Conseil de
l'Union européenne

Bruxelles, le 28 avril 2022
(OR. fr)

8179/22

LIMITE

CATS 22
JAI 489
COPEN 128
ENFOPOL 195
CYBER 122
TELECOM 151
DROIPEN 49
DATAPROTECT 103
EJUSTICE 41
MI 287
JAIEX 35

NOTE

Origine:	la présidence
Destinataire:	Comité de coordination dans le domaine de la coopération policière et judiciaire en matière pénale
Objet:	L'acces aux données dans le cadre des enquêtes pénales - Papier de discussion

En vue de la réunion 'CATS' du 5 mai 2022, les délégations trouveront en annexe un papier de discussion soumis par la Présidence.

ANNEXE

Document de discussion

L'accès aux données dans le cadre des enquêtes pénales

Dans leur déclaration commune du 24 mars 2016, à la suite des attentats terroristes perpétrés deux jours plus tôt à Bruxelles, les ministres de la justice et de l'intérieur des Etats membres de l'UE ainsi que les représentants d'institutions européennes avaient appelé à « *trouver, en priorité, des moyens de recueillir et d'obtenir plus rapidement et efficacement des preuves numériques, en intensifiant la coopération avec les pays tiers et les prestataires de services qui sont actifs sur le territoire européen, et permettre ainsi un meilleur respect de la législation de l'UE et des États membres et des contacts directs avec les services répressifs*[1] ».

Les 22 et 23 juin 2017, cet appel avait été repris par le Conseil européen qui avait affirmé que *« l'accès effectif aux preuves électroniques* ***[était]*** *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*[2] ».

En effet, l'accès aux données électroniques, au-delà même de la facilitation de la recherche de preuves à charge et à décharge, est rendu indispensable par l'évolution des technologies qui favorisent l'essor de nouvelles formes de criminalité en ligne, et offrent à la criminalité traditionnelle de nouveaux moyens et supports pour se développer, à une échelle et une rapidité inédites. Les enquêtes pénales ne peuvent désormais plus se concevoir sans l'intégration d'éléments de preuves sous forme électronique et par conséquent, sans l'accès aux données qui s'y rapportent. Les enquêteurs rencontrent plusieurs obstacles pour obtenir ces preuves, en particulier la volatilité des données, qui nécessite que ces données aient été conservées d'une façon ou d'une autre, et le fait que les services électroniques sont souvent prestés par des sociétés étrangères, ce qui requière, très souvent, de recourir à la coopération internationale.

---

1 Déclaration commune des ministres européens de la justice et de l'intérieur et des représentants des institutions de l'UE sur les attentats terroristes perpétrés le 22 mars 2016 à Bruxelles.

2 Conclusions du Conseil européen des 22 et 23 juin 2017.

C'est dans ce contexte que la Commission européenne a présenté, le 17 avril 2018, son paquet législatif relatif à l'accès à la preuve électronique. Après que le Conseil et le Parlement ont adopté leurs positions respectives, les trilogues sont en cours depuis plus de 16 mois et la Présidence est particulièrement engagée dans ces négociations qui répondent à un réel besoin opérationnel.

L'élaboration de mécanismes de coopération efficaces dans le domaine de la preuve électronique est indissociable des conditions permettant la conservation et l'accès à ce type de preuves.

Cette question fait depuis 2014 l'objet d'une jurisprudence nourrie de la Cour de justice de l'Union européenne.

En matière de conservation des données, la Cour a posé le principe de la prohibition de la conservation générale et indifférenciée des données de connexion à des fins de lutte contre la criminalité[3]. La Cour estime ainsi que, pour ce qui concerne la lutte contre la criminalité, la conservation des données ne peut être que ciblée (notamment sur la base de critères géographiques ou personnels), ou qu'elle doit se faire par le biais de la technique de la conservation rapide. Cette jurisprudence apparaît désormais bien établie dès lors qu'elle a été confirmée par l'arrêt du 5 avril 2022 (affaire C-140/20, G.D.).

La Cour a également encadré les possibilités d'accéder aux données conservées, en jugeant que cet accès doit être subordonné à une autorisation préalable donnée par une juridiction ou par une autorité administrative indépendante[4]. Elle précise à cet égard que l'exigence d'indépendance signifie que l'autorité en charge de ce contrôle préalable ne doit pas être impliquée dans la conduite de l'enquête pénale et doit avoir une position de neutralité à l'égard des parties à la procédure.

Ce cadre posé par la Cour de justice doit également être mis en perspective avec les nouveaux défis qui se poseront aux Etats membres, liés à l'évolution des technologies, notamment le chiffrement qui constitue un enjeu essentiel dans le contexte de l'accès aux données à des fins de lutte contre la criminalité.

---

3 CJUE, grande chambre, 21 décembre 2016, *Tele2 Sverige AB*, n° C-203/15 ; CJUE, grande chambre, 6 octobre 2020, *La Quadrature du Net e.a,.* n° C-511/18.

4 Cf. notamment CJUE, grande chambre, 2 mars 2021, *H.K., Prokuratuur*, n° C-746/18, confirmé par l'arrêt du 5 avril 2022.

Les délégués du CATS seront invités à répondre aux questions suivantes :

1. Quelle est la première analyse que vous faites de l'arrêt de la CJUE du 5 avril 2022 ? Identifiez-vous d'ores et déjà des conséquences particulières concernant vos législations nationales actuelles ou en cours d'élaboration ?

2. S'agissant de l'accès aux données conservées, la Cour de justice insiste particulièrement sur les exigences au stade de l'émission des demandes. A la lumière de ces arrêts, quelles garanties identifiez-vous comme particulièrement indispensables dans les situations d'accès aux preuves issues des communications électroniques ?