Conseil de
l'Union européenne

Bruxelles, le 24 novembre 2020
(OR. en)

13084/1/20
REV 1

LIMITE

JAI 999
COSI 216
CATS 90
ENFOPOL 314
COPEN 329
DATAPROTECT 131
CYBER 239
IXIM 122

NOTE

Origine:	la présidence
Destinataire:	délégations
Nº doc. préc.:	12863/20
Objet:	Résolution du Conseil sur le chiffrement - La sécurité grâce au chiffrement et malgré le chiffrement

Les délégations trouveront en annexe la résolution du Conseil sur le chiffrement.

ANNEXE

Résolution du Conseil sur le chiffrement
La sécurité grâce au chiffrement et malgré le chiffrement

1. Préambule: La sécurité grâce au chiffrement et malgré le chiffrement

L'Union européenne soutient pleinement le développement, la mise en œuvre et l'utilisation du chiffrement fort. Elle souligne la nécessité de garantir le plein respect des droits fondamentaux, des droits de l'homme et de l'état de droit dans toutes les actions liées à la présente résolution, en ligne et hors ligne. Le chiffrement est un moyen nécessaire pour protéger les droits fondamentaux et la sécurité numérique des pouvoirs publics, des entreprises et de la société. Dans le même temps, l'Union européenne doit veiller à ce que les autorités compétentes dans le domaine de la sécurité et de la justice pénale, par exemple les autorités répressives et judiciaires, puissent exercer leurs pouvoirs légaux, tant en ligne que hors ligne, pour protéger nos sociétés et nos citoyens.

Conformément aux conclusions du Conseil européen des 1er et 2 octobre 2020 (EUCO 13/20), l'UE *tirera parti de ses instruments et de ses pouvoirs de réglementation pour contribuer à la définition de règles et de normes mondiales*. Il a été convenu que les fonds au titre de la facilité pour la reprise et la résilience seraient utilisés pour atteindre des objectifs tels que *renforcer la capacité de l'UE à se protéger contre les cybermenaces, à assurer un environnement de communication sécurisé, notamment par le chiffrement quantique, et à garantir l'accès aux données à des fins judiciaires et répressives*.

2. Utilisation et situation actuelles du chiffrement

Dans le monde d'aujourd'hui, la technologie du chiffrement est de plus en plus utilisée dans tous les domaines de la vie publique et privée. Il s'agit d'un moyen de protéger les particuliers, la société civile, les infrastructures critiques, les médias et les journalistes ainsi que les entreprises et les pouvoirs publics en garantissant le caractère privé, la confidentialité, l'intégrité et la disponibilité des communications et des données à caractère personnel: il est évident que toutes les parties bénéficient de la technologie du chiffrement. Les autorités de l'UE chargées de la protection des données et de la cybersécurité ont établi que le chiffrement était un outil important qui contribue, par exemple, à la protection des données à caractère personnel transférées en dehors de l'UE, sous réserve que l'exigence d'un niveau de protection substantiellement équivalent soit respectée, ce qui, selon la Cour de justice, est une exigence légale pour les transferts de données[1]. Non seulement les appareils et applications électroniques sont de plus en plus programmés pour chiffrer par défaut les données stockées des utilisateurs, mais de plus en plus de canaux de communication et de services de stockage de données sont également sécurisés par le chiffrement de bout en bout (E2E). Cette évolution se manifeste de façon positive par une réaction de plus en plus déterminée de l'industrie de la communication et des applications, la plupart des applis de messagerie instantanée et autres plateformes en ligne ayant également mis en œuvre le chiffrement de bout en bout.

3. Défis à relever pour assurer la sécurité

La "vie numérique" et le cyberespace présentent non seulement de grandes opportunités, mais aussi des défis considérables: la numérisation des sociétés modernes amène avec elle certaines vulnérabilités et un potentiel d'exploitation à des fins criminelles. Ainsi, les criminels peuvent tirer parti, dans leurs modes opératoires, de solutions de chiffrement prêtes à l'emploi facilement accessibles et conçues à des fins légitimes[2].

Dans le même temps, les services répressifs sont de plus en plus tributaires de l'accès aux preuves électroniques pour lutter efficacement contre le terrorisme, la criminalité organisée, la pédopornographie (en particulier ses aspects en ligne) ainsi que toute une série d'autres formes de cybercriminalité et de criminalité facilitée par les technologies de l'information et de la communication. Pour les autorités compétentes, l'accès aux preuves électroniques peut s'avérer essentiel non seulement pour mener à bien des enquêtes et, ce faisant, traduire les criminels en justice, mais aussi pour protéger les victimes et contribuer à garantir la sécurité.

---

1 Arrêt du 16 juillet 2020 dans l'affaire C-311/18, Data Protection Commissioner/Facebook Ireland Ltd, Maximillian Schrems, ECLI:EU:C:2020:559.

2 iOCTA 2020, p. 25.

Toutefois, dans certains cas, le chiffrement rend extrêmement difficile ou pratiquement impossible l'accès au contenu des communications et son analyse aux fins de l'obtention des preuves électroniques, alors même que l'accès à ces données serait licite. Indépendamment de l'environnement technologique du moment, il est donc essentiel de préserver les pouvoirs des autorités compétentes dans le domaine de la sécurité et de la justice pénale grâce à un accès licite leur permettant d'accomplir les missions prescrites et autorisées par la loi. Ces lois prévoyant des pouvoirs d'exécution doivent toujours respecter pleinement le droit à un procès équitable et d'autres garanties, ainsi que les droits fondamentaux, en particulier le droit au respect de la vie privée et du caractère privé des communications ainsi que le droit à la protection des données à caractère personnel.

4. Trouver un juste équilibre

Le principe de la sécurité grâce au chiffrement et malgré le chiffrement doit être intégralement respecté. L'Union européenne continue de soutenir le chiffrement fort. Le chiffrement constitue un point d'ancrage pour assurer la confiance dans la numérisation et dans la protection des droits fondamentaux, et il convient de le promouvoir et de le développer.

Il est de la plus haute importance de protéger le caractère privé et la sécurité des communications grâce au chiffrement, tout en préservant la possibilité pour les autorités compétentes dans le domaine de la sécurité et de la justice pénale d'accéder légalement aux données pertinentes, à des fins légitimes et clairement définies, dans le cadre de la lutte contre la grande criminalité et/ou la criminalité organisée et le terrorisme, y compris dans la sphère numérique, et en sauvegardant l'état de droit. Toute mesure prise doit soigneusement respecter l'équilibre entre ces intérêts et les principes de nécessité, de proportionnalité et de subsidiarité.

5. Conjuguer nos forces avec celles du secteur des technologies

Pour aller de l'avant, l'Union européenne s'efforce d'engager une discussion active avec le secteur des technologies, tout en associant la recherche et le monde universitaire, afin de garantir la poursuite de la mise en œuvre et de l'utilisation de technologies de chiffrement fort. Les autorités compétentes doivent être en mesure d'accéder aux données de manière licite et ciblée, dans le plein respect des droits fondamentaux et des lois applicables en matière de protection des données, tout en préservant la cybersécurité. Les solutions techniques permettant d'accéder aux données chiffrées doivent respecter les principes de légalité, de transparence, de nécessité et de proportionnalité, y compris la protection des données à caractère personnel dès la conception et par défaut.

Comme il n'existe pas un moyen unique d'atteindre les objectifs fixés, les pouvoirs publics, les entreprises, les milieux de la recherche et le monde universitaire doivent collaborer de manière transparente afin de créer cet équilibre de façon stratégique.

6. Cadre réglementaire

Il pourrait être procédé à une évaluation plus approfondie de la nécessité de mettre en place, dans l'ensemble de l'UE, un cadre réglementaire qui permettrait aux autorités compétentes de s'acquitter efficacement de leurs tâches opérationnelles tout en protégeant la vie privée, les droits fondamentaux et la sécurité des communications.

Les solutions techniques potentielles devront permettre aux autorités d'exercer leurs pouvoirs d'enquête, qui sont soumis aux principes de proportionnalité et de nécessité ainsi qu'au contrôle juridictionnel en vertu de la législation nationale de ces autorités, tout en respectant les valeurs européennes communes, en protégeant les droits fondamentaux et en préservant les avantages du chiffrement. Les solutions possibles devraient être élaborées de manière transparente, en coopération avec les fournisseurs de services de communication nationaux et internationaux ainsi que d'autres parties prenantes. La conception de telles solutions et normes techniques, de même que l'évolution rapide des technologies d'une façon générale, nécessiterait en outre d'améliorer continuellement le savoir-faire et l'expertise techniques et opérationnels des autorités compétentes, afin qu'elles puissent relever efficacement les défis que pose la numérisation pour leur travail à l'échelle mondiale.

7. Capacités d'enquête innovantes

Enfin, il est de la plus haute importance d'améliorer la coordination au niveau de l'UE en vue:

1) de conjuguer les efforts de l'ensemble des États membres, institutions et organes de l'UE;

2) de concevoir et d'établir des approches innovantes tenant compte des technologies nouvelles;

3) d'analyser les solutions techniques et opérationnelles appropriées; et

4) de dispenser une formation sur mesure et de grande qualité.

Les solutions techniques et opérationnelles ancrées dans un cadre réglementaire fondé sur les principes de légalité, de nécessité et de proportionnalité devraient être conçues en étroite concertation avec les fournisseurs de services, d'autres parties prenantes et toutes les autorités compétentes concernées, même s'il conviendrait d'éviter que soit prescrite une solution technique unique pour donner accès aux données chiffrées.