nº 37.

40 Voir la recommandation nº 38.

41 Voir la recommandation nº 39.

Si les experts s'accordaient sur le fait de continuer à utiliser la décision d'enquête européenne (DEE) afin de demander l'interception par un autre État membre et d'échanger des éléments de preuve recueillis par ce biais, ils ont également discuté des limites de cet outil, notamment en ce qui concerne l'applicabilité partielle dans les États membres[42].

La notion de compétence territoriale en matière de données a été évoquée au cours des discussions. Les experts ont estimé que, dans les cas où le lien est national (lorsqu'une infraction est commise dans un État membre par un criminel situé dans le même État membre par exemple), l'autorité d'un État devrait pouvoir adopter des mesures d'interception au titre du droit procédural national fixant des exigences et des garanties, sans avoir à passer par un instrument de coopération transfrontière. Pour les situations dans lesquelles cela s'avère nécessaire afin de surmonter les conflits de lois avec d'autres juridictions, les experts ont examiné les initiatives que l'UE pourrait prendre, en s'inspirant du règlement sur les preuves électroniques, et qui pourraient également prendre la forme d'accords bilatéraux avec des pays tels que les États-Unis, fondées sur une analyse plus approfondie et une analyse d'impact qui tient également compte des droits fondamentaux et de la souveraineté des États.

Si les experts se sont accordés à dire qu'un certain niveau d'harmonisation au niveau de l'UE pourrait être recherché au moyen de dispositions non contraignantes (par exemple, une recommandation de la Commission), ils ont suggéré que des solutions pour répondre aux besoins opérationnels communs en matière d'interception légale pourraient être développées sur la base du document LEON[43].

Sur le plan technique, les experts ont eu un échange sur **la nécessité de mettre en place des mécanismes et des infrastructures permettant le transfert en temps réel d'interceptions de quantités potentiellement très importantes de données de diverses natures**[44]. À cet égard, les experts ont longuement débattu des avantages de la normalisation et des approches possibles dans ce domaine. Ils ont plaidé en faveur d'une participation accrue des autorités/administrations nationales à l'élaboration des normes pour la 5G/6G et pour la communication en général, et ont insisté sur la nécessité d'être représentés dans les enceintes les plus pertinentes telles que le 3GPP, l'ETSI, l'ISO et l'UIT. Le soutien de la Commission, d'Europol ou d'autres organes ou organismes de l'UE a également été jugé nécessaire[45].

---

42 Voir la recommandation nº 40.
43 Voir la recommandation nº 21.
44 Voir la recommandation nº 9.
45 Voir la recommandation nº 20.

Parallèlement, les experts ont mené une discussion approfondie sur les affaires incluant des fournisseurs non coopératifs et sur la manière de parvenir à sanctionner ceux-ci le cas échéant, par des sanctions administratives et/ou pénales, en fonction de l'intentionnalité[46]. Les experts étaient d'accord sur le fait que tout futur instrument de l'UE à cet égard devrait prendre en compte ce critère[47]. Cet instrument devrait également tenir compte de l'acquis de l'UE, notamment du règlement sur les services numériques.

En ce qui concerne les fournisseurs non coopératifs, les experts ont mené une discussion au terme de laquelle ils se sont accordés sur le fait que, quels que soient les instruments juridiques en place, dans certains **cas spécifiques** (par exemple, lorsqu'il s'agit de services essentiellement criminels, tels qu'EncroChat), **les services répressifs devront toujours exploiter les vulnérabilités** (c'est-à-dire avoir recours à des mesures intrusives). Si le fait que ces cas devraient rester exceptionnels et que de telles solutions sont loin d'être idéales faisait consensus, il importe de coopérer à l'harmonisation de ces aspects, notamment en vue d'établir des garanties[48] et, éventuellement, des règles harmonisées pour l'admissibilité mutuelle des preuves entre les États membres dans la mesure nécessaire pour faciliter la reconnaissance mutuelle des décisions de justice et la coopération policière et judiciaire en matière pénale[49]. Les experts ont insisté sur la manière dont des opérations telles que celles menées contre EncroChat ou Sky ECC sont contestées devant les tribunaux et ont souligné l'insécurité juridique qui découle des exigences différentes des législations nationales en ce qui concerne l'utilisation comme preuve dans un État membre du résultat d'une interception effectuée dans un autre.

Une autre question évoquée comme posant un problème et largement débattue concerne l'**accès aux données dans un format lisible**.

En plus des problèmes d'accès aux données qui se trouvent sur l'appareil, le chiffrement ajoute un certain degré de complexité en ce qui concerne l'accès en temps réel aux données relatives au contenu, tant pour ce qui est des services par contournement lorsqu'un mécanisme de chiffrement de bout en bout est mis en œuvre, que pour ce qui est des fournisseurs de services de télécommunications traditionnels lorsqu'ils appliquent, par exemple, un "routage domestique" pour la 5G.

---

46 Voir la recommandation nº 33.
47 Voir la recommandation nº 34.
48 Voir la recommandation nº 10.
49 Voir la recommandation nº 42.

Les experts ont longuement discuté de la question de l'**accès aux données relatives au contenu malgré le chiffrement**, et ils sont convenus qu'il est nécessaire que les services répressifs aient accès aux données en clair. Ils ont souligné que des solutions technologiques peuvent être mises en œuvre, lorsqu'elles existent, ou devraient être développées afin de préserver la vie privée et la protection des données, de garantir la cybersécurité et de permettre la mise en œuvre simultanée de mesures d'accès légal et ciblé, y compris aux données relatives au contenu. Les experts ont débattu de la nécessité d'une normalisation afin de répondre aux besoins fonctionnels des services répressifs, notamment en ce qui concerne de nouvelles normes de télécommunications telles que la 6G. Il convient d'élaborer, pour les technologies de communication actuelles et futures, des normes permettant un accès légal sans affaiblir les mécanismes de protection de la vie privée, de protection des données et de cybersécurité[50]. Cette approche, qui comprend l'évaluation et la certification de systèmes d'interception légale afin de garantir le respect effectif des exigences en matière de cybersécurité, de protection de la vie privée et d'accès légal, ouvre des perspectives à plus long terme et pour les technologies à venir telles que la 6G.

Les experts ont exprimé le souhait d'**examiner d'abord les aspects techniques**, en collaboration avec les experts en cybersécurité. Ils ont précisé qu'il était nécessaire de s'attaquer aux défis posés par le chiffrement (et l'interception en temps réel de manière générale) **dès la conception des technologies de communication**, notamment en **développant des projets associant des experts en technologie, en cybersécurité, en protection de la vie privée, en normalisation et en sécurité**. Ils ont insisté sur le fait que, pour s'acquitter de leurs tâches dans le monde numérique, les services répressifs doivent disposer d'un accès légal et préétabli à des données lisibles, conformément aux instruments internationaux tels que la convention de Budapest, et tout en préservant les exigences en matière de cybersécurité. À cette fin, le GHN a appelé l'UE à établir une feuille de route et à coordonner les travaux au moyen d'une structure permanente, éventuellement hébergée par le pôle d'innovation de l'UE pour la sécurité intérieure[51].

[50] Voir la recommandation nº 23.
[51] Voir la recommandation nº 22.

En lien avec ce qui précède, d'autres sujets de préoccupation comprenaient l'utilisation de services de communication enrichie (RCS) pour échanger des SMS chiffrés de bout en bout, l'augmentation de la communication 5G pour les clients itinérants entrants et les initiatives telles que le relais privé d'Apple. Ce type de technologies coupent l'accès des fournisseurs de services de télécommunications traditionnels aux informations les plus pertinentes, qui sont sinon accessibles en clair, ce qui a une incidence sur la capacité des services répressifs à accéder de manière effective et légale aux données en transit en temps réel. Les experts ont débattu de ces défis et souligné la nécessité de maintenir des capacités d'interception légale pour les opérateurs de télécommunications traditionnels malgré la 5G et la 6G et ont demandé que la coopération avec les fournisseurs de services soit facilitée au niveau de l'UE[52].

[52] Voir la recommandation nº 24.

Recommandations du groupe de haut niveau

En ce qui concerne les mesures de renforcement des capacités, le groupe de haut niveau recommande:

1. De cartographier et relier les **réseaux de criminalistique numérique existants** tout en améliorant l'accessibilité, en évitant les chevauchements et en encourageant le leadership. En ce qui concerne ce dernier point, il convient de mettre en place un secrétariat pour les réseaux, afin de simplifier la diffusion des connaissances parmi les experts; le secrétariat devrait réfléchir à des mécanismes visant à faire en sorte que les outils sensibles puissent être partagés dans le plein respect des règles nationales.

2. De réfléchir à des **mécanismes de mise en commun des connaissances**, afin de veiller à ce que les outils de criminalistique numérique puissent être partagés entre les États membres dans un environnement de confiance, tout en tenant compte des règles nationales. Il pourrait s'agir notamment d'étudier une approche européenne pour la gestion et la divulgation des vulnérabilités traitées par les services répressifs, sur la base des bonnes pratiques existantes.

3. La mise au point d'un mécanisme au niveau de l'UE pour **acheter conjointement des licences d'outils de criminalistique numérique**, afin de les partager entre les États membres.

4. D'augmenter **le financement pour la recherche et l'élaboration d'outils d'acquisition de données, d'accès aux données en clair y compris les capacités de déchiffrement, et des capacités fondées sur l'intelligence artificielle pour l'analyse de données** avec des objectifs clairs, et de promouvoir le répertoire d'outils d'Europol en tant que pôle central pour la diffusion de ces outils.

5. De créer un **mécanisme/système pour l'évaluation et, le cas échéant, pour la certification des outils commerciaux de criminalistique numérique** au niveau de l'UE, en tenant compte de toute incidence négative potentielle sur les procédures d'enquête et de poursuite (comme l'ajout de contraintes inutiles).

6. De mettre en place un processus consacré à l'**échange de capacités** pouvant impliquer l'utilisation de vulnérabilités, ce qui permettrait la mise en commun de connaissances et de ressources, tout en respectant la confidentialité et le caractère sensible des informations.

7. D'augmenter le nombre de **possibilités de formation** pour les experts et de créer un **système de certification au niveau de l'UE pour les experts en criminalistique numérique** (y compris ceux qui travaillent au déchiffrement), afin de garantir la qualité et l'uniformité des formations techniques offertes.

8. D'investir pour combler le déficit de compétences techniques en matière de normalisation et de sensibiliser davantage en établissant des **accords avec le monde universitaire** et d'autres institutions compétentes.

9. De mettre en place des **mécanismes (interopérabilité et cybersécurité) et des infrastructures (bande passante et scalabilité) compatibles avec le transfert en temps réel de grands ensembles de données**, tels que ceux collectés lorsque les autorités d'un État membre exécutent une demande d'accès légal au nom d'un autre État membre. Cela implique de poursuivre les travaux sur la normalisation des structures de données, sur les mécanismes de confiance et sur le filtrage des données, afin d'éviter la transmission de données non pertinentes pour l'enquête ou les enquêtes et de respecter les principes de protection des données que sont la limitation des finalités, la proportionnalité et la minimisation des données, ainsi que les travaux menés au niveau de l'UE sur la conception et le dimensionnement des moyens de transmission et les coûts y afférents.

10. De travailler de manière plus coordonnée et avec le soutien financier de l'UE à une **méthodologie pour élaborer, traiter et utiliser des mesures d'accès légal et ciblé** afin de répondre aux cas où l'accès aux données n'est pas possible via la coopération avec les services de communications électroniques. Compte tenu de son caractère sensible, une telle approche devrait être soumise à une autorisation judiciaire et assortie d'un cadre solide pour l'admissibilité des preuves. Ces cas devraient rester exceptionnels – c'est-à-dire que les services répressifs ne devraient recourir à ces outils que comme mesure de dernier recours – et faire obligatoirement l'objet d'évaluations de la proportionnalité.

En ce qui concerne la coopération avec l'industrie et la normalisation, le groupe de haut niveau recommande:

11. La création d'une **plateforme (équivalente à SIRIUS[53])** pour partager les outils, les bonnes pratiques et les connaissances sur la manière de se voir accorder l'accès aux données par les propriétaires de produits et les producteurs. En s'appuyant sur l'expérience de SIRIUS, il convient de l'étendre de manière à inclure les fabricants de matériel dans son mandat et de créer et cartographier les points de contact des services répressifs avec les fabricants de matériel et de logiciels numériques.

12. De favoriser la **coopération avec les producteurs et les développeurs d'outils de criminalistique numérique** afin de rationaliser la structure et le format des données obtenues par les services répressifs grâce à l'utilisation de ces outils, idéalement selon des normes convenues.

13. De continuer à financer, développer et **établir de façon permanente des structures UE** et des enceintes, y compris la plateforme SIRIUS, le RJE et/ou le RJEC aux fins de: a) développer les contacts entre les praticiens et les fournisseurs de services pour faciliter l'échange d'informations, le renforcement des capacités et la formation, b) nourrir un dialogue permanent, y compris dans le cadre d'une enceinte ou d'une autorité indépendante réunissant les praticiens (services répressifs, autorités judiciaires et fournisseurs de services), pour définir les principes et les modalités de coopération. Il pourrait s'agir notamment de créer ou de soutenir un **répertoire central d'outils et d'informations** permettant de partager la jurisprudence, les changements de législation et d'autres informations qui seraient d'utilité pour les États membres et les fournisseurs de services.

---

53 SIRIUS est un projet financé par l'UE qui facilite l'accès transfrontière aux preuves électroniques pour les services répressifs et les autorités judiciaires dans le cadre d'enquêtes et de procédures pénales. Mis en œuvre conjointement par Europol et Eurojust, en partenariat étroit avec le Réseau judiciaire européen, le projet SIRIUS est un point de référence central dans l'UE pour le partage des connaissances sur l'accès transfrontière aux preuves électroniques. Le projet SIRIUS aide les enquêteurs à faire face à la fois à la complexité et au volume des informations dans un environnement en ligne qui change rapidement. Le projet fournit des produits tels que des lignes directrices normalisées sur les processus de coopération entre les autorités compétentes et certains fournisseurs de services. Les autres services fournis par la plateforme SIRIUS comprennent des outils d'enquête et des coordonnées pour les fournisseurs de services, et SIRIUS facilite également les possibilités de partage d'expérience avec des pairs, tant en ligne qu'en présentiel.

14. L'adoption par les États membres de **protocoles d'accord** en tant que mécanisme efficace pour promouvoir la coopération et développer une compréhension commune entre les fournisseurs de services, les pouvoirs publics et les services répressifs afin de soutenir l'application des législations nationales, en utilisant les bonnes pratiques établies dans certains États membres.

15. La mise au point de formats de données suivant les **normes élaborées par l'Institut européen de normalisation des télécommunications (ETSI)** ou d'autres organismes de normalisation afin de favoriser l'interopérabilité et de faciliter l'exploitation par tous les États membres.

16. Le remplacement progressif des formats spécifiques utilisés par chaque fournisseur de services (et, en conséquence, par les autorités des États membres) par une approche horizontale, sur la base de normes élaborées par l'ETSI ou par d'autres organismes de normalisation pour le format des demandes et des réponses. *[La cohérence de la présente recommandation avec les règles établies par le règlement sur les preuves électroniques devrait faire l'objet d'une évaluation plus approfondie]*

17. **De favoriser les règles de transparence pour les fournisseurs de services de communications électroniques** en ce qui concerne les données qu'ils traitent, génèrent ou stockent (dans la mesure où elles ne coïncident pas toujours) dans le cadre de leurs activités, et sur l'information des services répressifs quant aux données disponibles, en tenant compte des limites posées par la confidentialité des enquêtes. Les experts suggèrent d'atteindre cet objectif par un accord de coopération avec les fournisseurs de services ou, si nécessaire, par la fixation d'obligations impératives. Une transparence accrue est également nécessaire dans la mise en œuvre des obligations légales en matière d'interception à des fins judiciaires, tant du côté des services de communications électroniques que de celui des autorités. Ces règles devraient aller de pair avec la notion de secret de l'enquête. Par exemple, dans toute enquête, il est impératif que les suspects ne soient pas notifiés pendant toute la durée de l'enquête.

18. De créer un centre d'échange pour identifier le ou les fournisseurs de services concernés et cibler les demandes licites qui leur sont adressées (par exemple, pour la portabilité du numéro pour les fournisseurs de télécommunications, comme c'est déjà le cas dans certains États membres de l'UE).

19. De mettre en place des mécanismes visant à faire en sorte que les demandes transfrontières ciblent les fournisseurs de services d'une manière qui soit efficace et évite les conflits potentiels, en s'inspirant des mécanismes établis pour les preuves électroniques. *[La cohérence de la présente recommandation avec les règles établies par le règlement sur les preuves électroniques devrait faire l'objet d'une évaluation plus approfondie]*

20. D'accompagner les futures initiatives de **mesures de normalisation** pertinentes. À cette fin, il est suggéré que la Commission présente une **feuille de route**, comprenant une perspective à long terme définissant des objectifs clairs, prévoyant un financement adéquat pour soutenir une participation accrue des experts des États membres et proposant un mécanisme de coordination, éventuellement par l'intermédiaire d'Europol et d'autres agences de l'UE. Il convient de veiller à ce que le champ d'application des activités de normalisation soit large et englobe l'internet des objets, y compris, par exemple, les voitures connectées ainsi que toute forme de connectivité dont, par exemple, les communications par satellite. Il convient que les activités ayant trait à la criminalistique numérique, à l'accès légal et à l'interception légale soient couvertes.

21. De s'inspirer, pour les futures initiatives législatives, pratiques et techniques, d'une définition commune des exigences, telle que définie dans le document **LEON** sur les besoins opérationnels des services répressifs en matière d'accès légal aux communications **(Law enforcement Operational Needs for Lawful Access to Communications[54])**. La mise en place d'un groupe ad hoc d'experts, éventuellement coordonné par Europol, apporterait une garantie de mise à jour de LEON si nécessaire, éventuellement sous la coordination du groupe de travail sur la normalisation pour la sécurité hébergé par Europol, qui devrait se poursuivre. Toute initiative devrait être technologiquement neutre. Différentes options peuvent être envisagées quant à la place de LEON dans les futures initiatives de l'UE: 1) une référence à LEON dans une proposition législative de l'UE, 2) une recommandation, 3) une source d'inspiration.

---

54 LEON est le résultat de travaux menés par les services répressifs suédois en étroite coopération avec les représentants des services répressifs d'États membres de l'UE, d'Amérique du Nord et d'Australie. L'objectif est de recenser et de décrire les besoins des services répressifs en matière d'accès licite aux contenus de communications, aux données relatives au contenu et aux informations relatives aux abonnés.

22. D'élaborer une feuille de route technologique qui rassemble des experts en matière de technologie, de cybersécurité, de respect de la vie privée, de normalisation et de sécurité et assure une coordination adéquate, par exemple dans le cadre d'une structure permanente, afin de mettre en œuvre un **accès légal par conception** à toutes les technologies pertinentes, conformément aux besoins exprimés par les services répressifs, tout en assurant une sécurité et une cybersécurité solides et en garantissant le plein respect des obligations légales en matière d'accès licite. Selon le GHN, les services répressifs devraient contribuer à la définition des exigences, mais leur rôle ne devrait pas être d'imposer des solutions particulières aux entreprises pour qu'elles puissent fournir un accès légal aux données à des fins d'enquête pénale sans compromettre la sécurité.

23. De veiller à ce que d'éventuelles nouvelles obligations, un nouvel instrument juridique et/ou des normes **n'entraînent pas, directement ou indirectement, d'obligations pour les fournisseurs d'affaiblir la sécurité des communications** en compromettant ou en affaiblissant de manière générale le chiffrement de bout en bout. Par conséquent, les éventuelles nouvelles règles en matière d'accès aux données devraient faire l'objet d'une évaluation prudente fondée sur des solutions technologiques de pointe (qui devraient à leur tour tenir compte des défis du chiffrement). Lorsqu'ils veillent à la possibilité d'un accès légal par conception prévu par la loi, les fabricants ou les fournisseurs de services devraient le faire de manière à ce qu'il n'ait pas d'incidence négative sur la posture de sécurité de leurs architectures matérielle ou logicielle.

24. De renforcer **la coordination et le soutien de l'UE** pour faire face aux situations dans lesquelles des solutions techniques pour permettre l'interception légale existent mais ne sont pas mises en œuvre par les fournisseurs de services de communications électroniques. Dans de tels cas, par exemple lorsque des accords de routage domestique ou la mise en œuvre spécifique d'un système de communication enrichie (RCS) ne permettent pas de disposer de capacités d'interception légale, des orientations claires et un dialogue facilité au niveau de l'UE amélioreraient la coopération avec les services de communications électroniques.

En ce qui concerne les mesures législatives, le groupe de haut niveau recommande:

25. De réaliser une **cartographie complète** de la législation en vigueur dans les États membres afin de préciser les responsabilités juridiques des fabricants de matériel numérique et de logiciels en ce qui concerne le respect des demandes de données émanant des services répressifs. Cette cartographie tiendrait aussi compte de scénarios et d'exigences spécifiques qui obligent les entreprises à accéder à des appareils, conformément également à la jurisprudence de la CJUE et à la jurisprudence de la Cour européenne des droits de l'homme. L'objectif devrait être d'élaborer un **manuel à l'échelle de l'UE** sur cette base et, en fonction de la cartographie susmentionnée, de promouvoir le rapprochement des législations dans ce domaine, ainsi que d'élaborer des normes sectorielles contraignantes pour les appareils mis sur le marché dans l'UE, afin d'intégrer l'accès légal.

26. De créer un **groupe de recherche chargé d'évaluer la faisabilité technique d'obligations en matière d'accès légal intégré** (y compris pour l'accès aux données chiffrées) en ce qui concerne les appareils numériques, tout en maintenant et sans compromettre la sécurité des appareils et la confidentialité des informations pour tous les utilisateurs, ainsi que sans affaiblir ou compromettre la sécurité des communications.

27. De mettre en place un **régime harmonisé au niveau de l'UE en matière de conservation des données**, qui présente les caractéristiques suivantes:

    i. être neutre sur le plan technologique et à l'épreuve du temps,

    ii. couvrir les "gestionnaires de données" actuels et futurs (c'est-à-dire les services par contournement et les fournisseurs de services de tout type qui pourraient donner accès à des preuves électroniques),

    iii. assurer l'accès à des données intelligibles (pour les métadonnées et les données relatives aux abonnés, le fournisseur de services devrait disposer d'un moyen permettant de déchiffrer les données si elles sont chiffrées à tout moment pendant la fourniture du service),

    iv. mettre l'accent non seulement sur la conservation des données, mais aussi sur l'accès aux données, en s'appuyant sur les règles relatives aux preuves électroniques,

    v. établir, à tout le moins, l'obligation pour les entreprises de conserver des données suffisantes pour que tout utilisateur puisse être clairement identifié (par exemple, adresse IP et numéro de port),

    vi. assurer le plein respect des règles en matière de protection des données et de la vie privée.

28. De **catégoriser** les données en fonction de leur finalité (identification, localisation, établissement de l'activité en ligne d'un sujet d'intérêt), bien que certains travaux soient nécessaires pour traduire les finalités en exigences techniques claires.

29. De **veiller à ce que l'accès aux données soit ciblé et différencié** en fonction des catégories de données ou de catégories spécifiques d'infractions (par exemple, les infractions qui ne se produisent que sur l'internet), ou en fonction de la menace pour les victimes.

30. D'**inclure des règles relatives à la responsabilité et à l'applicabilité** pour les fournisseurs de services afin de faire respecter les obligations de conservation et de fourniture de données, par exemple par la mise en œuvre de sanctions administratives ou de limites à l'exercice d'activités sur le marché de l'UE.

31. De **veiller à ce que les données des utilisateurs conservées à des fins commerciales et professionnelles** soient effectivement accessibles aux services répressifs, sous réserve des garanties applicables.

32. D'envisager de prévoir l'**obligation pour les fournisseurs de services** d'activer ou de désactiver certaines fonctions de leurs services afin d'obtenir certaines informations après avoir reçu un mandat (par exemple, le stockage de la géolocalisation d'un utilisateur spécifique après que celui-ci a été visé par une demande légale).

33. D'élaborer un mécanisme garantissant que les États membres peuvent **appliquer des sanctions** à l'encontre des **services de communications électroniques non coopératifs**[55] et que ces mesures ont un effet dissuasif à l'égard de ces entités. Des mesures tant administratives que pénales devraient être disponibles et appliquées selon qu'un fournisseur est simplement non coopératif ou qu'il héberge délibérément des activités à caractère criminel.

34. D'harmoniser au niveau de l'UE les mesures de droit pénal aux fins de la coopération, y compris en matière d'emprisonnement. Il devrait en aller de même pour les **fournisseurs d'hébergement non coopératifs** (en plus des services de communications électroniques) afin de veiller à ce que ces entreprises, lorsqu'elles hébergent des services de communications à caractère criminel, se conforment correctement aux ordonnances judiciaires qui leur sont adressées. *[La cohérence de la présente recommandation avec les règles établies par le règlement sur les services numériques devrait faire l'objet d'une évaluation plus approfondie]*

---

[55] Dans ce contexte, on entend par "**services de communications électroniques non coopératifs**" tout opérateur qui ne se conforme pas aux ordres légaux et aux demandes de nature technique adressés par les services répressifs et qui n'a aucune raison objective d'agir de la sorte.

35. Les initiatives potentielles devraient faire une distinction entre les fournisseurs de **services de communications électroniques criminels** (c'est-à-dire les plateformes spécifiquement conçues pour proposer des services exclusivement ou principalement à des acteurs criminels, tel qu'EncroChat) et les fournisseurs de **services de communications électroniques non coopératifs**, qui sont légalement établis et mènent des activités licites mais qui ne respectent pas pleinement les obligations nationales en matière d'interception légale.

36. D'établir une **obligation exécutoire pour les plateformes** (ou des mesures non contraignantes au moyen d'une coopération avec le secteur) de désigner un **PCU**[56] (**point de contact unique**) dans l'UE pour le traitement des demandes émanant des autorités de l'UE et des contacts avec celles-ci, en particulier pour les fournisseurs de services pour lesquels un contact d'urgence est nécessaire. Un mécanisme similaire (ou, idéalement, le même PCU, doté de prérogatives étendues) devrait également exister pour faciliter le **respect des obligations en matière d'interception légale**.

37. De soumettre les fournisseurs de services de communications électroniques (tels qu'ils sont définis dans le code des communications électroniques européen – CCEE[57]) aux mêmes règles que celles applicables aux fournisseurs de services traditionnels.

38. De poursuivre l'**harmonisation des cadres juridiques nationaux pour l'accès aux données en transit**[58] en plusieurs étapes:

    i. Veiller à ce que les obligations en matière d'interception légale prévues par les législations nationales soient **applicables à un plus large éventail de fournisseurs de services de communication**, y compris les catégories concernées de fournisseurs de services internet (et s'inspirer, à cet égard, du train de mesures relatif aux preuves électroniques).

    ii. Rechercher une harmonisation au niveau des États membres de l'UE sur la base de **principes communs arrêtés d'un commun accord** (notamment ceux qui font partie du document relatif aux besoins opérationnels des services répressifs) au moyen de dispositions non contraignantes (par exemple, une recommandation de la Commission).

---

56 L'initiative SIRIUS a créé en 2020 le réseau des points de contact SIRIUS avec une plateforme spécifique sur la plateforme d'experts Europol. Ce réseau est actuellement composé de 39 services répressifs de 22 pays de l'UE et de 2 pays tiers.

57 Article 2, point 4), de la directive (UE) 2018/1972.

58 La notion de données en transit peut couvrir les cas où l'acquisition de données n'est pas effectuée pendant le transit, mais lorsque les données de communication sont sur le point d'être envoyées ou ont été reçues (parfois définies comme des "données en direct").

iii. Réfléchir à une **définition de l'interception légale** dans le contexte large des services de communication par l'internet, en établissant en outre une distinction entre l'interception légale de données non relatives au contenu et l'interception légale de données relatives au contenu.

iv. Sur la base d'une analyse plus approfondie et d'une analyse d'impact, y compris sous l'angle des droits fondamentaux et en tenant compte de la souveraineté des États en matière pénale, proposer éventuellement une initiative de l'UE sur l'interception légale (consistant en des instruments non contraignants ou en des instruments juridiques), en s'inspirant des travaux réalisés dans le cadre des preuves électroniques et en travaillant sur des accords internationaux et bilatéraux (par exemple, avec les États-Unis). Une telle initiative devrait garantir que les principes de l'"accès légal dès la conception" sont correctement mis en œuvre par les parties prenantes concernées (par exemple, les fournisseurs de services de communications électroniques) afin de satisfaire aux exigences définies, notamment pour permettre l'accès aux données en clair lorsque cela est jugé nécessaire et proportionné.

39. D'ajuster le **concept de compétence territoriale en matière de données** afin de résoudre les conflits de lois potentiels avec d'autres juridictions. Dans les cas où le lien est national (par exemple, lorsqu'une infraction est commise dans un État membre par un criminel situé dans le même État membre), il devrait être possible de mettre en place une mesure d'interception dans le cadre du droit procédural national fixant des exigences et des garanties, sans avoir à passer par un instrument de coopération transfrontière.

40. D'étudier comment la **décision d'enquête européenne (DEE)** pourrait mieux soutenir l'efficacité des demandes transfrontières d'interception légale en améliorant la sécurité juridique, en raccourcissant les délais de réponse aux mandats et en favorisant une utilisation uniforme de la décision d'enquête européenne et de la convention de Budapest du Conseil de l'Europe sur la cybercriminalité dans toute l'Europe afin de combler les lacunes existantes en matière d'accès aux données.

41. De réfléchir aux **garanties nécessaires** lorsque l'interception légale s'applique aux fournisseurs de services de communications non traditionnels. Certains experts suggèrent que cette mesure d'enquête ne devrait concerner que les communications qui ont lieu après la réception d'une demande légale émanant des autorités. En outre, les mesures ne devraient pas entraîner d'obligation pour les fournisseurs d'adapter leurs systèmes informatiques d'une manière qui ait une incidence négative sur la cybersécurité de leurs utilisateurs.

42. D'adopter des règles minimales au niveau de l'UE permettant la recevabilité mutuelle entre les États membres des **preuves** obtenues au moyen de mesures d'interception légale à l'encontre de fournisseurs non coopératifs et prévoyant la recevabilité également en cas de recours à des mesures intrusives, dans la mesure nécessaire pour faciliter la reconnaissance mutuelle des jugements, les décisions judiciaires et la coopération policière et judiciaire en matière pénale.