

Bruxelles, le 8.12.2021
SWD(2021) 377 final

DOCUMENT DE TRAVAIL DES SERVICES DE LA COMMISSION

RÉSUMÉ DU RAPPORT D'ANALYSE D'IMPACT

accompagnant le document:

Proposition de directive du Parlement européen et du Conseil

**relative à l'échange d'informations entre les services répressifs des États membres,
abrogeant la décision-cadre 2006/960/JAI du Conseil**

{COM(2021) 782 final} - {SEC(2021) 420 final} - {SWD(2021) 374 final}

Résumé de l'analyse d'impact

Analyse d'impact relative à une proposition visant à moderniser la coopération existante en matière répressive au sein de l'UE par la création d'un code de coopération policière de l'UE sur l'échange et la communication d'informations

A. Nécessité d'une action

Pourquoi? Quel est le problème à résoudre?

La sécurité et la criminalité transfrontière (y compris les infractions fiscales) constituent, par définition, une question internationale. Ainsi qu'il est mentionné dans la stratégie de l'UE pour l'union de la sécurité publiée en 2020, l'Europe est confrontée à un **paysage sécuritaire en proie à des changements permanents**, dans lequel les menaces pour la sécurité évoluent et se complexifient. Ces menaces s'étendent au-delà des frontières et se manifestent sous la forme d'organisations criminelles qui se livrent à des activités criminelles très variées. Même une infraction apparemment locale est susceptible de présenter des liens avec d'autres infractions commises à travers l'Europe par les mêmes auteurs. Qui plus est, la **mobilité intraeuropéenne grandissante** est source de défis supplémentaires pour ce qui est de prévenir et de combattre toutes les formes de menaces criminelles.

L'**évolution rapide du paysage de la criminalité et la mobilité accrue des personnes** tendent à indiquer que la coopération transfrontalière entre les services répressifs dans l'UE sera essentielle pour lutter contre les infractions pénales et permettre aux citoyens de l'UE de jouir en toute sécurité de leurs droits à la libre circulation à l'avenir.

Toutefois, l'échange de données entre services répressifs continue de se heurter aux frontières et à des obstacles, ce qui crée des angles morts et des failles exploités par de nombreux criminels et terroristes qui agissent dans plusieurs États membres. Étant donné que la lutte contre la criminalité et le renforcement de la sécurité revêtent un caractère transfrontière, les États membres doivent compter les uns sur les autres pour combler le déficit d'information.

Les services répressifs dans l'UE coopèrent et échangent des informations, notamment sur le fondement de la décision-cadre 2006/960/JAI relative à la simplification de l'échange d'informations et de renseignements entre les services répressifs des États membres de l'UE (décision-cadre suédoise ou DCS), mais il existe d'importantes lacunes.

Les services répressifs **ne sont pas en mesure d'échanger des informations de manière efficace et efficiente** avec leurs partenaires des autres États membres en raison de **trois problèmes d'ordre juridique, structurel et technique**:

- 1) **les règles appliquées au niveau national entravent la circulation efficace et efficiente des informations.** En effet, la décision-cadre suédoise de 2006 n'est pas entièrement mise en œuvre, ce qui empêche les services répressifs des autres États membres de recevoir ces informations de manière efficace et efficiente;
- 2) **les structures à l'échelle nationale ne sont pas toujours organisées et équipées d'une manière suffisamment efficace et efficiente.** En effet, les États membres ne disposent pas toujours des structures nécessaires pour recevoir les demandes d'informations émanant d'autres États membres, les transmettre aux autorités compétentes au niveau national et communiquer, en conséquence, les informations demandées;
- 3) **le libre choix du canal ou des canaux de communication entre États membres entraîne une duplication récurrente des demandes.** En effet, les services répressifs des États membres utilisent de nombreux canaux différents pour adresser leurs demandes d'informations à d'autres États membres et répondre aux demandes de ceux-ci, ce qui nuit à l'efficacité et à l'efficience de l'échange d'informations.

Ces trois problèmes sont imbriqués. Ils imposent des choix stratégiques importants, nécessitant une analyse approfondie des causes, des objectifs s'y rapportant, des options d'action possibles et de leur incidence.

Quels objectifs cette initiative devrait-elle atteindre?

Cette initiative devrait fondamentalement aider les États membres à respecter leur engagement en faveur de la coopération en matière répressive. Elle répond à des besoins opérationnels urgents et aux invitations du Conseil

à envisager de «consolider le cadre juridique de l'UE afin de renforcer encore la coopération transfrontière en matière répressive, de soutenir la mise en place d'un échange d'informations fluide et rapide et la poursuite du développement des structures et plateformes pertinentes».

L'initiative vise à atteindre les **objectifs** suivants:

- 1) **objectif I**: faciliter l'**accès équivalent des services répressifs** aux informations détenues dans un autre État membre (selon des modalités semblables à celles régissant l'accès aux informations au sein de cet État membre), dans le respect concomitant des droits fondamentaux et des exigences en matière de protection des données;
- 2) **objectif II**: veiller à ce que tous les États membres aient un **point de contact unique** (PCU) qui fonctionne efficacement, y compris lorsqu'une **autorisation judiciaire** est requise pour la transmission des données à la demande d'un autre État membre, et garantir sa coopération efficace avec les **centres de coopération policière et douanière** (CCPD);
- 3) **objectif III**: instaurer un **canal de communication par défaut obligatoire** pour l'échange d'informations en matière répressive entre les États membres (s'il y a lieu).

Quelle est la valeur ajoutée d'une action à l'échelle de l'Union?

Une action de l'UE devrait procurer des avantages à l'ensemble de l'UE et avoir des retombées positives sur les pays associés à l'espace Schengen, en renforçant la sécurité et la confiance générales entre les États membres. Ce faisant, elle devrait soutenir le principe fondamental de Schengen (un espace sans contrôles aux frontières intérieures).

Des **règles ainsi que des normes et exigences minimales** communes **au niveau de l'UE** amélioreront nettement la circulation des informations, dans le respect des normes de **haut niveau en matière de sécurité des données** et de **protection des données**.

Des normes communes permettront, en outre, un certain degré d'automatisation dans l'organisation des tâches liées à l'échange d'informations, libérant ainsi les agents des services répressifs de certaines tâches manuelles à forte intensité de main-d'œuvre/chronophages.

B. Les solutions

Quelles sont les options législatives et non législatives envisagées? Y a-t-il une option privilégiée? Pourquoi?

Plusieurs options législatives ont été envisagées. À la suite d'une présélection, certaines d'entre elles ont été rapidement écartées. Les autres **options d'action ont été analysées dans le détail**:

- 1) Option d'action relative à l'**objectif I**: («faciliter l'accès équivalent aux informations»)
 - **option d'action 1.1**: proposition législative mettant à jour la décision-cadre suédoise de 2006 (DCS) afin qu'elle soit mise en conformité avec la directive de 2016 en matière de protection des données dans le domaine répressif + mesures d'accompagnement non contraignantes (formation et orientations de la Commission);
 - **option d'action 1.2**: option 1.1 + simplifier l'application de la décision-cadre suédoise + clarifier les ensembles de données nationaux mis à disposition à des fins d'échange éventuel;
 - **option d'action 1.3**: option 1.2 + des dispositions garantissant le respect des délais dans lesquels des données doivent être mises à la disposition d'un autre État membre (y compris lorsqu'une autorisation judiciaire est exigée).
- 2) Options d'action répondant à l'**objectif II**: [«veiller à ce que tous les États membres aient un point de contact unique (PCU) qui fonctionne efficacement, y compris lorsqu'une autorisation judiciaire est requise pour la transmission des données à la demande d'un autre État membre, et garantir sa coopération efficace avec les centres de coopération policière et douanière (CCPD)»]
 - **option d'action 2.1**: continuer avec les lignes directrices non contraignantes du Conseil concernant un point de contact unique + mesures d'accompagnement non contraignantes (formation, soutien financier et orientations);
 - **option d'action 2.2**: *rapprochement des normes minimales* concernant la composition des points de contact uniques (dont la présence obligatoire d'une autorité judiciaire), leurs fonctions, leurs

ressources en personnel et leurs systèmes informatiques, ainsi que leur coopération avec des structures régionales telles que les centres de coopération policière et douanière + mesures d'accompagnement non contraignantes (formation, soutien financier et orientations);

- option d'action 2.3: *harmonisation* des règles régissant la composition des points de contact uniques (dont la présence obligatoire d'une autorité judiciaire), leurs fonctions, leurs ressources en personnel et leurs systèmes informatiques, ainsi que leur coopération avec des structures régionales telles que les centres de coopération policière et douanière + mesures d'accompagnement non contraignantes (formation, soutien financier et orientations).

3) Options d'action répondant à l'**objectif III**: *«instaurer un canal de communication par défaut obligatoire pour l'échange d'informations en matière répressive entre les États membres (s'il y a lieu)»*

- option d'action 3.1: continuer avec les lignes directrices et recommandations non contraignantes du Conseil de mettre Europol en copie lorsque l'application SIENA¹ est utilisée, dans les cas relevant du mandat d'Europol + mesures d'accompagnement non contraignantes (formation et soutien financier);
- option d'action 3.2: obligation d'utiliser le même canal de communication pour la même finalité (faire de l'application SIENA d'Europol le canal privilégié, s'il y a lieu) + obligation de mettre Europol en copie lorsque l'application SIENA est utilisée dans les cas relevant du mandat d'Europol + mesures d'accompagnement non contraignantes (comme celles mentionnées dans l'option 3.1);
- option d'action 3.3: obligation d'utiliser par défaut l'application SIENA pour tous les échanges d'informations bilatéraux (sauf disposition contraire du droit de l'UE) + obligation de mettre Europol en copie dans les cas relevant du mandat de cette agence, au terme d'une période de transition et moyennant le soutien du Fonds pour la sécurité intérieure en faveur du déploiement de l'application SIENA + mesures d'accompagnement (comme celles mentionnées dans l'option d'action 3.1).

À la suite d'une analyse détaillée des incidences des principales options d'action, l'**ensemble des options privilégiées** se compose des **options d'action 1.3, 2.2 et 3.3**.

Qui soutient quelle option?

Les parties prenantes sont généralement favorables à la mise en place d'un échange d'informations fluide et rapide et à la poursuite du développement des structures et plateformes pertinentes.

Les États membres devraient soutenir la plupart des mesures envisagées dans le cadre de l'option privilégiée. Dans le même temps, ils sont conscients de l'importance de leur souveraineté nationale dans le domaine de l'action répressive, d'un point de vue opérationnel et procédural. Des avis favorables exprimés au niveau des experts sont susceptibles de ne plus être partagés au niveau politique.

Le principal point de discussion probable concerne l'option 3.3 [faire de l'application SIENA d'Europol le canal de communication obligatoire entre les États membres (sauf disposition contraire du droit de l'Union)]. Cette option a pourtant été défendue par des États membres au Conseil: *«Faire de l'application SIENA le canal de communication par défaut contribuerait à la rationalisation de l'échange d'informations en matière répressive et accroîtrait le niveau de sécurité dans le cadre de la coopération policière dans l'Union. De même, cela permettrait de concentrer les efforts sur la mise au point d'une solution unique plutôt que de solutions multiples, ce qui favoriserait l'objectif consistant à renforcer la sécurité intérieure de l'UE.»*

Le Parlement européen devrait vérifier l'existence de garanties solides en matière de protection des données. Les discussions menées avec toutes les parties prenantes ont, en effet, montré l'importance que revêtaient des garanties appropriées pour assurer le respect des droits fondamentaux, et notamment du droit à la protection des données à caractère personnel.

C. Incidences de l'option privilégiée

Quels sont les avantages des options privilégiées (ou, à défaut, des options principales)?

L'option d'action privilégiée, qui changerait la donne, permettrait de résoudre efficacement les problèmes recensés tout en renforçant le soutien apporté par Europol aux États membres, l'objectif final étant de **prévenir ou de détecter les infractions pénales et d'enquêter en la matière**, dans le strict **respect des droits**

¹«Application de réseau d'échange sécurisé d'informations» d'Europol.

fondamentaux.

Les **bénéficiaires ultimes de l'option privilégiée sont les citoyens**. Ces derniers profiteront directement et indirectement d'une amélioration de la lutte contre la criminalité et d'une diminution des taux de criminalité. Sur le plan de l'efficacité, les **principaux bénéficiaires sont les services répressifs nationaux**.

Quels sont les coûts des options privilégiées (le cas échéant, sinon des options principales)?

L'option d'action privilégiée nécessite des investissements tant au niveau de l'UE qu'au niveau des États membres. Ces coûts concerneraient essentiellement les mises à niveau informatiques et les formations correspondantes. Ils varieraient très fortement d'un État membre à l'autre en fonction de l'efficacité et de l'efficacité de leur point de contact unique national et de leur(s) centre(s) de coopération policière et douanière (s'il en existe).

L'option d'action privilégiée apporte des solutions efficaces aux problèmes, solutions qui, autrement, seraient plus onéreuses, peu compatibles ou moins efficaces.

Il est toutefois difficile de chiffrer certaines des options d'action. D'après les données d'Europol, le coût lié à l'intégration de l'application SIENA d'Europol dans les systèmes de gestion des dossiers respectifs (SGD) de 20 États membres et au développement d'un SGD dans 10 États membres est estimé à 2,5 millions d'EUR (investissement unique nécessaire). Les gains d'efficacité compenseraient ce coût (moins de ressources nécessaires à la gestion des dossiers, c'est-à-dire davantage de ressources consacrées à la «résolution d'affaires»).

L'option d'action privilégiée ne prévoit pas d'obligations réglementaires pour les citoyens/les consommateurs et ne génère donc pas non plus de coûts supplémentaires pour ces parties prenantes.

Quelle sera l'incidence sur les entreprises, les PME et les microentreprises?

L'option d'action privilégiée pourrait avoir une légère incidence positive sur les petites et moyennes entreprises, étant donné l'augmentation de la demande de produits et services informatiques.

Y aura-t-il une incidence notable sur les budgets nationaux et les administrations nationales?

Comme indiqué ci-dessus, l'option d'action privilégiée nécessite des investissements au niveau des États membres. Ces coûts concerneraient essentiellement les mises à niveau informatiques et les formations correspondantes. Il est toutefois difficile de chiffrer certaines des options d'action. Ces coûts varieraient très fortement d'un État membre à l'autre en fonction de l'efficacité et de l'efficacité de leur point de contact unique national et de leur(s) centre(s) de coopération policière et douanière (s'il en existe).

D'après les données d'Europol, le coût du développement d'un système de gestion des dossiers au niveau national pourrait s'élever à 150 000 EUR (dépense non récurrente) par État membre. Les gains d'efficacité compenseraient ce coût (moins de ressources nécessaires à la gestion des dossiers, c'est-à-dire davantage de ressources consacrées à la «résolution d'affaires»).

Les mises à niveau informatiques devant être effectuées tant dans les PCU que dans les CCPD pourraient atteindre un total général maximal de **11,5 millions** d'EUR (2,5 millions d'EUR pour les PCU + 9 millions d'EUR pour les CCPD).

Ces coûts (investissement unique), jugés acceptables, sont **proportionnés** au problème constaté et ne vont pas au-delà de ce qui est nécessaire pour réaliser l'objectif spécifique. Le Fonds européen pour la sécurité intérieure apportera un soutien (essentiellement par l'intermédiaire des programmes nationaux).

Y aura-t-il d'autres incidences notables?

L'option privilégiée donne plus de moyens d'action aux pôles d'information nationaux et régionaux des États membres en vue d'un accès aux données existantes et d'un partage de celles-ci plus efficaces et plus efficaces.

Elle garantit également la pleine conformité d'une nouvelle directive sur l'échange et la communication d'informations avec la directive en matière de protection des données dans le domaine répressif de 2016. Cette conformité garantit le respect explicite des droits fondamentaux, ce qui n'est actuellement pas le cas de la décision-cadre suédoise de 2006.

L'option d'action privilégiée répond à un **objectif d'intérêt général** et se limite strictement à ce qui est **nécessaire et proportionné** pour l'atteindre.

D. Suivi

Quand la législation sera-t-elle réexaminée?

[Deux] ans après l'expiration du délai de transposition, et tous les [quatre] ans par la suite, la Commission devrait présenter deux rapports au Parlement européen et au Conseil. **Le premier** devant déterminer dans quelle mesure les États membres auront pris les dispositions nécessaires pour se conformer à cette directive; **le second** devant évaluer ses résultats par rapport à ses objectifs, déterminer si les principes de base restent valables et tirer toutes les conséquences pour les options futures.