COMMISSION
EUROPÉENNE

Bruxelles, le 8.12.2021
COM(2021) 782 final

2021/0411 (COD)

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

{SEC(2021) 420 final} - {SWD(2021) 374 final} - {SWD(2021) 377 final}

EXPOSÉ DES MOTIFS

1. CONTEXTE DE LA PROPOSITION

• Contexte général

Comme indiqué dans la stratégie de l'UE pour l'union de la sécurité[1], dans le nouveau programme de lutte antiterroriste pour l'UE[2] et dans la stratégie de l'UE visant à lutter contre la criminalité organisée (2021-2025)[3], les menaces transnationales nécessitent une réponse coordonnée, plus ciblée et mieux adaptée. Si les autorités nationales opérant sur le terrain sont en première ligne dans la lutte contre la criminalité organisée et le terrorisme, une action au niveau de l'Union et des partenariats mondiaux sont essentiels pour assurer une coopération efficace ainsi que l'échange d'informations et de connaissances entre les autorités nationales, en s'appuyant sur un cadre commun de droit pénal et sur des moyens financiers efficaces. Par ailleurs, la criminalité organisée et le terrorisme sont emblématiques du lien existant entre sécurité intérieure et sécurité extérieure. Ces menaces s'étendent au-delà des frontières et se manifestent sous la forme d'organisations criminelles et de groupes terroristes qui se livrent à un large éventail d'activités criminelles.

Dans un espace sans contrôles aux frontières intérieures (ci-après l'«espace Schengen»[4]), les agents de police d'un État membre devraient bénéficier d'un accès équivalent aux informations dont disposent leurs homologues d'un autre État membre (dans les mêmes conditions). Ils devraient coopérer efficacement et, par défaut, dans toute l'Union. Par conséquent, l'échange d'informations en matière pénale est un élément essentiel pour garantir la sécurité dans l'espace Schengen.

Parallèlement à la suppression des contrôles aux frontières intérieures de l'espace Schengen, un ensemble de règles relatives à l'échange d'informations et à la coopération policière a été convenu dans la convention d'application de l'accord de Schengen (CAAS). En outre, le système d'information Schengen (SIS) a été mis en place, donnant lieu à la création d'une base de données commune de l'Union sur la sécurité et les frontières contenant des informations sur les personnes et les objets recherchés et disparus sous la forme de signalements.

Il ressort de l'évaluation 2021 de la menace que représente la grande criminalité organisée dans l'Union (SOCTA UE) que plus de 70 % des organisations criminelles sont présentes dans plus de trois États membres[5]. La SOCTA UE de 2021 et le rapport européen sur les drogues de l'OEDT[6] de la même année recensent les domaines dans lesquels la grande criminalité organisée semble en augmentation. Dans le même temps, comme l'indique le

---

1 COM(2020) 605 final.
2 COM(2020) 795 final.
3 COM(2021) 170 final.
4 L'espace Schengen se compose des pays suivants: l'Allemagne, l'Autriche, la Belgique, le Danemark, l'Espagne, l'Estonie, la Finlande, la France, la Grèce, la Hongrie, l'Islande, l'Italie, la Lettonie, le Liechtenstein, la Lituanie, le Luxembourg, Malte, la Norvège, les Pays-Bas, la Pologne, le Portugal, la Slovaquie, la Slovénie, la Suède, la Suisse et la République tchèque.
5 Europol (2021), *European Union Serious and Organised Crime Threat Assessment* (Évaluation de la menace que représente la grande criminalité organisée dans l'Union européenne - SOCTA UE).
6 Observatoire européen des drogues et des toxicomanies (OEDT), *European drug report 2021* (Rapport européen sur les drogues 2021).

programme de lutte antiterroriste de décembre 2020[7], le niveau d'alerte terroriste demeure élevé dans l'Union.

L'espace Schengen est le plus grand espace de libre circulation au monde. Il permet à plus de 420 millions de personnes de se déplacer librement et aux marchandises et services de circuler sans entrave. Grâce à la suppression des contrôles aux frontières entre les États membres, l'espace Schengen fait désormais partie de notre mode de vie européen. C'est un symbole de l'interconnexion de l'Europe et des liens tissés entre les citoyens européens[8]. L'espace Schengen contribue également au fonctionnement efficace du marché unique et, partant, à la croissance de l'économie de l'Union[9].

La mobilité croissante des personnes au sein de l'Union pose toutefois des difficultés supplémentaires, qu'il s'agisse de prévenir les menaces criminelles et de lutter contre celles-ci ou de garantir la sécurité publique. Les régions frontalières intérieures de l'Union voient transiter près de 2 millions de navetteurs, dont 1,3 million de travailleurs frontaliers[10]. Bien que la pandémie de COVID-19 ait réduit la mobilité à l'intérieur de l'Union, les flux de personnes resteront probablement importants à l'avenir.

Ces dernières années, l'espace Schengen a été mis à l'épreuve à plusieurs reprises par une série de crises et de difficultés qui ont conduit à la réintroduction des contrôles aux frontières intérieures dans plusieurs États membres. Les mouvements secondaires incontrôlés[11] de migrants en situation irrégulière ont été l'une des raisons invoquées par les États membres pour justifier une telle décision. Ces derniers estiment que ces mouvements constituent une menace sérieuse pour l'ordre public ou la sécurité intérieure, et justifient dès lors la nécessité de réintroduire les contrôles aux frontières. Conformément au règlement (UE) 2016/399[12] («code frontières Schengen»), la réintroduction temporaire des contrôles aux frontières ne peut être utilisée que pour une période limitée, dans des circonstances exceptionnelles (telles que la crise migratoire observée en 2015-2016), à titre de mesure de dernier recours. En particulier, des améliorations peuvent être apportées en ce qui concerne l'usage des contrôles de police et la coopération policière, y compris, bien entendu, en matière d'échange d'informations et de communication. Ces mesures, en particulier si elles sont combinées, peuvent donner les mêmes résultats en matière de contrôle des mouvements secondaires que les contrôles temporaires aux frontières intérieures, tout en étant moins intrusives en ce qui concerne la libre circulation des personnes, des marchandises et des services.

L'évolution rapide du paysage de la criminalité et la mobilité des personnes tendent à indiquer que la coopération transfrontalière entre les services répressifs dans l'Union et l'espace Schengen est essentielle pour lutter contre les infractions pénales et permettre aux citoyens de l'Union et aux ressortissants de pays tiers séjournant légalement sur le territoire de l'Union d'exercer en toute sécurité leur droit à la libre circulation. D'importants défis subsistent toutefois quant à la capacité des services répressifs à échanger des informations avec leurs homologues des autres États membres de manière efficace et efficiente. Cette capacité varie encore considérablement d'un État membre à l'autre, ce qui révèle un degré de fragmentation préjudiciable à un échange d'informations efficace et efficient. Par conséquent,

---

7 COM(2020) 795 final.

8 Eurobaromètre 474: *L'espace Schengen*.

9 COM(2021) 277 final du 2.6.2021.

10 Commission européenne (2017), *Stimuler la croissance et la cohésion des régions frontalières de l'Union européenne*.

11 Parmi les autres raisons les plus fréquemment invoquées par les États membres figurent la crise migratoire de 2015-2016, la menace terroriste persistante et la pandémie de COVID-19.

12 Règlement (UE) 2016/399 (code frontières Schengen).

les criminels et les organisations criminelles continuent de profiter de ces failles pour opérer par-delà les frontières, et les mouvements secondaires de migrants en situation irrégulière continueront de poser problème.

• Justification et objectifs de la proposition

L'objectif général de la présente proposition est de légiférer sur les aspects organisationnels et procéduraux de l'échange d'informations entre les services répressifs dans l'Union en vue de contribuer à l'échange efficace et efficient de ces informations, et de protéger ainsi un espace Schengen pleinement opérationnel et résilient. La proposition est (notamment) sans préjudice des règles régissant l'échange d'informations sur les signalements dans le SIS par l'intermédiaire des bureaux SIRENE (supplément d'information requis à l'entrée nationale).

La présente proposition de *directive relative à l'échange d'informations entre les services répressifs des États membres* fait partie d'un ensemble cohérent de propositions comprenant également une proposition de recommandation du Conseil visant à renforcer la coopération policière opérationnelle transfrontalière, une proposition de règlement portant révision du mécanisme d'échange automatisé de données dans le cadre de la coopération policière («Prüm II») ainsi qu'une proposition portant modification du code frontières Schengen telle que présentée dans la communication de la Commission de juin 2021 intitulée «*Une stratégie pour un espace Schengen pleinement opérationnel et résilient*»[13]. Cet ensemble de propositions vise à établir un code de coopération policière dans le but de rationaliser, de renforcer, de développer, de moderniser et de faciliter la coopération en matière répressive entre les agences nationales compétentes, apportant ainsi un soutien aux États membres dans leur lutte contre la grande criminalité organisée et le terrorisme.

Tenant pleinement compte de l'avis exprimé par le colégislateur, la présente proposition se fonde sur les conclusions présentées dans l'analyse d'impact qui l'accompagne. Ces conclusions couvrent également les informations, les analyses et les recommandations découlant des évaluations Schengen dans le domaine de la coopération policière réalisées au cours des six dernières années, de la communication de la Commission sur la marche à suivre en ce qui concerne la mise en conformité de l'acquis de l'ancien troisième pilier avec les règles en matière de protection des données[14], des consultations approfondies menées avec les parties prenantes concernées au cours des deux dernières années et de l'important corpus de documents d'orientation du Conseil élaboré au cours des quinze dernières années. Sur la base de cette analyse combinée, trois objectifs principaux ont été établis. La présente proposition vise à les réaliser en s'attaquant à trois problèmes sous-jacents.

(1) Absence de règles communes claires et solides sur l'échange d'informations

Le premier objectif de la présente proposition est de garantir, au moyen de règles précises, cohérentes et communes, **un accès équivalent des services répressifs de tout État membre aux informations disponibles dans d'autres États membres** afin de prévenir et de détecter les infractions pénales, ainsi que de mener des enquêtes pénales ou des opérations de lutte contre la criminalité, **dans le respect des droits fondamentaux, y compris des exigences en matière de protection des données**.

Les services répressifs des États membres participent quotidiennement à des échanges transfrontières d'informations dans le cadre d'opérations de lutte contre les infractions pénales. **Les règles appliquées au niveau national entravent toutefois la circulation efficace et efficiente des informations**. Les règles générales relatives à l'échange

[13] COM(2021) 277 final du 2.6.2021.
[14] COM(2020) 262 final du 24.6.2020.

d'informations en matière répressive présentant un intérêt transfrontière entre les services répressifs des États membres sont définies dans la décision-cadre 2006/960/JAI du Conseil relative à la simplification de l'échange d'informations et de renseignements entre les services répressifs des États membres de l'Union européenne (ci-après la «décision-cadre suédoise» ou la «DCS»[15]), adoptée en 2006 avant l'entrée en vigueur du traité de Lisbonne. La décision-cadre suédoise a remplacé en partie le chapitre sur la coopération policière de la convention d'application de l'accord de Schengen de 1990[16].

Elle établit les **principes** selon lesquels les informations devraient être partagées (principes de disponibilité et d'accès équivalent), le **délai** dans lequel une demande d'informations devrait recevoir une réponse, les **formulaires** qui devraient être utilisés pour introduire ces demandes et y répondre, ainsi que les **garanties** en matière de protection des données à prévoir lors du traitement de ces informations.

Dans la pratique, la décision-cadre suédoise de 2006 manque toutefois de clarté, ce qui empêche la pleine mise en œuvre des principes de disponibilité/d'accès équivalent applicables aux informations pertinentes dans un contexte transfrontière[17]. En conséquence, les règles appliquées au niveau national continuent d'entraver la circulation des informations malgré les efforts déployés pour compléter les exigences de la décision-cadre suédoise par des orientations non contraignantes du Conseil[18]. Par conséquent, les incertitudes actuelles demeureraient et continueraient de nuire à l'échange efficace et efficient d'informations, sans que les incidences sur l'évolution de la situation en matière de sécurité dans l'Union et sur l'augmentation de la mobilité transfrontière ne soient véritablement prises en compte.

C'est pourquoi l'établissement à ces fins d'un cadre juridique par la voie d'une directive permettra un meilleur contrôle et une meilleure application des règles au niveau de l'Union et des États membres, tout en garantissant une convergence des pratiques nationales, améliorant ainsi l'efficacité et l'efficience des flux d'informations entre les États membres.

(2) Absence de structures communes et d'outils de gestion efficaces pour l'échange d'informations

Le deuxième objectif de la présente proposition de directive est de rapprocher les normes minimales communes en vue de garantir un fonctionnement efficace et efficient des points de contact uniques. Ces exigences minimales communes portent sur la composition, les structures, les responsabilités, les ressources en personnel et les capacités techniques.

Les États membres sont responsables du maintien de l'ordre public et de la sauvegarde de la sécurité intérieure[19]. Ils sont en principe libres d'organiser leurs autorités et services répressifs comme ils l'entendent. En ce qui concerne les structures de coopération en matière répressive, tous les États membres ont mis en place ou sont en train de mettre en place un point de

15 JO L 386 du 29.12.2006, p. 89.

16 JO L 239 du 22.9.2000, p. 19.

17 Ces questions en suspens ont notamment été mises en exergue dans les évaluations Schengen dans le domaine de la coopération policière. Ces évaluations par pays soulignent l'existence de pratiques divergentes selon l'autre État partie. Elles couvrent également les documents d'orientation pertinents du Conseil et le chapitre sur la coopération policière de la convention d'application de l'accord de Schengen de 1990 et les accords bi/multilatéraux connexes.

18 Par exemple: document 5825/20 du Conseil du 2 décembre 2020, *Manuel sur l'échange d'informations en matière répressive*.

19 Article 72 du TFUE.

contact unique[20] compétent pour canaliser un maximum d'échanges d'informations. Sur la base du droit national ou des règles internes, les services répressifs peuvent également échanger des informations directement entre eux. Bien que différents manuels et fiches d'information nationales aient été produits afin de faciliter une approche harmonisée de l'organisation des points de contact uniques nationaux, il subsiste des différences importantes entre les États membres en ce qui concerne leurs structures, leurs fonctions, leurs moyens et leurs capacités.

En conséquence, **les États membres ne disposent pas toujours des structures nécessaires pour échanger des informations de manière efficace et efficiente avec les autres États membres**. Les points de contact uniques nationaux ne jouent pas toujours leur rôle de coordination et peuvent manquer de ressources pour répondre au nombre croissant de demandes.

En particulier, ils ne sont pas toujours dotés des outils nécessaires de gestion des informations (par exemple, un système de gestion des dossiers pourvu d'un tableau de bord commun et d'un système automatique de téléchargement et de recoupement des données). En outre, les **points de contact uniques ne disposent pas toujours d'un accès direct et convivial à toutes les bases de données** et plateformes **pertinentes de l'Union et internationales**. De plus, certains points de contact uniques ont un accès limité aux **bases de données nationales pertinentes**, ce qui retarde encore le processus global d'échange d'informations. Les points de contact uniques peuvent également manquer de ressources pour traiter rapidement et efficacement le nombre croissant de demandes reçues. En effet, cette tendance à la hausse ne s'est pas toujours accompagnée d'une augmentation proportionnelle des ressources humaines et informatiques.

Une architecture moderne de gestion des informations, déjà utilisée dans certains points de contact uniques «avancés», peut atténuer les tensions sur des ressources humaines limitées grâce à l'intégration des informations détenues par les autorités compétentes dans leurs bases de données respectives, ce qui permet également de contrôler et de suivre le délai de réponse aux demandes d'informations[21]. Les bases de données mises à la disposition des points de contact uniques ne sont pas toujours pleinement utilisées, en raison d'**outils de recherche rudimentaires** qui empêchent l'adoption de techniques de translittération[22] et de fonctions de recherche à «logique floue»[23]. L'absence de techniques de translittération et d'options de recherche à logique floue dans les systèmes d'information empêche les agents d'obtenir des résultats (réponses positives) exhaustifs au moyen d'une requête unique. En conséquence, les agents doivent effectuer une nouvelle recherche pour chaque renseignement à caractère personnel sur lequel ils enquêtent, ce qui entraîne une augmentation de la charge de travail et ralentit le processus de recherche (par exemple, inversion du prénom et du nom, orthographe différente utilisée pour une même personne, notamment en raison de langues, d'alphabets et d'accents diacritiques différents).

---

20 Le point de contact unique est le pôle d'information national qui centralise la réception, le traitement et l'envoi des informations aux autres pays. Il regroupe sous une même structure de gestion tous les principaux canaux de communication des services répressifs internationaux et de l'Union (INTERPOL, Europol et SIRENE).

21 Voir l'analyse d'impact qui accompagne la présente proposition.

22 La translittération désigne le processus de représentation des mots/noms d'une langue à l'aide de l'alphabet ou du système d'écriture d'une autre langue (reconnaissance multilingue des noms). Par exemple, la lettre «o» peut être «ò», «ó», «ô», «õ», «ö» ou «ø» selon la langue/l'alphabet utilisé(e).

23 Une base de données floue désigne une base de données capable de traiter des informations incertaines ou incomplètes en recourant à la logique floue, c'est-à-dire la capacité de trouver des correspondances même lorsque le nom d'une personne est mal orthographié.

Actuellement, les délais sont presque toujours dépassés lorsqu'une autorisation judiciaire est requise. La **disponibilité fonctionnelle d'une autorité judiciaire**, comme c'est déjà le cas dans les points de contact uniques plus efficaces et efficients, contribuera à réduire les retards injustifiés. En effet, les demandes qui requièrent une autorisation judiciaire peuvent être traitées plus rapidement qu'elles le sont actuellement, ce qui signifie que les délais peuvent être plus facilement respectés également dans ces cas.

(3) Absence de pratique commune dans l'utilisation du ou des canaux de communication existants pour échanger des informations au sein de l'Union

Le **troisième objectif** de la présente proposition de directive est de **remédier à la prolifération des canaux de communication utilisés pour l'échange d'informations en matière répressive entre les États membres, tout en renforçant le rôle d'Europol en tant que pôle d'information sur la criminalité de l'Union pour les infractions relevant de son mandat.**

Outre un certain nombre de cas spécifiques au système régis par le droit de l'Union (par exemple, les demandes d'informations supplémentaires liées à des signalements SIS doivent être faites par l'intermédiaire des bureaux SIRENE[24], et l'échange d'informations avec Europol se fait généralement par l'intermédiaire des UNE[25]), les États membres n'ont pas convenu d'un canal unique d'échange d'informations entre leurs services répressifs pour les affaires ayant une dimension européenne, ce qui se traduit par une duplication des demandes, des retards injustifiés et parfois des pertes d'informations.

En conséquence, les États membres utilisent des canaux différents à des degrés divers pour demander, envoyer et recevoir des informations, souvent sans justification claire et prédéfinie[26], ce qui entrave l'échange efficace et efficient d'informations. Les autorités nationales se voient également privées du soutien d'Europol, alors même que les États membres demandent à l'agence d'être un pôle d'information de l'Union sur la criminalité, capable de fournir des informations de qualité.

Les points de contact uniques n'assurent pas toujours en permanence le suivi des canaux existants, ce qui peut avoir une incidence négative sur les affaires transfrontières nécessitant un partage d'informations urgent. Dans le même temps, l'application de réseau d'échange sécurisé d'informations (ci-après «SIENA») est sous-utilisée en dépit de ses caractéristiques adaptées et de sa solide infrastructure de sécurité des données. Même lorsque les États membres utilisent l'application SIENA, ils **ne font pas toujours intervenir Europol (en le mettant en copie)**, même si les informations échangées relèvent de son mandat. Il peut en résulter des lacunes importantes en matière d'information au niveau de l'Union.

- **Cohérence avec les dispositions existantes dans le domaine d'action**

La présente proposition est cohérente avec les dispositions existantes et à venir dans le domaine de la coopération en matière répressive. La coopération en matière répressive est un domaine de compétence partagée entre l'Union et les États membres. Au cours des dernières

[24] L'échange d'informations supplémentaires liées aux signalements SIS doit se faire par l'intermédiaire d'un réseau unique de bureaux nationaux appelés «bureaux SIRENE».

[25] Unités nationales Europol. L'échange d'informations avec Europol doit se faire par l'intermédiaire des UNE au moyen de l'application SIENA.

[26] Un certain nombre de points de contact uniques nationaux suivent des lignes directrices internes qui recommandent ou exigent l'utilisation spécifique d'un canal de communication dans un but précis, garantissant ainsi la cohérence et évitant la duplication des demandes. D'autres points de contact uniques nationaux se fient toutefois aux habitudes et aux préférences des agents, une telle marge de manœuvre entraînant des inefficacités dans un contexte d'enquête transfrontière.

années, des progrès ont été réalisés en vue d'améliorer la coopération en matière d'échange d'informations entre les États membres et de restreindre le périmètre d'action des terroristes et des grands criminels. Le cadre législatif relatif à la lutte contre le terrorisme et à l'échange d'informations a été renforcé au lendemain des attentats terroristes perpétrés en Europe. À la suite de la crise migratoire de 2015, l'architecture générale des systèmes d'information et des bases de données dans le domaine de la justice et des affaires intérieures (JAI) a fait l'objet d'une refonte, l'accent ayant été mis sur l'interopérabilité[27] et la convergence dynamique entre la sécurité, les frontières et la gestion des flux migratoires. En outre, une plus grande coopération entre les services répressifs a été encouragée au niveau de l'Union par la publication de recommandations et de lignes directrices (non contraignantes) du Conseil visant à faciliter la convergence des pratiques nationales.

Étant donné que les deux volets de la coopération en matière répressive concernent essentiellement i) l'échange d'informations (qui fait l'objet de la présente proposition) et ii) la coopération opérationnelle transfrontalière, la présente proposition s'inscrira dans un ensemble cohérent dont fait également partie la proposition de recommandation du Conseil portant sur des aspects de la coopération policière opérationnelle transfrontalière Cet ensemble est complété par la proposition parallèle de règlement portant révision du mécanisme d'échange automatisé de données dans le cadre de la coopération policière («Prüm II»). La proposition «Prüm II» visera à renforcer l'architecture technique d'échange Prüm, à élargir le champ des catégories de données ainsi qu'à rationaliser et à accélérer l'échange de données en cas de réponse positive. La proposition renforcée «Prüm II» prévoirait des règles et des possibilités spécifiques pour l'échange **automatisé** de catégories précises – et particulièrement importantes – de données (par exemple, les empreintes digitales, l'ADN et les images faciales dans le cadre global et des règles générales pour l'échange d'informations d'ordre général que cette directive prévoira.

En tant que mesure importante pour renforcer la sécurité au sein de l'Union, la présente proposition contribuera également à rendre l'espace Schengen pleinement opérationnel et résilient, comme énoncé dans la stratégie Schengen. Cette proposition est également en parfaite cohérence avec la proposition de 2020 portant révision du mandat d'Europol[28] en vue de renforcer le mandat de l'agence en matière de traitement d'ensembles de données vastes et complexes, ainsi qu'avec les injonctions européennes de production et de conservation de preuves électroniques en matière pénale[29]. Elle complète le cadre juridique[30] relatif à

---

27 Règlement (UE) 2019/817 du Parlement européen et du Conseil du 20 mai 2019 portant établissement d'un cadre pour l'interopérabilité des systèmes d'information de l'UE dans le domaine des frontières et des visas et modifiant les règlements (CE) nº 767/2008, (UE) 2016/399, (UE) 2017/2226, (UE) 2018/1240, (UE) 2018/1726 et (UE) 2018/1861 du Parlement européen et du Conseil et les décisions 2004/512/CE et 2008/633/JAI du Conseil (JO L 135 du 22.5.2019, p. 27). Règlement (UE) 2019/818 du Parlement européen et du Conseil du 20 mai 2019 portant établissement d'un cadre pour l'interopérabilité des systèmes d'information de l'UE dans le domaine de la coopération policière et judiciaire, de l'asile et de l'immigration et modifiant les règlements (UE) 2018/1726, (UE) 2018/1862 et (UE) 2019/816 (JO L 135 du 22.5.2019, p. 85).

28 COM(2020) 796 final.

29 COM(2018) 225 final – 2018/0108 (COD).

30 JO L 312 du 7.12.2018, p. 1. Règlement (UE) 2018/1860 relatif à l'utilisation du système d'information Schengen aux fins du retour des ressortissants de pays tiers en séjour irrégulier; règlement (UE) 2018/1861 sur l'établissement, le fonctionnement et l'utilisation du système d'information Schengen (SIS) dans le domaine des vérifications aux frontières, modifiant la convention d'application de l'accord de Schengen et modifiant et abrogeant le règlement (CE) nº 1987/2006; règlement (UE) 2018/1862 sur l'établissement, le fonctionnement et l'utilisation du système d'information Schengen (SIS) dans le domaine de la coopération policière et de la coopération judiciaire en matière pénale, modifiant et abrogeant la décision 2007/533/JAI du Conseil, et abrogeant

l'échange d'informations sur les signalements dans le SIS par l'intermédiaire des bureaux SIRENE. La présente proposition est sans préjudice de tous ces autres actes du droit de l'Union, ainsi que d'autres actes tels que la directive (UE) 2019/1153 du 20 juin 2019 fixant les règles facilitant l'utilisation d'informations financières et d'une autre nature aux fins de la prévention ou de la détection de certaines infractions pénales, ou des enquêtes ou des poursuites en la matière, et abrogeant la décision 2000/642/JAI du Conseil dans le but de faciliter l'accès aux informations financières et aux informations relatives aux comptes bancaires et leur utilisation par les autorités chargées de la prévention ou de la détection d'infractions pénales, ou des enquêtes ou des poursuites en la matière[31].

- **Cohérence avec les autres politiques de l'Union**

La présente proposition vise à contribuer de manière positive à un espace Schengen pleinement opérationnel et résilient, permettant la libre circulation d'un plus grand nombre de personnes et la circulation sans entrave des marchandises et des services. Le fonctionnement du marché unique gagnera en efficacité et, partant, la croissance de l'économie de l'Union en sera renforcée. La présente proposition est donc pleinement cohérente avec les autres politiques de l'Union en matière d'emploi, de transports et, en définitive, de croissance économique dans les régions frontalières au sein de l'Union, mais aussi dans l'ensemble de l'Union.

2. BASE JURIDIQUE, SUBSIDIARITÉ ET PROPORTIONNALITÉ

- **Base juridique**

La base juridique de l'action de l'Union dans le domaine de la coopération en matière répressive au sein de l'Union est le titre V, chapitre 5, du traité sur le fonctionnement de l'Union européenne (TFUE). Aux termes de l'article 87 du TFUE: «*L'Union développe une coopération policière qui associe toutes les autorités compétentes des États membres, y compris les services de police, les services des douanes et autres services répressifs spécialisés dans les domaines de la prévention ou de la détection des infractions pénales et des enquêtes en la matière*». Plus précisément, l'article 87, paragraphe 2, point a), du TFUE porte sur les mesures relatives à la collecte, au stockage, au traitement, à l'analyse et à l'échange d'informations pertinentes aux fins de la prévention ou de la détection des infractions pénales et des enquêtes en la matière. La présente proposition législative doit être adoptée selon la procédure législative ordinaire.

- **Subsidiarité (en cas de compétence non exclusive)**

Une action au niveau de l'Union est nécessaire pour remédier comme il se doit aux problèmes recensés dans la première section du présent exposé des motifs. L'objectif d'améliorer les flux d'informations entre les services répressifs compétents et avec Europol ne peut être atteint de manière suffisante par les États membres agissant seuls. En raison du caractère transnational de la criminalité et du terrorisme, les États membres sont interdépendants. Par conséquent, l'établissement de règles communes pour l'échange d'informations peut être mieux réalisé au niveau de l'Union. Malgré l'existence d'un certain nombre de mesures nationales et régionales, les États membres ne seraient pas à même d'assurer à eux seuls la pleine application des principes de disponibilité des informations et d'accès équivalent aux informations. S'ils agissaient séparément et sur la base de régimes nationaux, les États membres ne parviendraient pas à surmonter les différences actuelles entre les points de

le règlement (CE) nº 1986/2006 du Parlement européen et du Conseil et la décision 2010/261/UE de la Commission, tel que modifié.

31 JO L 186 du 11.7.2019, p. 122.

contact uniques, qui entravent l'échange efficace et efficient d'informations pertinentes par-delà les frontières. Ils ne garantiraient pas un niveau approprié et uniforme de connaissances et de capacités dans l'utilisation des bases de données et des canaux de communication pertinents.

L'Union est mieux à même que les États membres séparément de garantir la cohérence des mesures prises au niveau national, de remédier aux divergences de pratiques, de prévenir les doubles emplois, les chevauchements et les incertitudes et, finalement, de faciliter une lutte efficace contre la criminalité transfrontière et le terrorisme. L'action de l'Union en réaction aux problèmes recensés devrait apporter une valeur ajoutée à l'ensemble de l'Union et, partant, à ses citoyens, car elle permettra de renforcer la résilience et la solidité de l'espace Schengen, avec un effet de ricochet sur les pays associés à l'espace Schengen[32]. Des règles, normes et exigences communes au niveau de l'Union facilitant l'échange d'informations sur la criminalité transfrontière entre les services répressifs permettront de réaliser d'importantes économies d'échelle et de garantir des normes de haut niveau en matière de sécurité et de protection des données.

La coopération en matière répressive au niveau de l'Union ne remplace pas les politiques nationales en matière de sécurité intérieure. Elle ne se substitue pas à l'action des services répressifs nationaux. En revanche, l'action menée au niveau de l'Union soutient et renforce les politiques de sécurité nationales et l'action des services répressifs nationaux contre la criminalité transfrontière et le terrorisme.

- **Proportionnalité**

La présente proposition vise à consolider le cadre juridique de l'Union dans un instrument juridique unique sur l'échange d'informations par la «lisbonnisation» de la décision-cadre suédoise. Elle contient également des dispositions découlant d'un ensemble de lignes directrices non contraignantes du Conseil adoptées au cours des quinze dernières années. Compte tenu de la demande du colégislateur et de la volonté exprimée par les États membres au cours de la phase de consultation, la présente proposition de directive aborde les problèmes recensés sans aller au-delà de ce qui est strictement nécessaire à la réalisation de l'objectif consistant à garantir des flux d'informations efficaces et efficients entre les États membres.

- **Choix de l'instrument**

S'appuyant sur les précédentes conclusions pertinentes du Conseil[33], la présente proposition de directive de la Commission vise à mettre en place des flux d'informations efficaces et efficients entre les services répressifs des États membres, grâce à un rapprochement substantiel des législations des États membres en matière d'échange et de communication d'informations. Ses dispositions garantissent le respect de l'attribution des compétences ainsi que des différences entre les systèmes et traditions juridiques des États membres, telles que reconnues par les traités. Compte tenu de ce qui précède, la présente proposition législative prend la forme d'une directive.

3. RÉSULTATS DES ÉVALUATIONS EX POST, DES CONSULTATIONS DES PARTIES INTÉRESSÉES ET DES ANALYSES D'IMPACT

- **Consultation des parties intéressées**

Menée auprès des **parties intéressées** d'un large éventail de domaines, des autorités policières, douanières, judiciaires et de protection des données des États membres, des

[32] L'Islande, le Liechtenstein, la Norvège et la Suisse.

[33] Conclusions du Conseil sur la sécurité intérieure et le partenariat européen de police, 13083/1/20.

organisations de la société civile, des universités et des membres du public, la consultation a porté sur leurs attentes et leurs préoccupations concernant le renforcement de la coopération en matière répressive dans l'Union[34].

La Commission a utilisé différents **moyens de dialogue**, tels que des questionnaires ciblés, des entretiens avec des experts, des groupes de discussion, des études de cas, et a organisé des ateliers thématiques avec des représentants des États membres et des pays associés à l'espace Schengen. Les questions et les options présentées dans l'analyse d'impact qui accompagne la présente proposition ont également été examinées au sein des groupes concernés du Conseil [par exemple, le groupe «Application de la loi» - sous-groupes «Police» et «Douanes», et le comité permanent de coopération opérationnelle en matière de sécurité intérieure].

En outre, conformément aux lignes directrices pour une meilleure réglementation[35], la Commission a lancé une **consultation publique**. Les **résultats des activités de consultation** (20 réponses) ont été dûment pris en considération lors de l'élaboration de la présente proposition[36].

- **Obtention et utilisation d'expertise**

De nombreuses activités de consultation, telles que des entretiens de cadrage, des questionnaires et des enquêtes en ligne, des entretiens semi-structurés, des études de cas et des groupes de discussion, ont également été menées par le contractant lors de la réalisation d'une étude intitulée «*Study to support the preparation of an impact assessment on EU policy initiatives facilitating cross-border law enforcement cooperation*» (étude visant à soutenir l'élaboration d'une analyse d'impact relative à des initiatives stratégiques de l'UE facilitant la coopération transfrontalière en matière répressive).

- **Analyse d'impact**

Conformément aux lignes directrices pour une meilleure réglementation, une analyse d'impact a été réalisée en vue de l'élaboration de la présente proposition législative. Sur la base de ses conclusions, la Commission a relevé trois problèmes majeurs qui correspondent aux trois principaux objectifs spécifiques de la présente proposition (tels que mentionnés ci-dessus). En conséquence, trois options caractérisées par différents degrés d'intervention ont été envisagées aux fins de la réalisation de chacun des objectifs spécifiques[37].

Objectif spécifique 1: *faciliter un accès équivalent des services répressifs aux informations détenues dans un autre État membre, tout en respectant les droits fondamentaux, y compris les exigences en matière de protection des données.*

Mesures:

(1) garantir la mise en conformité des dispositions actuellement contenues dans la DCS de 2006 avec la directive en matière de protection des données dans le domaine répressif de 2016;

---

34 Une présentation exhaustive des consultations des parties intéressées figure dans l'analyse d'impact qui accompagne la présente proposition.

35 SWD(2017) 350 final du 7.7.2017.

36 Code de coopération policière de l'UE – Lutte contre la grande criminalité organisée transfrontière (europa.eu)

37 Voir l'analyse d'impact qui accompagne la présente proposition.

(2) élaborer une série de nouvelles mesures d'accompagnement non contraignantes, telles que des formations et des orientations de la Commission sur des aspects spécifiques de l'échange d'informations entre les services répressifs, selon le cas;

(3) améliorer la clarté des dispositions de la DCS, grâce à une clarification du champ d'application de la DCS et à une simplification de son application. Des orientations de la Commission sur les ensembles de données nationaux disponibles dans chaque État membre en vue d'un éventuel échange peuvent également être élaborées afin d'améliorer encore la mise en œuvre, le cas échéant;

(4) faciliter le respect des délais dans lesquels les informations doivent être mises à la disposition d'un autre État membre, y compris lorsqu'une autorisation judiciaire est requise.

Objectif spécifique 2: *veiller à ce que tous les États membres disposent d'un point de contact unique efficace, y compris lorsqu'une autorisation judiciaire est requise pour fournir des informations à la demande d'un autre État membre.*

Mesures:

(1) élaborer une nouvelle série de mesures d'accompagnement non contraignantes, telles que des formations, un soutien financier et des orientations pertinentes de la Commission, selon le cas;

(2) établir des exigences communes minimales concernant la composition des points de contact uniques (y compris lorsqu'une autorisation judiciaire est requise), leurs fonctions, leurs ressources en personnel et leurs capacités.

Objectif spécifique 3: *remédier à la prolifération des canaux de communication utilisés pour l'échange d'informations en matière répressive entre les États membres, tout en renforçant le rôle d'Europol en tant que pôle d'information sur la criminalité de l'Union pour les infractions relevant de son mandat.*

Mesures:

(1) élaborer une nouvelle série de mesures d'accompagnement non contraignantes, telles que des formations, un soutien financier et des orientations de la Commission sur le partage d'informations, selon le cas;

(2) exiger des États membres qu'ils utilisent l'application SIENA pour tous les échanges d'informations bi/multilatéraux au titre de la directive proposée, après une période de transition nécessaire pour garantir le déploiement complet de cette application.

Ces mesures permettront **de rationaliser, de clarifier, de développer et de moderniser la coopération transfrontalière entre les services répressifs, tout en protégeant mieux les droits fondamentaux**, notamment en ce qui concerne la protection des données à caractère personnel (comme expliqué ci-dessous). Elles permettront également de renforcer le soutien apporté par Europol aux États membres pour faire face à l'évolution des menaces. L'option privilégiée permettra de garantir une forte convergence des pratiques nationales concernant le fonctionnement efficace et efficient du point de contact unique, grâce à des normes minimales communes.

Les effets les plus positifs de l'option privilégiée devraient résulter de l'établissement du point de contact unique en tant que «guichet unique» pour la coopération en matière répressive dans l'ensemble des États membres. Faire de l'application SIENA d'Europol le canal de communication par défaut contribuera à la rationalisation de l'échange d'informations entre les services répressifs, tout en garantissant la convergence des informations au sein d'Europol

et la sécurité de ces informations (et des données à caractère personnel). L'option privilégiée prévoit également des mesures d'accompagnement telles que des formations et un soutien financier, qui sont des éléments essentiels pour la réalisation des objectifs spécifiques présentés ci-dessus. L'option privilégiée donne les meilleurs effets cumulatifs en ce qui concerne la pertinence, la valeur ajoutée, l'efficacité, l'efficience, la cohérence et la proportionnalité. Tout en tirant les enseignements du passé, elle est suffisamment ambitieuse. L'option privilégiée tient dûment compte des avis exprimés par les États membres et répond aux attentes légitimes des citoyens et des entreprises de l'Union. Ce faisant, l'option privilégiée contribue au fonctionnement efficace et efficient de l'espace Schengen.

- **Droits fondamentaux**

L'analyse d'impact qui accompagne la présente proposition a permis d'analyser les effets que chaque option, y compris les mesures envisagées par la présente proposition de directive, pourrait avoir sur les droits fondamentaux des citoyens. Par définition, toute option portant sur le partage d'informations entre les services répressifs a une incidence sur le droit à la protection des données à caractère personnel, tel que prévu par l'article 8 de la charte des droits fondamentaux de l'Union européenne (ci-après la «charte») et l'article 16 du traité sur le fonctionnement de l'Union européenne.

Les options sont également susceptibles d'avoir une incidence sur d'autres droits fondamentaux, tels que ceux protégés par l'article 2 (droit à la vie), l'article 3 (droit à l'intégrité de la personne), l'article 6 (droit à la liberté et à la sûreté), l'article 17 (droit de propriété) et l'article 45 (liberté de circulation et de séjour) de la charte. Il ressort de l'analyse d'impact que les options retenues sont proportionnées puisqu'elles se limitent à ce qui est strictement nécessaire pour atteindre l'objectif de sauvegarde de la sécurité intérieure dans l'espace Schengen tout en protégeant la libre circulation des personnes[38].

En outre, la mise en conformité des règles applicables aux échanges d'informations à des fins répressives avec les règles applicables et adoptées ultérieurement en matière de traitement des données à caractère personnel à des fins répressives (conformément à la directive en matière de protection des données dans le domaine répressif de 2016; ci-après la «DPDR»[39]) devrait avoir une incidence positive sur la protection des droits fondamentaux des citoyens. L'utilisation de l'application SIENA en tant que canal de communication permettra également de renforcer la sécurité des systèmes de traitement des données à caractère personnel et leur protection globale contre d'éventuels abus. Étant donné que la DPDR prévoit et garantit le niveau requis de protection des données à caractère personnel dans l'Union, il n'est pas nécessaire d'aller au-delà de ce qu'elle prévoit. En revanche, la mise en conformité garantira une cohérence totale avec les règles de l'Union en matière de protection des données à caractère personnel, y compris celles contenues dans la DPDR. De cette manière, il est donné effet à l'engagement de la Commission, inscrit dans une communication de 2020, de présenter *«une proposition législative qui, au minimum, comprendra une modification de la décision-cadre 2006/960/JAI du Conseil afin de garantir l'alignement nécessaire en matière de protection des données, au cours du dernier trimestre de 2021»*[40].

---

38 Voir l'analyse d'impact qui accompagne la présente proposition.

39 Directive (UE) 2016/680 (JO L 119 du 4.5.2016, p. 89).

40 COM(2020) 262 final, *Marche à suivre en ce qui concerne la mise en conformité de l'acquis de l'ancien troisième pilier avec les règles en matière de protection des données*.

4. INCIDENCE BUDGÉTAIRE

Bien qu'elle dépende fortement des spécificités de chaque configuration informatique nationale et des paramètres juridiques, une estimation des coûts possibles a été fournie par Europol et présentée dans l'analyse d'impact qui accompagne la présente proposition. Les mises à niveau informatiques nécessaires tant dans les points de contact uniques que dans les centres de coopération policière et douanière[41] ont été estimées à un montant **total** maximal **unique** de **11,5 millions d'EUR**. Ces coûts devraient se répartir comme suit:

– 1,5 million d'EUR pour mettre en place des systèmes de gestion des dossiers (SGD) dans 10 États membres (non encore équipés);

– 1 million d'EUR pour intégrer l'application SIENA dans les SGD des points de contact uniques de 20 États membres (non encore équipés);

– 2,25 millions d'EUR pour établir une connexion à l'application SIENA dans un maximum de 45 centres de coopération policière et douanière (14 sur 59 étant déjà connectés);

– 6,75 millions d'EUR pour mettre en place des SGD dans un maximum de 45 centres de coopération policière et douanière (45 x 150 000 EUR).

Ces coûts (investissement unique) sont jugés acceptables et **proportionnés** au problème constaté et ne vont pas au-delà de ce qui est nécessaire pour réaliser les objectifs spécifiques fixés par la présente proposition de directive. Il convient de noter que les États membres poursuivent en tout état de cause la modernisation de leurs systèmes informatiques (également dans le contexte de l'interopérabilité des systèmes d'information de l'Union). Cette modernisation leur permet ainsi de mettre en œuvre de manière rentable les changements envisagés par la présente proposition. Ces estimations ne couvrent pas les besoins en formation car, en particulier pour les mises à niveau informatiques, les coûts de formation dépendent fortement des spécificités de chaque configuration informatique nationale et des paramètres juridiques.

En tout état de cause, les coûts au niveau national devraient être couverts par les programmes des États membres au titre du Fonds pour la sécurité intérieure[42]. Le Fonds pour la sécurité intérieure prévoit les objectifs spécifiques suivants: *«améliorer et faciliter l'échange d'informations*» et «*améliorer et intensifier la coopération transfrontière*»[43]. Par conséquent, lors de l'élaboration de leurs programmes nationaux, les États membres sont invités à prévoir des activités qui revêtent un intérêt particulier pour la mise en œuvre de la directive envisagée, en faisant explicitement référence aux points de contact uniques et aux centres de coopération policière et douanière, ainsi qu'à la connexion à l'application SIENA. Certains États membres étant plus avancés que d'autres quant à leur niveau de coopération, le coût de mise en œuvre de la directive proposée variera d'un État membre à l'autre.

En dehors des coûts susceptibles d'être couverts par les programmes des États membres au titre du Fonds pour la sécurité intérieure, il n'y aura pas d'autres coûts supportés au niveau de l'Union.

---

41 Les centres de coopération policière et douanière sont des pôles d'information régionaux mis en place dans les régions frontalières de deux ou plusieurs États membres. Ils sont composés de membres du personnel des services répressifs de ces États membres. Jusqu'à présent, 59 centres de coopération policière et douanière ont été mis en place en Europe.

42 Règlement (UE) 2021/1149.

43 Voir l'article 3, paragraphe 2, points a) et b), du règlement (UE) 2021/1149.

5. AUTRES ÉLÉMENTS

- **Plans de mise en œuvre et modalités de suivi, d'évaluation et d'information**

L'évaluation des incidences des mesures proposées dépend des informations qui seront reçues des États membres. Pour cette raison, la présente proposition contient des **dispositions relatives à la collecte d'indicateurs de données**. La responsabilité de la collecte des données de suivi pertinentes devrait incomber aux autorités nationales, idéalement aux points de contact uniques. Par la suite, le suivi de ces indicateurs d'activité sera utilisé pour fournir des informations sur l'application des mesures proposées.

À cet égard, la présente proposition impose à la Commission de soumettre au Parlement européen et au Conseil un rapport évaluant dans quelle mesure les États membres auront pris les mesures nécessaires pour se conformer à la directive proposée. L'article en question prévoit également que la Commission soumette au Parlement européen et au Conseil un rapport évaluant la valeur ajoutée de la directive, cinq ans après son entrée en vigueur, et envisage une éventuelle révision de la directive en fonction de sa pertinence.

Outre cette proposition législative, la Commission, agissant en vertu de son autonomie administrative, mettra en place un **groupe d'experts informel** composé d'experts de chaque État membre, qui sera chargé de la conseiller et de la soutenir dans le contrôle et l'application de la directive, y compris dans l'élaboration de ses documents d'orientation. Ce groupe d'experts pourrait s'appuyer sur le réseau informel existant des responsables des points de contact uniques. Enfin, le mécanisme d'évaluation et de contrôle destiné à vérifier l'application de l'acquis de Schengen dans le domaine de la coopération policière continuera d'être mis en œuvre, conformément au règlement du Conseil en vigueur[44] et, à terme, conformément au règlement susceptible de le modifier[45]. Ces rapports d'évaluation ont jusqu'à présent porté sur la mise en œuvre de la décision-cadre suédoise. Les évaluations futures porteront sur l'application de la nouvelle directive envisagée.

- **Explication détaillée de certaines dispositions de la proposition**

La présente proposition de directive est structurée en six chapitres:

(1) Dispositions générales relatives à l'échange d'informations entre les services répressifs des États membres aux fins de la prévention ou de la détection des infractions pénales et des enquêtes en la matière (articles 1er, 2 et 3)

Ce premier ensemble de dispositions se fonde sur la structure et le contenu de la décision-cadre suédoise en vigueur depuis 2006. En outre, il aligne son champ d'application et son contenu sur les dispositions relatives à la coopération policière (titre V, chapitre 4) telles qu'introduites par le traité de Lisbonne en vigueur depuis 2009.

L'article 1er définit le champ d'application des règles horizontales relatives à l'échange d'informations aux fins de la prévention ou de la détection des infractions pénales et des enquêtes en la matière. Les dispositions de la présente directive s'appliquent, sauf dispositions contraires prévues par d'autres actes spécifiques du droit de l'Union.

L'article 2 définit un certain nombre de termes clés, tels que les autorités soumises aux règles horizontales sur l'échange d'informations, les infractions pénales concernées et les types d'informations dont disposent les services répressifs.

---

44 JO L 295 du 6.11.2013, p. 27.

45 Proposition de règlement du Conseil relatif à la création et au fonctionnement d'un mécanisme d'évaluation et de contrôle destiné à vérifier l'application de l'acquis de Schengen, et abrogeant le règlement (UE) nº 1053/2013, présentée par la Commission le 2 juin 2021.

L'article 3 énonce trois principes qui doivent être respectés lors de l'échange d'informations entre les États membres au titre de la directive: le principe d'accès équivalent selon lequel essentiellement les mêmes conditions doivent s'appliquer aux échanges d'informations au sein d'un État membre et entre États membres; le principe de disponibilité en vertu duquel les informations concernant une infraction pénale disponibles dans un État membre doivent, en règle générale, être également mises à la disposition des autres États membres; et le principe de confidentialité garantissant que les États membres respectent les exigences de confidentialité des autres lors du traitement de ces informations, en assurant un niveau de protection similaire.

(2) Échange d'informations par l'intermédiaire du point de contact unique (articles 4, 5 et 6)

L'article 4 énonce plusieurs exigences en ce qui concerne les demandes d'informations adressées au point de contact unique. Il s'agit notamment des critères justifiant la demande et qualifiant l'urgence. La demande doit être présentée par le point de contact unique des autres États membres ou, lorsqu'un État membre en décide ainsi, par d'autres services répressifs. La langue utilisée pour la demande doit être choisie dans une liste de langues que chaque État membre est tenu d'établir et qui doit être publiée au *Journal officiel de l'Union européenne*.

L'article 5 établit l'obligation pour le point de contact unique recevant les demandes d'informations visées à l'article 4 de traiter ces demandes et d'y répondre dans des délais précis, auxquels il ne peut être dérogé que dans certaines circonstances strictement déterminées, à savoir lorsqu'une autorisation judiciaire est requise. Cette communication d'informations doit se faire dans la même langue que celle utilisée pour la demande.

L'article 6 établit une liste exhaustive des motifs que le point de contact unique peut invoquer, pour autant qu'ils soient objectivement justifiés, pour refuser la divulgation des informations demandées, et dont l'autorité compétente de l'État membre requérant doit être promptement informée. La possibilité pour le point de contact unique de demander des éclaircissements sur le contenu des demandes est prévue, suspendant ainsi les délais applicables, mais uniquement si les éclaircissements sont objectivement nécessaires pour éviter un rejet de la demande. En ce qui concerne les autres éclaircissements qui pourraient être jugés nécessaires, une telle suspension n'est pas prévue.

(3) Autres échanges d'informations (articles 7 et 8)

L'article 7 établit l'obligation pour les États membres de partager des informations avec un ou plusieurs autres États membres de manière spontanée, c'est-à-dire de la propre initiative de l'autorité compétente sans qu'une demande d'informations n'ait été soumise, lorsque ces informations sont susceptibles de contribuer à la réalisation de l'un des objectifs énoncés dans la directive.

L'article 8 garantit que les points de contact uniques concernés sont tenus informés de tout échange d'informations sur demande, autre que les demandes soumises au point de contact unique, c'est-à-dire soit des échanges d'informations sur demande traités directement entre les services répressifs de différents États membres, soit des demandes d'informations soumises par un point de contact unique à un service répressif d'un autre État membre. Sont concernés les échanges d'informations pertinentes par les centres de coopération policière et douanière et tout autre organisme équivalent, dans la mesure où ils sont considérés comme des services répressifs au sens de la directive proposée.

(4) Règles supplémentaires relatives à la communication d'informations au titre des chapitres II et III (articles 9 à 13)

L'article 9 traite des situations dans lesquelles, en vertu du droit national de l'État membre qui dispose d'informations pertinentes, une autorisation judiciaire est requise pour la communication de ces informations, sur demande ou spontanément, par le point de contact unique ou par un service répressif. Cette disposition donne effet au principe d'accès équivalent et le définit plus précisément, ce qui signifie qu'essentiellement les mêmes conditions doivent s'appliquer lorsque les informations demandées sont soumises à une autorisation judiciaire, indépendamment du fait que les informations doivent être communiquées à une autorité d'un autre État membre et non à une autorité du même État membre. Cet article établit également que l'autorité concernée doit immédiatement prendre toutes les mesures nécessaires, tant sur le plan pratique que juridique, conformément à son droit national, en vue d'obtenir cette autorisation judiciaire dans les meilleurs délais.

L'article 10 énonce certaines exigences visant à garantir une protection adéquate des données à caractère personnel, résultant notamment de la mise en conformité avec les règles de la DPDR.

L'article 11 régit la langue que doivent utiliser les points de contact uniques et les services répressifs dans les situations spécifiées dans la présente directive, tant en ce qui concerne la fourniture effective d'informations que toute autre communication y afférente. Aucune exigence linguistique de ce type ne s'applique aux échanges directs d'informations et autres communications visés à l'article 8. Les États membres doivent établir une liste de langues acceptables pour eux, qui devrait également inclure l'anglais. Ces listes doivent être publiées par la Commission au *Journal officiel de l'Union européenne*.

L'article 12 prévoit l'obligation pour le point de contact unique ainsi que pour tous les autres services répressifs de tenir systématiquement Europol informé (ce qui signifie «mettre en copie»), dans la mesure où les échanges concernent des infractions relevant du mandat d'Europol tel que défini dans son acte de base. Cette obligation garantit qu'Europol peut remplir son rôle de pôle d'information dans l'Union en ce qui concerne les informations qui revêtent un intérêt à des fins répressives.

L'article 13 impose à toutes les autorités compétentes d'utiliser l'application de réseau d'échange sécurisé d'informations (SIENA), gérée par Europol, pour tous les échanges d'informations et les communications y afférentes couverts par la directive et, à cette fin, d'y être directement connectées. Ces règles relatives à l'utilisation obligatoire de l'application SIENA ne s'appliquent pas lorsque des actes spécifiques du droit de l'Union prévoient des exigences différentes quant au canal de communication à utiliser, par exemple pour les échanges d'informations régis par le règlement SIS[46], étant donné que les échanges effectués en vertu de ces actes spécifiques sont exclus du champ d'application de la présente directive.

[46] JO L 312 du 7.12.2018, p. 1. Règlement (UE) 2018/1860 relatif à l'utilisation du système d'information Schengen aux fins du retour des ressortissants de pays tiers en séjour irrégulier; règlement (UE) 2018/1861 sur l'établissement, le fonctionnement et l'utilisation du système d'information Schengen (SIS) dans le domaine des vérifications aux frontières, modifiant la convention d'application de l'accord de Schengen et modifiant et abrogeant le règlement (CE) nº 1987/2006; règlement (UE) 2018/1862 sur l'établissement, le fonctionnement et l'utilisation du système d'information Schengen (SIS) dans le domaine de la coopération policière et de la coopération judiciaire en matière pénale, modifiant et abrogeant la décision 2007/533/JAI du Conseil, et abrogeant le règlement (CE) nº 1986/2006 du Parlement européen et du Conseil et la décision 2010/261/UE de la Commission, tel que modifié.

(5) Exigences minimales relatives à l'établissement d'un point de contact unique en tant qu'entité centrale chargée de coordonner l'échange d'informations entre les États membres (articles 14, 15 et 16)

Le cinquième ensemble de dispositions énonce et développe l'obligation imposée à chaque État membre d'établir ou de désigner un point de contact unique en tant qu'entité centrale chargée de coordonner les échanges d'informations entre ses services répressifs et ceux des autres États membres dans le cadre de la directive. Il énonce un certain nombre d'exigences minimales auxquelles tout point de contact unique doit se conformer.

L'article 14 définit les tâches et les capacités du point de contact unique. Pour pouvoir exercer ses fonctions, le point de contact unique doit avoir accès aux informations nécessaires et être tenu systématiquement informé de tous les échanges directs d'informations entre ses autorités nationales et celles des autres États membres. L'établissement effectif ou la désignation effective des points de contact uniques doivent être notifiés, dans un délai déterminé, à la Commission, qui doit ensuite publier ces notifications au *Journal officiel de l'Union européenne*.

L'article 15 établit des exigences minimales relatives à la composition du point de contact unique, en laissant une certaine latitude à chaque État membre pour en déterminer précisément l'organisation et la composition, comme il le juge le plus approprié en fonction de sa situation nationale, à condition que les exigences de la directive soient respectées.

L'article 16 définit les exigences minimales applicables au système de gestion des dossiers des points de contact uniques.

(6) Dispositions finales

Les dispositions finales garantissent que la mise en œuvre de la directive proposée est correctement contrôlée, premièrement, par les États membres, au titre de l'obligation de collecter et de fournir un ensemble minimal de données statistiques sur une base annuelle (article 17), deuxièmement, par la Commission, au titre de l'obligation de faire rapport au Parlement européen et au Conseil, en tenant compte notamment des données fournies par les États membres, permettant ainsi, troisièmement, à ces deux institutions de contrôler également la mise en œuvre de la directive (article 18).

Enfin, les articles 19 à 23 traitent d'un certain nombre de questions juridico-techniques nécessaires, à savoir la suppression ou l'abrogation des dispositions en vigueur que les dispositions de la directive proposée remplacent, la transposition en droit national, ainsi que l'entrée en vigueur et les destinataires. En ce qui concerne les dispositions en vigueur contenues dans la CAAS (article 19), l'article 39 de celle-ci n'est remplacé que dans la mesure où il concerne l'échange d'informations aux fins spécifiées dans la directive proposée. L'article 39 reste applicable aux autres formes de coopération policière visées par cet article. En revanche, l'article 46 de la CAAS, qui porte spécifiquement sur cet échange d'informations, est entièrement remplacé par la directive proposée et est par conséquent supprimé.

2021/0411 (COD)

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

LE PARLEMENT EUROPÉEN ET LE CONSEIL DE L'UNION EUROPÉENNE,

vu le traité sur le fonctionnement de l'Union européenne, et notamment son article 87, paragraphe 2, point a),

vu la proposition de la Commission européenne,

après transmission du projet d'acte législatif aux parlements nationaux,

statuant conformément à la procédure législative ordinaire,

considérant ce qui suit:

(1) Les menaces transnationales impliquant des activités criminelles nécessitent une réponse coordonnée, ciblée et adaptée. Si les autorités nationales opérant sur le terrain sont en première ligne dans la lutte contre la criminalité organisée et le terrorisme, une action au niveau de l'Union est essentielle pour assurer une coopération efficace et efficiente, y compris en ce qui concerne l'échange d'informations. Par ailleurs, la criminalité organisée et le terrorisme, en particulier, sont emblématiques du lien existant entre sécurité intérieure et sécurité extérieure. Ces menaces s'étendent au-delà des frontières et se manifestent sous la forme d'organisations criminelles et de groupes terroristes qui se livrent à un large éventail d'activités criminelles.

(2) Dans un espace sans contrôles aux frontières intérieures, les agents de police d'un État membre devraient pouvoir, dans le cadre du droit de l'Union et du droit national applicables, bénéficier d'un accès équivalent aux informations dont disposent leurs homologues d'un autre État membre. À cet égard, les services répressifs devraient coopérer efficacement et, par défaut, dans toute l'Union. Aussi la coopération policière en matière d'échange d'informations pertinentes à des fins répressives est-elle une composante essentielle des mesures qui sous-tendent la sécurité publique dans un espace interdépendant sans contrôles aux frontières intérieures. L'échange d'informations sur la criminalité et les activités criminelles, y compris le terrorisme, sert l'objectif général de protection de la sécurité des personnes physiques.

(3) L'échange d'informations entre les États membres aux fins de la prévention ou de la détection des infractions pénales est régi par la convention d'application de l'accord de Schengen du 14 juin 1985[47], adoptée le 19 juin 1990, notamment à ses articles 39

[47] Convention d'application de l'accord de Schengen du 14 juin 1985 entre les gouvernements des États de l'Union économique Benelux, de la République fédérale d'Allemagne et de la République française relatif à la suppression graduelle des contrôles aux frontières communes (JO L 239 du 22.9.2000, p. 19).

et 46. La décision-cadre 2006/960/JAI du Conseil[48] a remplacé en partie ces dispositions et a introduit de nouvelles règles relatives à l'échange d'informations et de renseignements entre les services répressifs des États membres.

(4) Il ressort des évaluations, y compris de celles réalisées en application du règlement (UE) nº 1053/2013 du Conseil[49], que la décision-cadre 2006/960/JAI n'est pas suffisamment claire et ne garantit pas un échange adéquat et rapide des informations pertinentes entre les États membres. Les évaluations ont également montré que cette décision-cadre était en fait peu utilisée, en partie en raison du manque de clarté constaté en pratique entre le champ d'application de la convention d'application de l'accord de Schengen et celui de la décision-cadre.

(5) En conséquence, il conviendrait d'actualiser et de remplacer le cadre juridique existant, constitué des dispositions pertinentes de la convention d'application de l'accord de Schengen et de la décision-cadre 2006/960/JAI, de façon à faciliter et à garantir, par l'établissement de règles claires et harmonisées, l'échange adéquat et rapide d'informations entre les services répressifs compétents de différents États membres.

(6) En particulier, il convient de remédier aux divergences entre les dispositions pertinentes de la convention d'application de l'accord de Schengen et de la décision-cadre 2006/960/JAI en intégrant les échanges d'informations aux fins de la prévention ou de la détection des infractions pénales et des enquêtes en la matière, afin de remplacer entièrement, dans la mesure où ces échanges sont concernés, les articles 39 et 46 de ladite convention et, partant, de garantir la sécurité juridique nécessaire. Il conviendrait, en outre, de simplifier et de clarifier les règles applicables, de façon à faciliter leur application effective dans la pratique.

(7) Il est nécessaire de définir des règles régissant les aspects transversaux de cet échange d'informations entre les États membres. Les règles de la présente directive ne devraient pas porter atteinte à l'application des règles du droit de l'Union relatives à des systèmes ou cadres spécifiques pour de tels échanges, prévues notamment par les règlements (UE) 2018/1860[50], (UE) 2018/1861[51], (UE) 2018/1862[52]

---

48 Décision-cadre 2006/960/JAI du Conseil du 18 décembre 2006 relative à la simplification de l'échange d'informations et de renseignements entre les services répressifs des États membres de l'Union européenne (*JO L 386 du 29.12.2006, p. 89).*

49 Règlement (UE) nº 1053/2013 du Conseil du 7 octobre 2013 portant création d'un mécanisme d'évaluation et de contrôle destiné à vérifier l'application de l'acquis de Schengen et abrogeant la décision du comité exécutif du 16 septembre 1998 concernant la création d'une commission permanente d'évaluation et d'application de Schengen (JO L 295 *du 6.11.2013, p. 27).*

50 Règlement (UE) 2018/1860 du Parlement européen et du Conseil du 28 novembre 2018 relatif à l'utilisation du système d'information Schengen aux fins du retour des ressortissants de pays tiers en séjour irrégulier (JO L 312 du 7.12.2018, *p. 1).*

51 Règlement (UE) 2018/1861 du Parlement européen et du Conseil du 28 novembre 2018 sur l'établissement, le fonctionnement et l'utilisation du système d'information Schengen (SIS) dans le domaine des vérifications aux frontières, modifiant la convention d'application de l'accord de Schengen et modifiant et abrogeant le règlement (CE) nº 1987/2006 (JO L 312 du 7.12.2018, p. 14).

52 Règlement (UE) 2018/1862 du Parlement européen et du Conseil du 28 novembre 2018 sur l'établissement, le fonctionnement et l'utilisation du système d'information Schengen (SIS) dans le domaine de la coopération policière et de la coopération judiciaire en matière pénale, modifiant et abrogeant la décision 2007/533/JAI du Conseil, et abrogeant le règlement (CE) nº 1986/2006 du Parlement européen et du Conseil et la décision 2010/261/UE de la Commission (JO L 312 du 7.12.2018, p. 56).

et (UE) 2016/794[53] du Parlement européen et du Conseil, par les directives (UE) 2016/681[54] et (UE) 2019/1153[55] du Parlement européen et du Conseil, ainsi que par les décisions 2008/615/JAI[56] et 2008/616/JAI[57] du Conseil.

(8) La présente directive ne régit pas la communication et l'utilisation d'informations comme preuves dans une procédure judiciaire. En particulier, elle ne devrait pas être comprise comme établissant un droit d'utiliser comme preuves les informations communiquées au titre de la présente directive et, par conséquent, elle laisse telle quelle toute exigence prévue par le droit applicable relative à l'obtention du consentement de l'État membre qui communique les informations aux fins de cette utilisation. La présente directive laisse inchangés les actes du droit de l'Union sur les éléments de preuve, tels que le règlement (UE) .../...[58] [*relatif aux injonctions européennes de production et de conservation de preuves électroniques en matière pénale*] et la directive (UE) .../...[59] [*établissant des règles harmonisées concernant la désignation de représentants légaux aux fins de la collecte de preuves en matière pénale*].

(9) Tous les échanges d'informations au titre de la présente directive devraient être soumis à trois principes généraux, à savoir le principe de disponibilité, le principe d'accès équivalent et le principe de confidentialité. Bien que ces principes soient sans préjudice des dispositions plus particulières de la présente directive, ils devraient guider son interprétation et son application, s'il y a lieu. Par exemple, le principe de disponibilité devrait être compris comme indiquant que les informations pertinentes dont disposent le point de contact unique ou les services répressifs d'un État membre devraient également être accessibles, dans toute la mesure du possible, à ceux des autres États membres. Ce principe ne devrait toutefois pas porter atteinte à l'application, lorsqu'elle est justifiée, de dispositions spéciales de la présente directive restreignant la disponibilité d'informations, telles que celles relatives aux motifs de refus de demandes d'informations et à l'autorisation judiciaire. En outre, selon le principe d'accès équivalent, l'accès du point de contact unique et des services répressifs d'un autre ou d'autres États membres aux informations pertinentes devrait

---

53 Règlement (UE) 2016/794 du Parlement européen et du Conseil du 11 mai 2016 relatif à l'Agence de l'Union européenne pour la coopération des services répressifs (Europol) et remplaçant et abrogeant les décisions du Conseil 2009/371/JAI, 2009/934/JAI, 2009/935/JAI, 2009/936/JAI et 2009/968/JAI (JO L 135 du 24.5.2016, p. 53).

54 Directive (UE) 2016/681 du Parlement européen et du Conseil du 27 avril 2016 relative à l'utilisation des données des dossiers passagers (PNR) pour la prévention et la détection des infractions terroristes et des formes graves de criminalité, ainsi que pour les enquêtes et les poursuites en la matière (*JO L 119 du 4.5.2016, p. 132).*

55 Directive (UE) 2019/1153 du Parlement européen et du Conseil du 20 juin 2019 fixant les règles facilitant l'utilisation d'informations financières et d'une autre nature aux fins de la prévention ou de la détection de certaines infractions pénales, ou des enquêtes ou des poursuites en la matière, et abrogeant la décision 2000/642/JAI du Conseil (*JO L 186 du 11.7.2019, p. 122).*

56 Décision 2008/615/JAI du Conseil du 23 juin 2008 relative à l'approfondissement de la coopération transfrontalière, notamment en vue de lutter contre le terrorisme et la criminalité transfrontalière (JO L 210 du 6.8.2008, p. 1).

57 Décision 2008/616/JAI du Conseil du 23 juin 2008 concernant la mise en œuvre de la décision 2008/615/JAI relative à l'approfondissement de la coopération transfrontalière, notamment en vue de lutter contre le terrorisme et la criminalité transfrontalière (JO L 210 du 6.8.2008, p. 12). Une proposition de règlement relatif à l'échange automatisé de données dans le cadre de la coopération policière («Prüm II») vise à abroger certaines parties de ces décisions du Conseil.

58 Proposition de règlement, COM(2018) 225 final – 2018/0108 (COD).

59 Proposition de directive, COM(2018) 226 final – 2018/0107 (COD).

être essentiellement le même, et, partant, ni plus ni moins strict, que l'accès de ceux d'un seul et même État membre, sous réserve des dispositions plus particulières de la directive.

(10) Afin de réaliser l'objectif visant à faciliter et à garantir l'échange adéquat et rapide d'informations entre États membres, il convient de prévoir la possibilité d'obtenir ces informations en adressant une demande d'informations au point de contact unique de l'autre État membre concerné, conformément à certaines exigences claires, simplifiées et harmonisées. En ce qui concerne la teneur de ces demandes d'informations, il convient notamment de préciser, de manière exhaustive et suffisamment détaillée et sans préjudice de la nécessité d'une appréciation au cas par cas, quand ces demandes doivent être considérées comme urgentes et quelles explications elles doivent contenir au minimum.

(11) S'il est vrai que le point de contact unique de chaque État membre devrait, en tout état de cause, avoir la possibilité de soumettre des demandes d'informations au point de contact unique d'un autre État membre, pour plus de souplesse, les États membres devraient être autorisés à décider que leurs services répressifs peuvent également soumettre de telles demandes. Afin que les points de contact uniques puissent exercer leurs fonctions de coordination au titre de la présente directive, il est toutefois nécessaire que, si un État membre prend une telle décision, son point de contact unique soit informé de toutes ces demandes sortantes, ainsi que de toute communication y afférente, en étant toujours mis en copie.

(12) Des délais sont nécessaires pour garantir un traitement rapide des demandes d'informations soumises à un point de contact unique. Ces délais devraient être clairs et proportionnés et tenir compte du point de savoir si la demande d'informations est urgente et si une autorisation judiciaire préalable est requise. Afin de garantir le respect des délais applicables tout en permettant une certaine souplesse dans les cas objectivement justifiés, il est nécessaire d'autoriser, à titre exceptionnel, des dérogations uniquement si, et dans la mesure où, l'autorité judiciaire compétente de l'État membre requis a besoin de temps supplémentaire pour se prononcer sur l'octroi de l'autorisation judiciaire nécessaire. Cela pourrait être nécessaire, par exemple, en raison de la large portée ou de la complexité des questions soulevées par la demande d'informations.

(13) Dans des cas exceptionnels, il peut être objectivement justifié pour un État membre de refuser de donner suite à une demande d'informations soumise à un point de contact unique. Afin de garantir le bon fonctionnement du système créé par la présente directive, il convient de définir ces cas de manière exhaustive et de les interpréter de manière restrictive. Lorsque seules certaines parties des informations faisant l'objet d'une telle demande se rapportent aux motifs du refus de la demande, les autres informations doivent être communiquées dans les délais fixés par la présente directive. Il convient de prévoir la possibilité de demander des éclaircissements, ce qui devrait entraîner une suspension des délais applicables. Cette possibilité ne devrait toutefois exister que lorsque les éclaircissements sont objectivement nécessaires et proportionnés, en ce que la demande d'informations devrait, autrement, être refusée pour l'un des motifs énumérés dans la présente directive. Dans l'intérêt d'une coopération efficace, il devrait rester possible de demander les éclaircissements nécessaires également dans d'autres situations, sans que cela n'entraîne toutefois la suspension des délais.

(14) Afin de permettre la souplesse nécessaire eu égard aux besoins opérationnels susceptibles de varier dans la pratique, il convient de prévoir deux autres moyens d'échange d'informations, en plus des demandes d'informations soumises aux points de contact uniques. Le premier est la communication spontanée d'informations, c'est-à-dire de la propre initiative des points de contact uniques ou des services répressifs sans demande préalable. Le second est la communication d'informations à la suite de demandes d'informations soumises soit par des points de contact uniques, soit par des services répressifs, non pas au point de contact unique d'un autre État membre, mais directement aux services répressifs de ce dernier. Pour ces deux moyens, il convient de ne fixer qu'un nombre limité d'exigences minimales, notamment en ce qui concerne l'information des points de contact uniques et, pour ce qui est de la communication spontanée d'informations, les situations dans lesquelles les informations doivent être communiquées et la langue qu'il convient d'utiliser.

(15) L'exigence d'une autorisation judiciaire préalable pour la communication d'informations peut constituer une garantie importante. Les systèmes juridiques des États membres diffèrent à cet égard et la présente directive ne devrait pas être comprise comme portant atteinte à ces exigences établies en droit national, mais uniquement comme les soumettant à la condition que les échanges nationaux et les échanges entre États membres soient traités de manière équivalente, tant sur le fond que sur le plan procédural. En outre, afin de limiter au maximum les retards et complications éventuels liés à l'application d'une telle exigence, le point de contact unique ou les services répressifs, selon le cas, de l'État membre de l'autorité judiciaire compétente devraient prendre toutes les mesures pratiques et juridiques nécessaires, s'il y a lieu en coopération avec le point de contact unique ou le service répressif d'un autre État membre qui a demandé les informations, en vue d'obtenir l'autorisation judiciaire dès que possible.

(16) Il est particulièrement important que la protection des données à caractère personnel, conformément au droit de l'Union, soit garantie dans le cadre de tous les échanges d'informations effectués au titre de la présente directive. À cette fin, les règles de la présente directive devraient être mises en conformité avec la directive (UE) 2016/680 du Parlement européen et du Conseil[60]. En particulier, il convient de préciser que les éventuelles données à caractère personnel échangées par les points de contact uniques et les services répressifs doivent rester limitées aux catégories de données énumérées à l'annexe II, section B, point 2, du règlement (UE) 2016/794 du Parlement européen et du Conseil[61]. En outre, il convient, dans la mesure du possible, d'opérer une distinction entre ces données à caractère personnel en fonction de leur degré d'exactitude et de fiabilité, en distinguant les faits des appréciations personnelles, afin de garantir à la fois la protection des personnes et la qualité et la fiabilité des informations échangées. S'il apparaît que les données à caractère personnel sont incorrectes, elles devraient être rectifiées ou effacées sans délai. Cette rectification ou

---

60 Directive (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, et abrogeant la décision-cadre 2008/977/JAI du Conseil (JO L 119 du 4.5.2016, p. 89).

61 Règlement (UE) 2016/794 du Parlement européen et du Conseil du 11 mai 2016 relatif à l'Agence de l'Union européenne pour la coopération des services répressifs (Europol) et remplaçant et abrogeant les décisions du Conseil 2009/371/JAI, 2009/934/JAI, 2009/935/JAI, 2009/936/JAI et 2009/968/JAI (*JO L 135 du 24.5.2016, p. 53).*

cet effacement, ainsi que tout autre traitement de données à caractère personnel en rapport avec les activités relevant de la présente directive, devraient être effectués conformément aux règles applicables du droit de l'Union, en particulier la directive (UE) 2016/680 et le règlement (UE) 2016/679 du Parlement européen et du Conseil[62], que la présente directive ne modifie pas.

(17) Afin de permettre une communication adéquate et rapide des informations par les points de contact uniques, soit sur demande, soit de leur propre initiative, il importe que les fonctionnaires compétents des États membres concernés se comprennent. Les barrières linguistiques entravent souvent l'échange transfrontière d'informations. C'est la raison pour laquelle il convient d'établir des règles relatives à l'utilisation des langues dans lesquelles doivent être rédigées les demandes d'informations soumises aux points de contact uniques, les informations devant être communiquées par les points de contact uniques ainsi que toute autre communication y afférente, concernant les refus et les éclaircissements, par exemple. Ces règles devraient assurer un équilibre entre, d'une part, le respect de la diversité linguistique au sein de l'Union et la limitation des coûts de traduction et, d'autre part, les besoins opérationnels liés à des échanges d'informations adéquats et rapides par-delà les frontières. Les États membres devraient, dès lors, établir une liste contenant non seulement une ou plusieurs langues officielles de l'Union de leur choix, mais également une langue qui soit largement comprise et utilisée dans la pratique, à savoir l'anglais.

(18) La poursuite du développement de l'Agence de l'Union européenne pour la coopération des services répressifs (Europol) en tant que pôle d'information de l'Union sur la criminalité constitue une priorité. C'est pourquoi, lorsque des informations ou d'éventuelles communications y afférentes sont échangées, que ce soit à la suite d'une demande d'informations soumise à un point de contact unique ou à un service répressif ou de la propre initiative de l'un ou de l'autre, il conviendrait d'envoyer une copie à Europol, mais uniquement dans la mesure où ces informations ou communications concernent des infractions relevant des objectifs d'Europol. Dans la pratique, cela peut se faire en cochant par défaut la case «application SIENA» correspondante.

(19) Il convient de remédier à la prolifération des canaux de communication utilisés pour la transmission d'informations en matière répressive entre les États membres et des communications y afférentes, car cette prolifération entrave l'échange adéquat et rapide de ces informations. L'utilisation de l'application de réseau d'échange sécurisé d'informations SIENA, gérée par Europol conformément au règlement (UE) 2016/794, devrait, par conséquent, être rendue obligatoire pour toutes les transmissions et communications de ce type effectuées au titre de la présente directive, y compris pour l'envoi des demandes d'informations soumises aux points de contact uniques et directement aux services répressifs, pour la communication d'informations à la suite de ces demandes ou de la propre initiative des points de contact uniques ou des services répressifs, pour les communications sur les refus et les éclaircissements, ainsi que pour les copies aux points de contact uniques et à Europol. À cette fin, tous les points de contact uniques, ainsi que tous les services répressifs susceptibles de participer à ces échanges, devraient être directement connectés à

[62] Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données) (JO L 119 du 4.5.2016, p. 1).

l'application SIENA. À cet égard, il convient toutefois de prévoir une période de transition afin de permettre le déploiement complet de l'application SIENA.

(20) Afin de simplifier, de faciliter et de mieux gérer les flux d'informations, les États membres devraient chacun établir ou désigner un point de contact unique compétent chargé de coordonner les échanges d'informations au titre de la présente directive. Les points de contact uniques devraient, en particulier, contribuer à atténuer la fragmentation du paysage des services répressifs, notamment en ce qui concerne les flux d'informations, afin de répondre à la nécessité croissante de lutter conjointement contre la criminalité transfrontière, comme le trafic de stupéfiants et le terrorisme. Pour que les points de contact uniques soient en mesure de remplir efficacement leurs fonctions de coordination en ce qui concerne l'échange transfrontière d'informations à des fins répressives au titre de la présente directive, ils devraient se voir confier un certain nombre de tâches spécifiques minimales et disposer de certaines capacités minimales.

(21) Ces capacités des points de contact uniques devraient inclure un accès à toutes les informations disponibles dans leur propre État membre, y compris un accès convivial à toutes les bases de données et plateformes pertinentes de l'Union et internationales, conformément aux modalités précisées dans le droit de l'Union et dans le droit national applicables. Afin de pouvoir satisfaire aux exigences de la présente directive, notamment celles relatives aux délais, les points de contact uniques devraient être dotés de ressources suffisantes, y compris de capacités de traduction appropriées, et fonctionner en permanence. À cet égard, le fait de disposer d'un guichet d'accueil capable de filtrer, de traiter et de canaliser les demandes d'informations entrantes peut accroître leur efficacité et leur efficience. Ces capacités devraient également inclure le fait, pour les points de contact uniques, d'avoir, à tout moment, à leur disposition des autorités judiciaires compétentes pour accorder les autorisations judiciaires nécessaires. Dans la pratique, cela peut se faire, par exemple, en garantissant la présence physique ou la disponibilité fonctionnelle de ces autorités judiciaires, soit dans les locaux du point de contact unique, soit directement sur appel.

(22) Pour qu'ils soient en mesure d'exercer efficacement leurs fonctions de coordination au titre de la présente directive, les points de contact uniques devraient être composés de représentants des services répressifs nationaux dont la participation est nécessaire à l'échange adéquat et rapide d'informations au titre de la présente directive. Bien qu'il appartienne à chaque État membre de décider précisément de l'organisation et de la composition nécessaires pour satisfaire à cette exigence, ces représentants peuvent inclure les services de police, les services des douanes et d'autres services répressifs compétents aux fins de la prévention ou de la détection des infractions pénales et des enquêtes en la matière, ainsi que des points de contact possibles pour les bureaux régionaux et bilatéraux, tels que des officiers de liaison et des attachés détachés ou affectés dans d'autres États membres et auprès des agences répressives concernées de l'Union, telles qu'Europol. Toutefois, dans l'intérêt d'une coordination efficace, les points de contact uniques devraient être composés au moins de représentants de l'unité nationale Europol, du bureau SIRENE, de l'unité d'informations passagers et du bureau central national INTERPOL, tels qu'établis par la législation applicable et nonobstant le fait que la présente directive n'est pas applicable aux échanges d'informations expressément régis par cette législation de l'Union.

(23) Le déploiement et l'exploitation par les points de contact uniques d'un système électronique unique de gestion des dossiers doté de certaines fonctions et capacités minimales sont nécessaires pour leur permettre d'accomplir les tâches qui leur

incombent en application de la présente directive de manière efficace et efficiente, notamment en ce qui concerne la gestion des informations.

(24) Afin de permettre le contrôle et l'évaluation nécessaires de l'application de la présente directive, les États membres devraient être tenus de collecter certaines données et de les communiquer chaque année à la Commission. Cette exigence est nécessaire, notamment, pour remédier à l'absence de données comparables quantifiant les échanges d'informations pertinentes et permet également à la Commission de s'acquitter plus aisément de son obligation d'établissement de rapports.

(25) Le caractère transfrontière de la criminalité et du terrorisme oblige les États membres à compter les uns sur les autres pour lutter contre ces infractions pénales. Les objectifs consistant à garantir des flux d'informations adéquats et rapides entre les services répressifs compétents et vers Europol ne peuvent être atteints de manière suffisante par les États membres agissant isolément. En raison des dimensions et des effets de l'action, ils peuvent l'être mieux au niveau de l'Union par l'établissement de règles communes sur l'échange d'informations. L'Union peut ainsi adopter des mesures conformément au principe de subsidiarité énoncé à l'article 5 du traité sur l'Union européenne. Conformément au principe de proportionnalité tel qu'énoncé audit article, la présente directive n'excède pas ce qui est nécessaire pour réaliser ces objectifs.

(26) Conformément aux articles 1er et 2 du protocole nº 22 sur la position du Danemark annexé au traité sur l'Union européenne et au traité sur le fonctionnement de l'Union européenne, le Danemark ne participe pas à l'adoption de la présente directive et n'est pas lié par celle-ci ni soumis à son application. La présente directive développant l'acquis de Schengen, le Danemark devrait décider, conformément à l'article 4 dudit protocole, dans un délai de six mois à partir de la décision du Conseil sur la présente directive, s'il la transpose dans son droit interne.

(27) La présente directive constitue un développement des dispositions de l'acquis de Schengen auxquelles l'Irlande participe, conformément à la décision 2002/192/CE du Conseil[63]; l'Irlande participe donc à l'adoption de la présente directive et est liée par celle-ci.

(28) En ce qui concerne l'Islande et la Norvège, la présente directive constitue un développement des dispositions de l'acquis de Schengen au sens de l'accord conclu par le Conseil de l'Union européenne, la République d'Islande et le Royaume de Norvège sur l'association de ces deux États à la mise en œuvre, à l'application et au développement de l'acquis de Schengen[64], qui relèvent du domaine visé à l'article 1er, point H, de la décision 1999/437/CE du Conseil[65].

(29) En ce qui concerne la Suisse, la présente directive constitue un développement des dispositions de l'acquis de Schengen au sens de l'accord entre l'Union européenne, la Communauté européenne et la Confédération suisse sur l'association de la Confédération suisse à la mise en œuvre, à l'application et au développement de

63 Décision 2002/192/CE du Conseil du 28 février 2002 relative à la demande de l'Irlande de participer à certaines dispositions de l'acquis de Schengen (JO L 64 du 7.3.2002, p. 20).

64 JO L 176 du 10.7.1999, p. 36.

65 Décision 1999/437/CE du Conseil, du 17 mai 1999, relative à certaines modalités d'application de l'accord conclu par le Conseil de l'Union européenne et la République d'Islande et le Royaume de Norvège sur l'association de ces États à la mise en œuvre, à l'application et au développement de l'acquis de Schengen (JO L 176 du 10.7.1999).

l'acquis de Schengen[66], qui relèvent du domaine visé à l'article 1er, point H, de la décision 1999/437/CE du Conseil, lue en liaison avec l'article 3 de la décision 2008/146/CE[67] du Conseil et l'article 3 de la décision 2008/149/JAI du Conseil[68].

(30) En ce qui concerne le Liechtenstein, la présente directive constitue un développement des dispositions de l'acquis de Schengen au sens du protocole entre l'Union européenne, la Communauté européenne, la Confédération suisse et la Principauté de Liechtenstein sur l'adhésion de la Principauté de Liechtenstein à l'accord entre l'Union européenne, la Communauté européenne et la Confédération suisse sur l'association de la Confédération suisse à la mise en œuvre, à l'application et au développement de l'acquis de Schengen[69], qui relèvent du domaine visé à l'article 1er, point H, de la décision 1999/437/CE du Conseil, lue en liaison avec l'article 3 de la décision 2011/350/UE[70] du Conseil et l'article 3 de la décision 2011/349/UE du Conseil[71],

ONT ADOPTÉ LA PRÉSENTE DIRECTIVE:

CHAPITRE I

Dispositions générales

Article premier
Objet et champ d'application

1. La présente directive établit des règles relatives à l'échange d'informations entre les services répressifs des États membres, lorsque cela est nécessaire aux fins de la prévention ou de la détection des infractions pénales et des enquêtes en la matière.

En particulier, la présente directive établit des règles sur:

---

66 JO L 53 du 27.2.2008, p. 52.

67 Décision 2008/146/CE du Conseil du 28 janvier 2008 relative à la conclusion, au nom de la Communauté européenne, de l'accord entre l'Union européenne, la Communauté européenne et la Confédération suisse sur l'association de la Confédération suisse à la mise en œuvre, à l'application et au développement de l'acquis de Schengen (JO L 53 du 27.2.2008).

68 Décision 2008/149/JAI du Conseil du 28 janvier 2008 relative à la conclusion, au nom de l'Union européenne, de l'accord entre l'Union européenne, la Communauté européenne et la Confédération suisse sur l'association de la Confédération suisse à la mise en œuvre, à l'application et au développement de l'acquis de Schengen (JO L 53 du 27.2.2008).

69 JO L 160 du 18.6.2011, p. 21.

70 Décision 2011/350/UE du Conseil du 7 mars 2011 relative à la conclusion, au nom de l'Union européenne, du protocole entre l'Union européenne, la Communauté européenne, la Confédération suisse et la Principauté de Liechtenstein sur l'adhésion de la Principauté de Liechtenstein à l'accord entre l'Union européenne, la Communauté européenne et la Confédération suisse sur l'association de la Confédération suisse à la mise en œuvre, à l'application et au développement de l'acquis de Schengen en ce qui concerne la suppression des contrôles aux frontières intérieures et la circulation des personnes (JO L 160 du 18.6.2011).

71 Décision 2011/349/UE du Conseil du 7 mars 2011 relative à la conclusion, au nom de l'Union européenne, du protocole entre l'Union européenne, la Communauté européenne, la Confédération suisse et la Principauté de Liechtenstein sur l'adhésion de la Principauté de Liechtenstein à l'accord entre l'Union européenne, la Communauté européenne et la Confédération suisse sur l'association de la Confédération suisse à la mise en œuvre, à l'application et au développement de l'acquis de Schengen notamment en ce qui concerne la coopération judiciaire en matière pénale et la coopération policière (JO L 160 du 18.6.2011),

(a) les demandes d'informations soumises aux points de contact uniques établis ou désignés par les États membres, notamment des règles sur la teneur de ces demandes, les délais obligatoires dans lesquels les informations demandées sont communiquées, les motifs pour lesquels ces demandes sont refusées et le canal de communication devant être utilisé en ce qui concerne ces demandes;

(b) la communication spontanée d'informations pertinentes au point de contact unique ou aux services répressifs d'un autre ou d'autres États membres, en particulier les situations dans lesquelles ces informations doivent être communiquées et les modalités de leur communication;

(c) le canal de communication devant être utilisé pour tous les échanges d'informations et pour les informations qui doivent être communiquées aux points de contact uniques en ce qui concerne les échanges d'informations directement entre les services répressifs des États membres;

(d) l'établissement, les tâches, la composition et les capacités du point de contact unique, y compris des règles sur le déploiement d'un système électronique unique de gestion des dossiers pour l'accomplissement de ses tâches.

2. La présente directive ne s'applique pas aux échanges d'informations entre les services répressifs des États membres aux fins de la prévention ou de la détection des infractions pénales et des enquêtes en la matière qui sont expressément régis par d'autres actes du droit de l'Union.

3. La présente directive n'impose aucune obligation aux États membres:

a) d'obtenir des informations par des mesures coercitives, prises conformément au droit national, afin de les communiquer aux services répressifs d'un autre ou d'autres États membres;

b) de stocker des informations dans le but mentionné au point a);

c) de communiquer des informations aux services répressifs d'un autre ou d'autres États membres devant être utilisées comme preuves dans une procédure judiciaire.

4. La présente directive n'établit aucun droit d'utiliser les informations communiquées conformément à la présente directive comme preuves dans une procédure judiciaire.

Article 2
Définitions

Aux fins de la présente directive, on entend par:

(1) «service répressif»: tout service des États membres compétent en vertu du droit national aux fins de la prévention ou de la détection des infractions pénales et des enquêtes en la matière;

(2) «infractions pénales»: les infractions suivantes:

(a) les infractions énumérées à l'article 2, paragraphe 2, de la décision-cadre 2002/584/JAI du Conseil[72];

[72] Décision-cadre 2002/584/JAI du Conseil du 13 juin 2002 relative au mandat d'arrêt européen et aux procédures de remise entre États membres (JO L 190 du 18.7.2002, *p. 1).*

(b) les infractions visées à l'article 3, paragraphes 1 et 2, du règlement (UE) 2016/794;

(c) les infractions fiscales liées aux impôts directs et indirects, telles qu'elles sont définies en droit national;

(3) «informations»: tout contenu concernant une ou plusieurs personnes physiques, des faits ou des circonstances qui revêtent un intérêt pour les services répressifs dans le cadre de l'exercice des missions de prévention ou de détection des infractions pénales et d'enquête en la matière qui leur incombent en application du droit national;

(4) informations «disponibles/dont dispose(nt)»: les informations détenues soit par le point de contact unique soit par les services répressifs de l'État membre requis, ou les informations que ce point de contact unique ou ces services répressifs peuvent obtenir auprès d'autres autorités publiques ou de parties privées établies dans cet État membre sans prendre de mesures coercitives;

(5) «application SIENA»: l'application de réseau d'échange sécurisé d'informations, gérée par Europol, destinée à faciliter l'échange d'informations entre les États membres et Europol;

(6) «données à caractère personnel»: les données à caractère personnel telles que définies à l'article 4, point 1), du règlement (UE) 2016/679.

Article 3

Principes régissant l'échange d'informations

Les États membres veillent, en ce qui concerne tous les échanges d'informations au titre de la présente directive, à ce que:

(a) les informations pertinentes dont disposent le point de contact unique ou les services répressifs d'un État membre soient communiquées au point de contact unique ou aux services répressifs des autres États membres («principe de disponibilité»);

(b) les conditions applicables aux demandes d'informations émanant du point de contact unique ou des services répressifs des autres États membres, et celles régissant la communication d'informations au point de contact unique ou aux services répressifs des autres États membres, soient équivalentes à celles applicables aux demandes et à la communication d'informations similaires entre leurs propres services répressifs («principe d'accès équivalent»);

(c) les informations communiquées au point de contact unique ou aux services répressifs d'un autre État membre qui sont qualifiées de confidentielles soient protégées par ces services répressifs conformément aux exigences énoncées dans le droit national de cet État membre qui garantissent un niveau de confidentialité similaire («principe de confidentialité»).

Chapitre II

Échanges d'informations par l'intermédiaire des points de contact uniques

Article 4

Demandes d'informations au point de contact unique

1. Les États membres veillent à ce que leur point de contact unique et, s'ils en ont décidé ainsi, leurs services répressifs soumettent des demandes d'informations aux points de contact uniques respectifs des autres États membres conformément aux conditions énoncées aux paragraphes 2 à 5.

   Si un État membre a décidé que, outre son point de contact unique, ses services répressifs peuvent également soumettre des demandes d'informations aux points de contact uniques respectifs des autres États membres, il veille à ce que ces services envoient, en même temps qu'ils soumettent ces demandes, une copie de ces dernières, et de toute autre communication y afférente, aux points de contact uniques respectifs de ces États membres.

2. Les demandes d'informations au point de contact unique d'un autre État membre ne sont soumises que lorsqu'il existe des raisons objectives de penser que:

   (a) les informations demandées sont nécessaires et proportionnées à la réalisation de l'objectif mentionné à l'article 1er, paragraphe 1;

   (b) les services répressifs de l'État membre requis disposent des informations demandées .

3. Toute demande d'informations soumise au point de contact unique d'un autre État membre précise si elle revêt, ou non, un caractère urgent.

   Ces demandes d'informations sont considérées comme urgentes si, eu égard à l'ensemble des faits et circonstances pertinents du cas d'espèce, il existe des raisons objectives de penser que les informations demandées remplissent l'une ou plusieurs des conditions suivantes:

   (a) elles sont essentielles à la prévention d'une menace immédiate et grave pour la sécurité publique d'un État membre;

   (b) elles sont nécessaires à la protection des intérêts vitaux d'une personne qui sont exposés à un risque imminent;

   (c) elles sont nécessaires à l'adoption d'une décision susceptible d'impliquer le maintien de mesures restrictives qui s'apparentent à une privation de liberté;

   (d) elles présentent un risque imminent de perdre de leur intérêt si elles ne sont pas communiquées d'urgence.

4. Les demandes d'informations soumises au point de contact unique d'un autre État membre contiennent toutes les explications nécessaires pour en permettre le traitement adéquat et rapide conformément à la présente directive, dont au moins les éléments suivants:

   (a) une spécification des informations demandées qui soit aussi détaillée que cela est raisonnablement possible, dans les circonstances données;

   (b) une description de la finalité pour laquelle les informations sont demandées;

   (c) les raisons objectives qui donnent à penser que les services répressifs de l'État membre requis disposent des informations demandées;

   (d) une explication du lien entre la finalité et la ou les personnes auxquelles les informations se rapportent, s'il y a lieu;

(e) les raisons pour lesquelles la demande est considérée comme urgente, s'il y a lieu.

5. Les demandes d'informations soumises au point de contact unique d'un autre État membre sont présentées dans l'une des langues figurant sur la liste établie par l'État membre requis et publiée conformément à l'article 11.

Article 5

Communication d'informations à la suite d'une demande soumise au point de contact unique

1. Sous réserve du paragraphe 2 du présent article et de l'article 6, paragraphe 3, les États membres veillent à ce que leur point de contact unique communique les informations demandées conformément à l'article 4 dès que possible et, en tout état de cause, dans les délais suivants, selon le cas:

(a) huit heures pour les demandes urgentes portant sur des informations dont disposent les services répressifs de l'État membre requis sans qu'il soit nécessaire d'obtenir une autorisation judiciaire;

(b) trois jours civils pour les demandes urgentes portant sur des informations dont disposent les services répressifs de l'État membre requis et dont la communication est subordonnée à l'obtention d'une autorisation judiciaire;

(c) sept jours civils pour toutes les demandes qui ne sont pas urgentes.

Les délais prévus au premier alinéa commencent à courir au moment de la réception de la demande d'informations.

2. Si, selon son droit national, conformément à l'article 9, les informations demandées ne sont disponibles qu'après l'obtention d'une autorisation judiciaire, l'État membre requis peut déroger aux délais prévus au paragraphe 1 dans la mesure où cela est nécessaire pour obtenir cette autorisation.

En pareils cas, les États membres veillent à ce que leur point de contact unique s'acquitte des deux obligations suivantes:

i) informer immédiatement le point de contact unique ou, s'il y a lieu, le service répressif de l'État membre requérant du retard attendu, en précisant la durée et les motifs dudit retard;

ii) tenir le point de contact unique ou le service répressif ultérieurement informé et communiquer les informations demandées dès que possible après obtention de l'autorisation judiciaire.

3. Les États membres veillent à ce que leur point de contact unique communique les informations demandées conformément à l'article 4 au point de contact unique ou, s'il y a lieu, au service répressif de l'État membre requérant, dans la langue dans laquelle la demande d'informations a été soumise conformément à l'article 4, paragraphe 5.

Les États membres veillent à ce que, lors de la communication des informations demandées au service répressif de l'État membre requérant, leur point de contact unique envoie simultanément une copie de ces informations au point de contact unique de cet État membre.

Article 6

Refus de demandes d'informations

1. Les États membres veillent à ce que leur point de contact unique ne refuse de communiquer les informations demandées conformément à l'article 4 que dans la mesure où l'un des motifs suivants s'applique:

   (a) le point de contact unique et les services répressifs de l'État membre requis ne disposent pas des informations demandées;

   (b) la demande d'informations ne satisfait pas aux exigences énoncées à l'article 4;

   (c) l'autorisation judiciaire exigée par application du droit national de l'État membre requis conformément à l'article 9 a été refusée;

   (d) les informations demandées constituent des données à caractère personnel autres que celles relevant des catégories de données à caractère personnel visées à l'article 10, point i);

   (e) il existe des raisons objectives de penser que la communication des informations demandées:

      i) serait contraire aux intérêts essentiels de l'État membre requis en matière de sécurité;

      ii) nuirait au bon déroulement d'une enquête en cours en matière pénale; ou

      iii) porterait indûment atteinte aux intérêts vitaux d'une personne physique ou morale.

   Tout refus ne concerne que la partie des informations demandées à laquelle se rapportent les motifs énoncés au premier alinéa et est, le cas échéant, sans préjudice de l'obligation de communiquer les autres parties des informations conformément à la présente directive.

2. Les États membres veillent à ce que leur point de contact unique informe le point de contact unique ou, s'il y a lieu, le service répressif de l'État membre requérant du refus, en précisant les motifs de ce refus, dans les délais prévus à l'article 5, paragraphe 1.

3. Les États membres veillent à ce que leur point de contact unique sollicite immédiatement du point de contact unique ou, s'il y a lieu, du service répressif de l'État membre requérant les éclaircissements supplémentaires nécessaires au traitement d'une demande d'informations qui, à défaut, devrait être rejetée.

   Les délais mentionnés à l'article 5, paragraphe 1, sont suspendus entre la date à laquelle le point de contact unique ou, s'il y a lieu, le service répressif de l'État membre requérant reçoit la demande d'éclaircissements, et celle à laquelle le point de contact unique de l'État membre requis reçoit ces éclaircissements.

4. Les refus, les motifs de refus, les demandes d'éclaircissements et les éclaircissements visés aux paragraphes 3 et 4, ainsi que toute autre communication relative à une demande d'informations soumise au point de contact unique d'un autre État membre, sont communiqués dans la langue dans laquelle cette demande a été soumise conformément à l'article 4, paragraphe 5.

Chapitre III

Autres échanges d'informations

Article 7

Communication spontanée d'informations

1. Les États membres veillent à ce que leur point de contact unique ou leurs services répressifs communiquent, de leur propre initiative, toutes informations dont ils disposent au point de contact unique ou aux services répressifs d'un autre ou d'autres États membres, lorsqu'il existe des raisons objectives de penser que ces informations pourraient présenter un intérêt pour cet État ou ces États membres aux fins énoncées à l'article 1er, paragraphe 1. Toutefois, une telle obligation n'existe pas pour autant que les motifs mentionnés à l'article 6, paragraphe 1, points c), d) ou e), s'appliquent à ces informations.

2. Les États membres veillent à ce que, lorsque leur point de contact unique ou leurs services répressifs communiquent des informations de leur propre initiative conformément au paragraphe 1, ils le fassent dans l'une des langues figurant sur la liste établie par l'État membre requis et publiée conformément à l'article 11.

   Les États membres veillent à ce que, lorsque leur point de contact unique ou leurs services répressifs communiquent ces informations au service répressif d'un autre État membre, ils envoient aussi, simultanément, une copie de ces informations au point de contact unique de cet autre État membre.

Article 8

Échanges d'informations sur demandes soumises directement aux services répressifs

En cas de demandes d'informations que les points de contact uniques ou les services répressifs adressent directement aux services répressifs d'un autre État membre, les États membres veillent à ce que leur point de contact unique ou leurs services répressifs, en même temps qu'ils envoient ces demandes, communiquent des informations en réponse à ces demandes ou transmettent toute autre communication y afférente, en fassent parvenir une copie au point de contact unique de cet autre État membre et, lorsque l'expéditeur est un service répressif, une copie également au point de contact unique de son propre État membre.

Chapitre IV

Règles supplémentaires relatives à la communication d'informations au titre des chapitres II et III

Article 9

Autorisation judiciaire

1. Les États membres n'exigent pas d'autorisation judiciaire pour la communication d'informations au point de contact unique ou aux services répressifs d'un autre État membre au titre des chapitres II et III, lorsqu'aucune exigence de ce type ne s'applique à la communication équivalente d'informations à leur propre point de contact unique ou à leurs propres services répressifs.

2. Lorsque leur droit national exige une autorisation judiciaire pour la communication d'informations au point de contact unique ou aux services répressifs d'un autre État membre conformément au paragraphe 1, les États membres veillent à ce que leur point de contact unique ou leurs services répressifs prennent immédiatement toutes les mesures nécessaires, conformément à leur droit national, pour obtenir cette autorisation judiciaire dès que possible.

3. Les demandes d'autorisation judiciaire visées au paragraphe 1 font l'objet d'une appréciation et d'une décision conformément au droit national de l'État membre de l'autorité judiciaire compétente.

Article 10

Règles supplémentaires relatives aux informations constituant des données à caractère personnel

Lorsque leur point de contact unique ou leurs services répressifs communiquent des informations au titre des chapitres II et III qui constituent des données à caractère personnel, les États membres veillent à ce que:

i) les catégories de données à caractère personnel communiquées restent limitées à celles énumérées à l'annexe II, section B, point 2, du règlement (UE) 2016/794;

ii) leur point de contact unique ou leurs services répressifs communiquent aussi, simultanément et dans la mesure du possible, les éléments nécessaires permettant au point de contact unique ou au service répressif de l'autre État membre d'apprécier le degré d'exactitude, d'exhaustivité et de fiabilité des données à caractère personnel, ainsi que la mesure dans laquelle ces données sont à jour.

Article 11

Liste des langues

1. Les États membres établissent et tiennent à jour une liste comportant une ou plusieurs des langues officielles de l'Union dans lesquelles leur point de contact unique est en mesure de communiquer des informations sur demande ou de sa propre initiative. Cette liste comprend l'anglais.

2. Les États membres fournissent chacun cette liste, ainsi que ses éventuelles mises à jour, à la Commission. La Commission publie ces listes, ainsi que leurs éventuelles mises à jour, au *Journal officiel de l'Union européenne*.

Article 12

Communication d'informations à Europol

Les États membres veillent à ce que, lorsque leur point de contact unique ou leurs services répressifs adressent des demandes d'informations, communiquent des informations en réponse à ces demandes, transmettent des informations de leur propre initiative ou envoient d'autres communications y afférentes au titre des chapitres II et III, ils en envoient aussi, simultanément, une copie à Europol, dans la mesure où les informations sur lesquelles porte la communication concernent des infractions relevant des objectifs d'Europol conformément au règlement (UE) 2016/794.

Article 13

Utilisation de l'application SIENA

1. Les États membres veillent à ce que, lorsque leur point de contact unique ou leurs services répressifs adressent des demandes d'informations, communiquent des informations en réponse à ces demandes, transmettent des informations de leur propre initiative ou envoient d'autres communications y afférentes au titre des chapitres II et III ou de l'article 12, ils le fassent par l'intermédiaire de l'application SIENA.

2. Les États membres veillent à ce que leur point de contact unique, ainsi que tous leurs services répressifs susceptibles de participer à l'échange d'informations au titre de la présente directive, soient directement connectés à l'application SIENA.

Chapitre V

Point de contact unique pour l'échange d'informations entre les États membres

Article 14

Établissement, tâches et capacités

1. Chaque État membre établit ou désigne un point de contact unique national, qui est l'entité centrale chargée de coordonner les échanges d'informations au titre de la présente directive.

2. Les États membres veillent à ce que leur point de contact unique soit habilité à accomplir au moins l'ensemble des tâches suivantes:

   (a) recevoir et évaluer les demandes d'informations;

   (b) transmettre les demandes d'informations aux services répressifs nationaux appropriés et, si nécessaire, coordonner entre ces derniers le traitement de ces demandes et la communication d'informations en réponse à ces demandes;

   (c) analyser et structurer les informations en vue de les communiquer au point de contact unique et, s'il y a lieu, aux services répressifs d'un autre ou d'autres États membres;

   (d) communiquer, sur demande ou de sa propre initiative, des informations au point de contact unique et, s'il y a lieu, aux services répressifs d'un autre ou d'autres États membres, conformément aux articles 5 et 7;

   (e) refuser de communiquer des informations conformément à l'article 6 et, si nécessaire, demander des éclaircissements conformément à l'article 6, paragraphe 3;

   (f) adresser des demandes d'informations au point de contact unique d'un autre ou d'autres États membres conformément à l'article 4 et, s'il y a lieu, fournir des éclaircissements conformément à l'article 6, paragraphe 3.

3. Les États membres veillent à ce que:

   (a) leur point de contact unique ait accès à toutes les informations dont disposent leurs services répressifs, dans la mesure où cela est nécessaire à l'exécution des tâches qui lui incombent en application de la présente directive;

(b) leur point de contact unique accomplisse ses tâches 24 heures sur 24 et sept jours sur sept;

(c) leur point de contact unique soit doté du personnel, des ressources et des capacités, y compris en matière de traduction, nécessaires à l'accomplissement de ses tâches de manière adéquate et rapide conformément à la présente directive et notamment aux délais fixés à l'article 5, paragraphe 1;

(d) les autorités judiciaires compétentes pour accorder les autorisations judiciaires requises en droit national conformément à l'article 9 soient à la disposition du point de contact unique 24 heures sur 24 et sept jours sur sept.

4. Dans le mois qui suit l'établissement ou la désignation de leur point de contact unique, les États membres en font notification à la Commission. Ils mettent cette information à jour si nécessaire.

La Commission publie ces notifications, ainsi que leurs éventuelles mises à jour, au *Journal officiel de l'Union européenne*.

Article 15
Composition

1. Les États membres déterminent l'organisation et la composition de leur point de contact unique de manière à ce que ce dernier puisse s'acquitter des tâches qui lui incombent en application de la présente directive de manière efficace et efficiente.

2. Les États membres veillent à ce que leur point de contact unique soit composé de représentants des services répressifs nationaux dont la participation est nécessaire à l'échange adéquat et rapide d'informations au titre de la présente directive, dont au moins les structures suivantes, dans la mesure où l'État membre concerné est tenu par la législation applicable d'établir ou de désigner ces unités ou bureaux:

a) l'unité nationale Europol instituée par l'article 7 du règlement (UE) 2016/794;

b) le bureau SIRENE institué par l'article 7, paragraphe 2, du règlement (UE) 2018/1862 du Parlement européen et du Conseil[73];

c) l'unité d'informations passagers instituée par l'article 4 de la directive (UE) 2016/681;

d) le bureau central national INTERPOL institué par l'article 32 du statut de l'Organisation internationale de police criminelle – INTERPOL.

Article 16
Système de gestion des dossiers

1. Les États membres veillent à ce que leur point de contact unique déploie et exploite un système électronique unique de gestion des dossiers en tant que répertoire lui permettant d'accomplir les tâches qui lui incombent en application de la présente

[73] Règlement (UE) 2018/1862 du Parlement européen et du Conseil du 28 novembre 2018 sur l'établissement, le fonctionnement et l'utilisation du système d'information Schengen (SIS) dans le domaine de la coopération policière et de la coopération judiciaire en matière pénale, modifiant et abrogeant la décision 2007/533/JAI du Conseil, et abrogeant le règlement (CE) nº 1986/2006 du Parlement européen et du Conseil et la décision 2010/261/UE de la Commission (JO L 312 du 7.12.2018, p. 56).

directive. Le système de gestion des dossiers est doté au moins de l'ensemble des fonctions et capacités suivantes:

a) enregistrement des demandes d'informations entrantes et sortantes visées aux articles 5 et 8, ainsi que de toute autre communication avec les points de contact uniques et, s'il y a lieu, les services répressifs d'un autre ou d'autres États membres concernant ces demandes, y compris les informations sur les refus ainsi que les demandes et communications d'éclaircissements prévues à l'article 6, respectivement, paragraphes 2 et 3;

b) enregistrement des communications entre le point de contact unique et les services répressifs nationaux, conformément à l'article 15, paragraphe 2, point b);

c) enregistrement des informations communiquées au point de contact unique et, s'il y a lieu, aux services répressifs d'un autre ou d'autres États membres, conformément aux articles 5, 7 et 8;

d) recoupement des demandes d'informations entrantes, visées aux articles 5 et 8, avec les informations dont dispose le point de contact unique, y compris les informations communiquées conformément à l'article 5, paragraphe 3, deuxième alinéa, et à l'article 7, paragraphe 2, deuxième alinéa, et avec les autres informations pertinentes enregistrées dans le système de gestion des dossiers;

(e) suivi adéquat et rapide des demandes d'informations entrantes visées à l'article 4, notamment en vue de respecter les délais de communication des informations demandées fixés à l'article 5;

(f) interopérabilité avec l'application SIENA, afin notamment que les communications entrantes qui transitent par cette application puissent être directement enregistrées dans le système de gestion des dossiers et que les communications sortantes qui empruntent cette même application puissent être directement envoyées à partir dudit système;

(g) production de statistiques sur les échanges d'informations au titre de la présente directive à des fins d'évaluation et de contrôle, notamment aux fins de l'article 17;

(h) journalisation des accès et des autres activités de traitement pour ce qui est des informations contenues dans le système de gestion des dossiers, à des fins d'obligation de rendre compte et de cybersécurité.

2. Les États membres prennent les mesures nécessaires afin que tous les risques en matière de cybersécurité liés au système de gestion des dossiers, notamment en ce qui concerne son architecture, sa gouvernance et son contrôle, soient gérés et traités de manière prudente et efficace et que des garanties adéquates contre les accès non autorisés et les abus soient prévues.

3. Les États membres veillent à ce que les données à caractère personnel traitées par leur point de contact unique ne figurent dans le système de gestion des dossiers que pour la durée nécessaire et proportionnée aux fins pour lesquelles ces données sont traitées, puis à ce qu'elles soient irrévocablement supprimées.

Chapitre VI

Dispositions finales

Article 17
Statistiques

1. Les États membres fournissent à la Commission des statistiques sur les échanges d'informations avec les autres États membres au titre de la présente directive, au plus tard le 1er mars de chaque année.

2. Ces statistiques portent au minimum sur:

   a) le nombre de demandes d'informations soumises par leur point de contact unique et par leurs services répressifs;

   b) le nombre de demandes d'informations qui ont été reçues et auxquelles il a été répondu par leur point de contact unique et par leurs services répressifs, ventilé selon le caractère urgent ou non de ces demandes, et ventilé selon les autres États membres qui ont reçu les informations;

   c) le nombre de demandes d'informations refusées en vertu de l'article 6, ventilé par État membre requérant et par motif de refus;

   d) le nombre de cas dans lesquels il a été dérogé aux délais prévus à l'article 5, paragraphe 1, en raison de l'obligation d'obtenir une autorisation judiciaire conformément à l'article 5, paragraphe 2, ventilé par État membre ayant soumis les demandes d'informations concernées.

Article 18
Établissement de rapports

1. Au plus tard le *[date d'entrée en vigueur + 3 ans]*, la Commission soumet au Parlement européen et au Conseil un rapport évaluant la mise en œuvre de la présente directive.

2. Au plus tard le *[date d'entrée en vigueur + 5 ans]*, la Commission soumet au Parlement européen et au Conseil un rapport évaluant l'effectivité et l'efficacité de la présente directive. La Commission tient compte des informations communiquées par les États membres et de toute autre information pertinente liée à la transposition et à la mise en œuvre de la présente directive. Sur la base de cette évaluation, la Commission décide des actions de suivi appropriées, y compris, si nécessaire, d'une proposition législative.

.Article 19
Modifications de la convention d'application de l'accord de Schengen

À compter du *[date indiquée à l'article 21, paragraphe 1, premier alinéa]*, la convention d'application de l'accord de Schengen est modifiée comme suit:

   i) l'article 39 est remplacé par la présente directive dans la mesure où cet article concerne l'échange d'informations aux fins prévues à l'article 1er, paragraphe 1, de la présente directive;

   ii) l'article 46 est supprimé.

Article 20

Abrogation

La décision-cadre 2006/960/JAI est abrogée à partir du *[date indiquée à l'article 21, paragraphe 1, premier alinéa]*.

Les références faites à cette décision-cadre s'entendent comme faites aux dispositions correspondantes de la présente directive.

Article 21

Transposition

1. Les États membres mettent en vigueur les dispositions législatives, réglementaires et administratives nécessaires pour se conformer à la présente directive au plus tard le *[date d'entrée en vigueur + 2 ans]*. Ils communiquent immédiatement à la Commission le texte de ces dispositions.

   Ils appliquent ces dispositions à partir de cette date. Ils appliquent toutefois l'article 13 à partir du *[date d'entrée en vigueur + 4 ans*].

   Lorsque les États membres adoptent ces dispositions, celles-ci contiennent une référence à la présente directive ou sont accompagnées d'une telle référence lors de leur publication officielle. Les modalités de cette référence sont arrêtées par les États membres.

2. Les États membres communiquent à la Commission le texte des dispositions essentielles de droit interne qu'ils adoptent dans le domaine régi par la présente directive.

Article 22

Entrée en vigueur

La présente directive entre en vigueur le vingtième jour suivant celui de sa publication au *Journal officiel de l'Union européenne*.

Article 23

Destinataires

Les États membres sont destinataires de la présente directive conformément aux traités.

Fait à Bruxelles, le

Par le Parlement européen	*Par le Conseil*
Le président	*Le président*