COMMISSION
EUROPÉENNE

Bruxelles, le 7.12.2012
COM(2012) 735 final

COMMUNICATION DE LA COMMISSION AU PARLEMENT EUROPÉEN ET AU CONSEIL

Renforcer la coopération dans le domaine de la répression au sein de l'UE: le modèle européen d'échange d'informations (EIXM)

COMMUNICATION DE LA COMMISSION AU PARLEMENT EUROPÉEN ET AU CONSEIL

Renforcer la coopération dans le domaine de la répression au sein de l'UE: le modèle européen d'échange d'informations (EIXM)

1. INTRODUCTION

Pour garantir un niveau élevé de sécurité au sein de l'UE et de l'espace Schengen, la lutte contre les réseaux criminels appelle une action européenne concertée[1]. Celle-ci est nécessaire pour s'attaquer, d'une part, à la grande criminalité et à la criminalité organisée, comme la traite des êtres humains, le trafic illicite de drogues ou d'armes à feu, mais aussi, d'autre part, aux infractions moins graves commises à grande échelle par des groupes criminels mobiles et aux infractions commises par les personnes dans plusieurs États membres.

L'échange d'informations entre États membres constitue, dans ce contexte, un outil essentiel pour les services répressifs. Des accords internationaux et bilatéraux ont donc été complétés par des instruments et des systèmes au niveau de l'Union, comme le système d'information Schengen et le système d'information Europol, qui intègrent des garanties visant à protéger la vie privée et les données à caractère personnel, conformément à la charte des droits fondamentaux. La présente communication fait le point sur **la manière dont l'échange d'informations transfrontière** qui en résulte **fonctionne aujourd'hui dans l'Union européenne** et formule des recommandations pour l'améliorer.

Sa conclusion est que l'échange d'informations fonctionne bien de manière générale, des exemples de résultats positifs étant fournis ci-après à titre d'illustration. **Dès lors, à ce stade, aucune nouvelle base de données dans le domaine de la répression ni aucun nouvel instrument d'échange d'informations n'est nécessaire à l'échelle de l'UE.** Toutefois, les instruments existants de l'UE pourraient et devraient bénéficier d'une meilleure mise en œuvre, et les échanges devraient être organisés de manière plus cohérente.

Par conséquent, la présente communication formule des recommandations aux États membres sur les moyens d'**améliorer la mise en œuvre des instruments existants** et de **rationaliser les canaux de communication utilisés**. Elle souligne la nécessité de **garantir un niveau élevé de qualité, de sécurité et de protection des données**. Elle explique également comment la Commission apportera son aide aux États membres, notamment **en matière de financement et de formation**. Elle offre en ce sens un modèle pour guider les actions de l'UE et des États membres.

La présente communication répond à l'invitation faite à la Commission dans le programme de Stockholm d'évaluer la nécessité d'un modèle européen en matière d'échange d'informations à partir d'une évaluation des instruments existants. Elle s'appuie sur la communication de la Commission de 2010 qui dresse une présentation générale de la gestion de l'information dans le domaine de la liberté, de la sécurité et de la justice (ci-après la «communication de 2010»)[2] et sur la stratégie de gestion de l'information pour la sécurité intérieure de l'UE convenue

[1] La stratégie de sécurité intérieure de l'UE en action, COM(2010) 673.

[2] COM(2010) 385.

en 2009[3], ainsi que sur les actions entreprises par les États membres, la Commission et Europol en vue de sa mise en œuvre (ci-après les «actions relatives à la stratégie de gestion de l'information»). Elle s'inspire également d'un recensement des échanges d'informations au niveau de l'Union qui associent des experts nationaux et autres experts (CEPD, agences de l'UE, Interpol), d'une étude sur l'échange d'informations entre les services répressifs[4] et de discussions avec des parties concernées, y compris les autorités chargées de la protection des données.

2. LA SITUATION ACTUELLE

Les services répressifs échangent des informations à différentes fins: pour des enquêtes pénales, pour la prévention et la détection de la criminalité (par exemple, en recourant à des opérations de renseignement en matière pénale) et pour le maintien de l'ordre et de la sécurité publics. En ce qui concerne l'ampleur des échanges transfrontières, l'étude susmentionnée de 2010 rendait compte des réponses données par des agences nationales des États membres, selon lesquelles dans environ un quart de leurs enquêtes et opérations de renseignement en matière pénale, des demandes étaient envoyées à d'autres États membres de l'UE ou de l'espace Schengen.

2.1. Instruments

La communication de 2010 décrivait toutes les mesures régissant, au niveau de l'Union, la collecte, le stockage ou l'échange transfrontière d'informations à caractère personnel à des fins répressives ou de gestion des flux migratoires. La présente communication s'attache plus particulièrement aux **instruments utilisés pour les échanges transfrontières entre États membres.** Les États membres ont fourni des exemples de la manière dont ils utilisent les instruments.

L'**initiative suédoise**[5] fixe des règles, y compris des délais, pour l'échange d'informations et de renseignements entre les services répressifs des États membres dans le but de mener des enquêtes pénales ou des opérations de renseignement en matière pénale. Elle applique le principe de l'«accès équivalent»: les informations doivent être fournies aux États membres demandeurs à des conditions qui ne sont pas plus strictes que celles applicables au niveau national. Les informations doivent également être communiquées à Europol et à Eurojust dans la mesure où l'échange porte sur une infraction relevant de leur mandat.

En 2012, une société suédoise a été escroquée par un fraudeur italien connu, qui a conduit la société à verser 65 000 € sur un compte italien. Le point de contact unique suédois (voir point 3.2 ci-dessous) a reçu une demande de l'Italie, par le canal SIRENE (voir ci-dessous), le priant de contacter le directeur de la société pour vérifier si le versement avait été effectué, auquel cas l'Italie bloquerait les fonds. La Suède a pris des mesures et répondu dans le cadre de l'initiative suédoise en moins de 24 heures. Grâce à cette réaction rapide, la police suédoise a reçu des informations lui indiquant qu'une société était victime de fraude, et les autorités italiennes ont obtenu les informations nécessaires pour agir, et il est probable que les fonds pourront être récupérés.

[3] Conclusions du Conseil du 30 novembre 2009, 16637/09.
[4] http://ec.europa.eu/dgs/home-affairs/e-library/documents/categories/studies/index_en.htm
[5] Décision-cadre 2006/960/JAI du Conseil.

En 2012, aux urgences d'un hôpital de la région parisienne, un homme originaire de Belgique a donné des explications confuses sur l'origine d'une grave blessure par balle dont il souffrait. Les déclarations de la personne qui l'accompagnait ont orienté les enquêteurs vers de possibles agissements en Belgique. Les premières investigations ont montré que l'homme était connu en BE, notamment pour meurtre. Les services français ont immédiatement envoyé, dans le cadre de l'initiative suédoise, des informations spontanées à la police belge, qui a rapidement fait le lien avec des évènements survenus deux jours plus tôt en Belgique, au cours desquels quatre hommes armés avaient kidnappé un employé de bijouterie. L'intervention de la police avait mis les hommes en fuite. Dans leur fuite, l'un d'eux avait été blessé lors d'un échange de coups de feu avec la police. Grâce à ces informations, les services français ont placé l'homme sous surveillance dans l'attente d'un mandat d'arrêt européen, qui a été délivré le jour même en Belgique et transmis à la France par l'intermédiaire de SIRENE.

La décision **Prüm**[6] prévoit l'échange automatisé des profils ADN, des données relatives aux empreintes digitales et à l'immatriculation des véhicules à des fins d'enquête pénale (ADN, empreintes digitales et immatriculation des véhicules), de prévention des infractions pénales (empreintes digitales et immatriculation des véhicules) et de maintien de la sécurité publique (immatriculation des véhicules). La comparaison des données biométriques (ADN, empreintes digitales) se fait sur la base d'un système de concordance/non-concordance: une comparaison automatisée met en évidence une concordance anonyme si les données relatives à l'ADN ou aux empreintes digitales détenues par l'État membre demandeur concordent avec les données détenues par un autre État membre. Les données relatives à la personne ou à l'affaire ne sont fournies qu'en réponse à une demande de suivi distincte.

Un homme a été retrouvé sans vie, poignardé dans un appartement d'une ville allemande. Une empreinte digitale a été relevée sur le chambranle d'une porte. Une recherche automatisée dans le cadre de la décision Prüm a mis en évidence une concordance dans la base de données bulgare. Les informations de suivi demandées à la Bulgarie le lendemain ont été transmises dans un délai de 3 heures et immédiatement saisies dans le système d'information Schengen (SIS, voir ci-dessous). Le lendemain, l'auteur présumé des faits a été arrêté en Autriche.

En 2007, au début des échanges Prüm, du matériel a été volé dans une voiture de police à Vienne. Une trace d'ADN relevée dans la voiture concordait, dans la base de données autrichienne, avec une trace relevée dans une affaire semblable, mais c'est une concordance Prüm dans la base de données allemande qui a permis d'identifier un cambrioleur en série polonais. Un mandat d'arrêt européen a été délivré en Autriche. Le suspect a été arrêté en Pologne (grâce à une concordance sur un signalement SIS) et a par la suite été condamné en Autriche.

Europol soutient l'action des États membres et leur coopération en matière de prévention de la criminalité organisée, du terrorisme et d'autres formes graves de criminalité (telles qu'elles sont énumérées dans l'annexe à la décision du Conseil portant création d'Europol[7]) affectant deux États membres ou plus et de lutte contre ces phénomènes. L'Office sert de plateforme aux États membres, par le biais des unités nationales Europol, pour échanger des renseignements et des informations d'ordre pénal. Le système d'information Europol est une base de données qui comprend des informations (183 000 éléments) fournies par les États

[6] Décision 2008/615/JAI du Conseil.
[7] Décision 2009/371/JAI du Conseil.

membres sur la criminalité transfrontière relevant du mandat d'Europol, sur les personnes concernées (41 000) et d'autres données y afférentes. Europol l'utilise pour ses analyses et les États membres peuvent y avoir recours pour leurs enquêtes. Depuis 2011, d'autres services répressifs que les unités nationales Europol peuvent être désignés par les États membres pour accéder aux fonctions de recherche sur la base d'un système de concordance/non-concordance. Les fichiers de travail à des fins d'analyse permettent à Europol de fournir des analyses opérationnelles à l'appui des enquêtes transfrontières.

En Slovénie, de fausses cartes de paiement ont été utilisées pour retirer de grosses sommes d'argent dans des distributeurs de billets. Deux citoyens bulgares ont fait l'objet d'une enquête; l'utilisation du système d'information Europol a mis en évidence une concordance montrant que l'un d'entre eux avait commis des actes semblables en France et en Italie. La France a fourni des informations détaillées au système d'information Europol. Grâce à la réponse rapide de la France par l'intermédiaire de SIENA (voir ci-dessous), suivie d'une vérification des empreintes digitales et de la levée d'une restriction de traitement, les services slovènes ont pu se servir des données comme éléments de preuve devant les tribunaux. Le fichier de travail à des fins d'analyse établi par Europol a révélé l'existence de liens entre des affaires survenues en SI, BG, FR, IE, IT et NO.

Le **système d'information Schengen (SIS)** enregistre des signalements sur des personnes et des objets. À titre de mesure compensatoire pour la levée des contrôles aux frontières intérieures, il est utilisé tant au sein de l'espace Schengen qu'à ses frontières extérieures dans le but d'y maintenir un niveau élevé de sécurité. Il s'agit d'un système à grande échelle (plus de 43 millions de signalements) accessible aux agents en première ligne sur la base d'un système de concordance/non-concordance. En cas de concordance (c'est-à-dire si les données relatives à une personne ou un objet concordent avec un signalement), des informations supplémentaires peuvent être obtenues par l'intermédiaire des bureaux SIRENE (voir ci-dessous). Le SIS sera remplacé par le **système d'information Schengen de deuxième génération** (**SIS II)**, qui apportera entre autres améliorations la possibilité d'associer des signalements connexes (par exemple, un signalement sur une personne et sur un véhicule), de nouvelles catégories de signalement et un espace pour stocker les empreintes digitales, les photographies et les copies des mandats d'arrêt européens. La décision du Conseil relative au SIS II[8] définit des catégories de signalement pour soutenir la coopération entre les autorités policières et judiciaires en matière pénale. À cette fin, tous les États membres de l'UE participeront au SIS II, et Europol et Eurojust continueront à y avoir accès. La gestion des parties centrales de SIS II sera transférée à l'agence IT[9].

D'autres instruments de l'UE ou systèmes informatiques permettent l'échange d'informations en matière répressive entre les services de douane [convention Naples II, système d'information douanier dans le cadre des bases de données du système d'information antifraude gérées par l'Office européen de lutte antifraude (OLAF)], les cellules de renseignement financier, les bureaux de recouvrement des avoirs et les plateformes de signalement de la cybercriminalité[10]. L'accès des services répressifs à d'autres systèmes de l'UE à grande échelle est prévu (système d'information sur les visas) ou proposé

8 Décision 2007/533/JAI du Conseil.

9 Agence européenne pour la gestion opérationnelle des systèmes d'information à grande échelle au sein de l'espace de liberté, de sécurité et de justice.

10 La future stratégie européenne en matière de cybersécurité permettra d'évaluer les besoins futurs d'échange d'informations entre le réseau, les autorités chargées de la sécurité de l'information et les services répressifs, par exemple, par le biais du Centre européen de lutte contre la cybercriminalité.

(EURODAC[11]) aux fins de la prévention et de la détection des infractions terroristes et des autres infractions pénales graves, ainsi qu'aux fins des enquêtes en la matière. La question de l'octroi ou non d'un accès aux services répressifs et, dans l'affirmative, dans quelles conditions, est aussi actuellement à l'étude dans le cadre des travaux préparatoires engagés dans la perspective de la proposition de système d'entrée/sortie qui sera présentée prochainement.

Un système européen de surveillance des frontières (EUROSUR) est en cours de développement pour permettre l'échange d'informations et une coopération opérationnelle entre les centres nationaux de coordination et Frontex, afin d'améliorer l'information sur la situation aux frontières extérieures de l'UE et la capacité de réaction dans le cadre de la prévention de la migration clandestine et de la criminalité transfrontière. Un environnement commun de partage de l'information (CISE) pour la surveillance du domaine maritime de l'UE, visant notamment à permettre une connaissance plus fine de la situation maritime, est en cours d'élaboration afin de permettre les échanges transfrontières d'informations entre les autorités publiques de sept secteurs pertinents (y compris l'application de la réglementation), tout en assurant l'interopérabilité entre les systèmes de surveillance existants et futurs, comme EUROSUR.

Les États membres échangent également des informations au titre de lois nationales et d'accords bilatéraux. Ils sont également tous membres d'Interpol, qui peut servir à l'échange d'informations avec des pays du monde entier, soit par l'intermédiaire des avis et des bases de données d'Interpol (par exemple, sur les documents de voyage volés ou perdus), soit de manière bilatérale, par le canal Interpol.

2.2. Canaux et outils de communication

Trois canaux principaux sont utilisés pour l'échange d'informations transfrontière, chacun d'entre eux reposant, dans chaque État membre, sur des unités nationales qui utilisent un outil de communication spécifique:

(1) Les bureaux **SIRENE**[12] peuvent, suite à une concordance sur un signalement dans SIS, obtenir des informations supplémentaires auprès de l'État membre à l'origine du signalement. Ils fonctionnent 24 heures sur 24 et 7 jours sur 7 et appliquent les procédures du manuel SIRENE. À l'heure actuelle, ils échangent des informations via un système appelé SISNET, qui sera remplacé par le réseau de communication SIS II d'ici la fin du mois de mars 2013.

(2) Les unités nationales **Europol** (UNE) échangent des informations avec Europol. Elles peuvent également échanger de manière bilatérale des informations en matière pénale qui ne relèvent pas du mandat d'Europol, et ce sans passer par Europol. Les UNE sont à même d'échanger des informations directement ou par le biais des officiers de liaison d'Europol, qui font partie d'une UNE mais sont détachés au siège d'Europol. Un outil de communication sécurisé, **SIENA**[13], a été mis au point par Europol pour les échanges avec Europol et entre États membres. En 2011, les États

[11] La base de données européenne des empreintes digitales des demandeurs d'asile et des personnes franchissant les frontières de manière irrégulière.

[12] **S**upplementary **I**nformation **RE**quest at the **N**ational **E**ntry (supplément d'information requis à l'entrée nationale).

[13] **S**ecure **I**nformation **E**xchange **N**etwork **A**pplication (application de réseau d'échange sécurisé d'informations).

membres ont eu recours à SIENA pour échanger 222 000 messages; dans 53 % des cas, les informations contenues dans le message ont été transmises à Europol.

(3) Les bureaux centraux nationaux d'**Interpol**, qui fonctionnent 24 heures sur 24 et 7 jours sur 7, échangent des informations avec Interpol, mais également dans un contexte bilatéral, sans passer par ce dernier. Les bureaux centraux nationaux utilisent l'outil de communication I-24/7 mis au point par Interpol.

D'autres canaux existent, comme les officiers de liaison bilatéraux (détachés dans d'autres États membres et généralement sollicités dans les affaires plus complexes) et les centres de coopération policière et douanière (instaurés par des États membres voisins pour soutenir l'échange d'informations et la coopération opérationnelle dans les zones frontalières).

Le **choix du canal** est en partie régi par la législation de l'UE: les demandes d'informations supplémentaires survenant à la suite d'une concordance dans le SIS doivent être effectuées via les bureaux SIRENE, et l'échange d'informations avec Europol via les UNE. Dans les autres cas, ce sont les États membres qui choisissent.

2.3. Interaction des différents instruments, canaux et outils

Il existe divers instruments, canaux et outils, chacun étant conçu dans un but particulier. Une enquête pénale peut nécessiter l'utilisation parallèle ou séquentielle de plusieurs instruments. Dans le cadre d'une affaire transfrontière impliquant la grande criminalité ou la criminalité organisée, une personne ou un objet peut faire l'objet d'une vérification à la fois dans le système d'information Europol et dans le SIS, et en cas de concordance, des demandes de suivi peuvent être formulées par les canaux Europol ou SIRENE respectivement. Une trace biométrique peut faire l'objet d'un échange Prüm, suivi d'une demande post-concordance dans le cadre de l'initiative suédoise par l'intermédiaire de l'outil SIENA.

Quelle que soit la combinaison ou la séquence, les règles de chaque instrument doivent être respectées. Il s'agit notamment des règles relatives à la protection des données, à la sécurité et à la qualité des données, et aux fins pour lesquelles les instruments sont susceptibles d'être utilisés. Le traitement au niveau national des données résultant d'échanges transfrontières doit également respecter la législation de l'UE sur la protection des données à caractère personnel[14]. Le principe de proportionnalité doit être respecté; par exemple, des demandes peuvent être refusées dans le cadre de l'initiative suédoise si la fourniture d'informations est manifestement disproportionnée par rapport à la finalité de la demande. Le respect de ces règles exige que les demandes et réponses soient validées par du personnel suffisamment qualifié et travaillant avec les outils d'information appropriés.

2.4. Interface avec la coopération judiciaire

Le processus de justice pénale concerne autant les services répressifs que les autorités judiciaires, mais des différences existent entre les États membres, notamment la mesure dans laquelle les services judiciaires (y compris les procureurs) dirigent ou supervisent l'enquête pénale. Lorsque ce sont les services judiciaires qui conduisent l'enquête, de même que lorsque des informations sont nécessaires pour servir d'éléments de preuve, des procédures de coopération judiciaire comme l'entraide judiciaire sont généralement nécessaires.

[14] Décision-cadre 2008/977/JAI du Conseil.

Par ailleurs, des informations directement accessibles aux services répressifs dans un État membre peuvent nécessiter une autorisation judiciaire dans un autre. L'initiative suédoise exige que lorsque des informations demandées nécessitent une autorisation judiciaire, le service répressif requis en fasse la demande auprès de l'autorité judiciaire, qui doit appliquer les mêmes règles que pour une affaire strictement interne.

L'exercice de recensement des échanges d'information a toutefois révélé que les experts en matière de répression perçoivent les règles divergentes comme une source de retard dans les enquêtes transfrontières. Bien que cela ne relève pas du champ de la présente communication, il est à noter qu'Eurojust facilite la coopération judiciaire. La décision d'enquête européenne, qui fait actuellement l'objet de discussions, présenterait également de l'intérêt et pourrait remplacer les règles actuellement appliquées pour l'obtention transfrontière de preuves, conformément au principe de reconnaissance mutuelle. Il faudrait qu'elle soit reconnue et exécutée avec la même célérité que dans une affaire nationale similaire et, en tout état de cause, dans les délais prévus.

2.5. Principes

Dans sa communication de 2010, la Commission a énoncé des principes matériels et des principes axés sur les processus pour développer de nouvelles initiatives et évaluer les instruments actuels.

Les principes matériels sont:

(1) *Protéger les droits fondamentaux, notamment le droit au respect de la vie privée et à la protection des données.* Il s'agit de droits prévus aux articles 7 et 8 de la charte et à l'article 16 du traité sur le fonctionnement de l'Union européenne.

(2) *Nécessité.* Une restriction du droit au respect de la vie privée ne peut être justifiée que si elle est prévue par la loi, si elle poursuit un but légitime et si elle est nécessaire dans une société démocratique.

(3) *Subsidiarité.*

(4) *Gestion rigoureuse des risques.* Il est essentiel de vérifier la nécessité de toute mesure adoptée et de respecter le principe de limitation des finalités.

Les principes axés sur les processus sont:

(1) *Un bon rapport coût-efficacité.* Cela exige de se fonder sur les solutions existantes et de déterminer si un meilleur usage des instruments existants permettrait d'atteindre les objectifs d'une proposition.

(2) *Élaborer les politiques en partant de la base.* Citons, à titre d'exemple, l'exercice de recensement auquel ont participé des experts en matière de répression pour préparer la présente communication.

(3) *Une répartition claire des responsabilités.* La communication de 2010 relevait que les États membres n'avaient aucun «chef de projet» vers qui se tourner pour obtenir des conseils relatifs à la mise en œuvre de la décision Prüm. Le rapport Prüm de la Commission relève que cette lacune est désormais en partie comblée par le soutien offert par Europol. En ce qui concerne l'idée formulée dans la communication

de 2010 selon laquelle l'agence IT puisse peut-être prodiguer des conseils techniques, les priorités actuelles de l'agence sont ailleurs. L'évaluation triennale qui doit être rendue d'ici la fin de l'année 2015 sera l'occasion de réexaminer cette position.

(4) *Clauses de réexamen et de caducité.* La Commission a rendu des rapports sur l'initiative suédoise et la décision Prüm. La présente communication en tient compte.

3. ÉVALUATION ET RECOMMANDATIONS

Cette partie porte plus particulièrement sur l'initiative suédoise, la décision Prüm et le canal Europol. Bien que le SIS et le canal SIRENE totalisent un volume important des échanges d'informations, aucune recommandation n'est formulée à leur égard, dans la mesure où d'importants changements sont déjà engagés, notamment avec le prochain passage à SIS II.

3.1. Améliorer l'utilisation des instruments existants

Hormis la future réforme d'Europol, la Commission n'entend pas, à court terme, proposer de modifications des instruments européens susmentionnés. Il n'y a pas non plus besoin, à l'heure actuelle, de nouveaux instruments. **Les instruments existants doivent avant tout être mis en œuvre.**

C'est le cas notamment de la décision Prüm. Le rapport Prüm de la Commission joint à la présente communication constate que l'échange de données dans le cadre de la décision Prüm est fortement apprécié pour les enquêtes, mais que sa mise en œuvre accuse un sérieux retard. **De nombreux États membres n'échangent pas encore de données dans le cadre de la décision Prüm alors que la date limite de transposition était fixée au 26 août 2011**[15]. Les principales raisons sont de nature technique et résultent d'un manque de ressources humaines et financières dans les États membres. Toutefois, au vu des possibilités de soutien offertes par l'UE (financement, Mobile Competence Team, service d'assistance), c'est surtout la volonté politique de la mettre en œuvre qui semble faire défaut. Comme l'indique le rapport, la Commission continuera à apporter son aide en proposant un financement de l'Union. Toutefois, le contexte sera différent en décembre 2014, car la Commission sera alors en mesure d'engager des procédures en manquement. Les règles en matière de contrôle de la mise en œuvre au niveau national ne s'appliquent pas jusqu'à cette date, puisque la décision Prüm, comme l'initiative suédoise, a été adoptée dans le cadre de l'ancien troisième pilier.

En ce qui concerne **l'initiative suédoise**, la Commission a fait savoir en 2011 que l'instrument n'avait pas encore réalisé tout son potentiel mais que son importance irait en grandissant[16]. Cette appréciation reste valable, tous les États membres n'ayant pas encore mis en œuvre l'instrument[17]. La plupart des États membres ont signalé sa transposition dans leur législation nationale[18], tandis que d'autres ont fait savoir qu'une telle transposition n'était pas

---

15 Les États membres suivants l'ont mise en œuvre:
ADN: BG/CZ/DE/ES/EE/FR/CY/LV/LT/LU/HU/NL/AT/PT/RO/SI/SK/FI;
Empreintes digitales: BG/CZ/DE/EE/ES/FR/CY/LT/LU/HU/NL/AT/SI/SK;
Immatriculation des véhicules: BE/DE/ES/FR/LT/LU/NL/AT/PL/RO/SI/FI/SE.
Pour de plus amples informations, voir le rapport Prüm.

16 SEC(2011) 593.

17 Les États membres suivants n'ont pas encore adopté de dispositions d'application: BE/EL/IT/LU.

18 BG/CZ/DK/DE/EE/ES/FR/CY/HU/LT/LV/NL/PL/PT/RO/SI/SK/FI/SE.

nécessaire car leur législation nationale était déjà conforme à cet instrument[19]. Néanmoins, malgré ses avantages, notamment le principe d'accès équivalent et la fixation de délais, l'instrument demeure peu utilisé dans la pratique. Parmi les raisons avancées figurent le fait que d'autres solutions sont jugées adéquates et la complexité du formulaire de demande (même dans sa version simplifiée de 2010[20]).

La Commission a été invitée à examiner son utilité pour les demandes de suivi post-concordance relevant de la décision Prüm[21]. Lorsque des informations de suivi sont nécessaires pour servir de preuves devant une juridiction, une demande de coopération judiciaire est normalement requise. Toutefois, lorsque les informations ne sont pas ou pas encore requises à des fins de preuves, le recours systématique à l'initiative suédoise comme base juridique et à SIENA comme outil de communication devrait être encouragé afin de tirer le meilleur parti des avantages offerts par chacun de ces deux instruments et d'adopter pour l'ensemble des États membres une seule bonne pratique.

En ce qui concerne **Europol**, une évaluation réalisée en 2012[22] a confirmé d'autres constatations, selon lesquelles les États membres ne partagent pas les informations de manière adéquate avec Europol (et donc pas non plus entre eux). La Commission traitera cette question dans une proposition de modification de la base juridique d'Europol. Pour sa part, le Conseil a invité les États membres à utiliser davantage le système d'information Europol[23].

En accord avec le programme de Stockholm, la Commission a commandé une étude sur un éventuel **système européen d'information sur les registres de la police** (EPRIS)[24]. L'idée est de répondre à la nécessité perçue de permettre, au vu de la nature transfrontière accrue de la criminalité, à un fonctionnaire de police travaillant dans un État membre de savoir si un suspect est connu de la police dans un autre État membre. Conformément au principe exigeant un bon rapport coût-efficacité, la Commission estime que la création d'un EPRIS **ne se justifie pas à l'heure actuelle,** dans la mesure où les instruments et outils existants, susceptibles de satisfaire ce besoin en partie ou en totalité s'ils étaient mieux ou davantage utilisés, ne sont pas pleinement exploités. Cela concerne en particulier le système d'information Europol (par le téléchargement des données pertinentes et l'élargissement de l'accès au niveau national), le SIS II (par une utilisation accrue des signalements pertinents sur les personnes ou les véhicules à des fins de vérifications, afin de poursuivre les infractions pénales et de prévenir des menaces à la sécurité publique), SIENA (par le renforcement de l'accès au niveau national, la liaison avec les systèmes nationaux et, le cas échéant, l'automatisation des tâches) et la décision Prüm (par sa pleine mise en œuvre afin d'améliorer l'identification des criminels agissant dans différents États membres).

Les États membres sont invités à:

- mettre pleinement en œuvre l'initiative suédoise, y compris son principe d'accès équivalent;
- mettre pleinement en œuvre la décision Prüm, en recourant aux soutiens disponibles auprès de l'UE;

19 IE/MT/AT/UK.
20 9512/1/10.
21 Conclusions du Conseil des 27 et 28 octobre 2011, 15277/11.
22 https://www.europol.europa.eu/sites/default/files/publications/rand_evaluation_report.pdf
23 Conclusions du Conseil des 7 et 8 juin 2012, 10333/12.
24 http://ec.europa.eu/dgs/home-affairs/e-library/documents/categories/studies/index_en.htm

- pour les demandes de suivi post-concordance fondées sur la décision Prüm, utiliser l'initiative suédoise et l'outil SIENA.

La Commission:

- continuera à offrir un financement européen pour soutenir la mise en œuvre de la décision Prüm;

- se préparera, d'ici décembre 2014, à appliquer dans ce domaine les règles garantissant une mise en œuvre de la législation de l'Union européenne au niveau national.

3.2. Rationaliser et gérer les canaux

Choix du canal. Le fait que les États membres puissent choisir librement le canal (à l'exception des exigences juridiques relatives aux bureaux SIRENE et aux UNE) a notamment pour résultat qu'ils utilisent différents canaux à des degrés divers. Le guide de bonnes pratiques concernant les unités chargées de la coopération policière internationale au niveau national (ci-après le «guide de 2008»)[25], rédigé sous l'égide des chefs de police de l'UE, énonce des critères[26], mais ceux-ci ne sont pas contraignants et n'ont pas conduit à une convergence des pratiques nationales. Certains États membres ont évolué vers une utilisation plus systématique du canal Europol. D'autres continuent à compter en grande partie sur le canal Interpol, dont l'attrait semble reposer en partie sur son rôle traditionnellement central dans la coopération policière internationale et en partie sur son apparente simplicité d'utilisation. SISNET est utilisé par certains États membres pour des questions qui ne relèvent pas du SIS, par exemple des demandes dans le cadre de l'initiative suédoise.

La Commission estime qu'il est temps d'adopter une approche plus cohérente au sein de l'UE, qui attribue un rôle central au canal Europol. À ce titre, lorsque le canal n'est pas défini par une exigence juridique, **le canal Europol, par l'intermédiaire de l'outil SIENA, devrait être le canal par défaut**, à moins que des raisons particulières n'exigent d'en utiliser un autre. Ainsi, à titre d'exemple, les demandes de coopération policière actuellement effectuées à l'aide de SISNET (qui disparaîtra lorsque SIS II entrera en service[27]) devront à l'avenir être effectuées par l'intermédiaire de SIENA.

Certains États membres privilégient une approche qui laisse une grande liberté quant à l'utilisation des différents canaux, ce que réprouve la Commission. La mise au point, par tous les États membres, de règles nationales sur le choix du canal et leur convergence vers une approche commune unique seraient préférables aux disparités actuelles. Le choix du canal Europol se justifie par ses avantages. Il peut être demandé aux officiers de liaison Europol d'intervenir si nécessaire. Utilisé pour les échanges bilatéraux directs, SIENA facilite aussi le partage des informations avec Europol conformément aux exigences juridiques de la décision Europol et de l'initiative suédoise. Les messages SIENA sont structurés, peuvent prendre en charge de gros volumes de données et leurs échanges sont hautement sécurisés. La protection des données est accrue lorsque les informations sont échangées dans un format structuré, par exemple au moyen de SIENA. L'approche proposée cadre parfaitement avec la future proposition de la Commission visant à réformer Europol et avec les orientations stratégiques

[25] 7968/08.

[26] Reproduits dans les lignes directrices concernant la mise en œuvre de l'initiative suédoise, 9512/1/10.

[27] Le réseau de communication SIS II se limite, en vertu de la législation, aux données et informations supplémentaires relevant de SIS II.

définies par le Conseil européen dans le programme de Stockholm, qui indiquent que «Europol devrait devenir le centre névralgique de l'échange d'informations entre les services répressifs des États membres et jouer le rôle de prestataire de services et de plate-forme pour les services répressifs».

Gestion des canaux. Un point de contact unique (PCU) est un «guichet unique» pour la coopération policière internationale, qui fonctionne 24 heures sur 24 et 7 jours sur 7. L'État membre y rassemble son bureau SIRENE, son UNE et ses bureaux centraux nationaux Interpol, ainsi que les points de contact d'autres canaux. La création par chaque État membre d'un PCU (même si ce terme n'a pas toujours été employé) figurait, en 2007, parmi les conclusions de la troisième série de visites d'évaluations mutuelles[28] et était recommandée dans le guide de 2008. La plupart des États membres disposent de services spécifiques pour la coopération policière internationale, mais seuls certains d'entre eux offrent les caractéristiques d'un PCU à part entière. En 2012, le Conseil a invité les États membres à «explorer les possibilités d'établir» un PCU[29]. La Commission irait plus loin: pour améliorer l'ensemble de l'échange d'informations en matière répressive à l'échelle de l'UE, **tous les États membres devraient instaurer des PCU** respectant certaines caractéristiques minimales.

Pour les demandes adressées à un autre État membre, le fait de rassembler les différents canaux au sein d'une structure organisationnelle unique qui suit les règles nationales en matière de choix du canal garantira le bien fondé et la cohérence du choix du canal, ainsi que la qualité des demandes. La qualité est garantie par le fait que les PCU valident les demandes pour confirmer qu'elles sont nécessaires et opportunes. Lorsque les informations ne sont pas échangées par l'intermédiaire d'un PCU (par exemple, par l'intermédiaire de centres de coopération policière et douanière ou des agences nationales qui échangent directement à l'aide de SIENA), la coordination nationale peut être assurée par un PCU. Pour les demandes reçues, les PCU devraient, si la loi l'autorise, avoir un accès direct aux bases de données nationales pour répondre rapidement aux demandes, en particulier dans les délais prévus par l'initiative suédoise. Les règles du manuel SIRENE (par exemple, sur la sécurité, les systèmes de gestion du flux de travail, la qualité des données et la dotation en personnel) pourraient servir de base à une organisation cohérente de tous les canaux. Le partage des ressources, comme le personnel et l'infrastructure, peut contribuer à réduire les coûts ou, pour le moins, à mieux utiliser les ressources.

Les PCU devraient englober toutes les autorités répressives, y compris les services de douanes. Une coopération devrait être établie entre les PCU et les centres nationaux de coordination en matière de surveillance des frontières. Dans la mesure où cela est compatible avec les systèmes juridiques nationaux, des liens devraient être tissés avec les services judiciaires, en particulier lorsque ces derniers dirigent les enquêtes pénales.

De plus en plus de centres de coopération policière et douanière[30] échangent avec succès des informations aux niveaux local et régional. Des conférences annuelles organisées au niveau de l'UE permettent de partager les expériences et de discuter d'approches communes. Bien que le nombre généralement élevé d'échanges ne concerne pas, pour l'essentiel, les formes les plus graves de criminalité et la criminalité organisée, l'un des défis consiste à s'assurer que les informations sur les affaires pertinentes sont transmises au niveau national (PCU) et, s'il y a lieu, à Europol. Dans ce contexte, la Commission attend avec impatience les résultats d'un

[28] 13321/3/07.
[29] Conclusions du Conseil des 7 et 8 juin 2012, 10333/12.
[30] 38 à la fin de l'année 2011.

projet pilote en cours (mené dans le cadre d'une action relative à la stratégie de gestion de l'information) qui utilise SIENA dans un centre de coopération policière et douanière.

La **plateforme d'échange d'informations** est une action relevant de la stratégie de gestion de l'information menée par Europol dans le but d'élaborer un portail commun pour accéder aux canaux et systèmes existants tout en respectant pleinement leurs règles en matière de sécurité et de protection des données. La Commission estime que le fait de faciliter l'utilisation des canaux et des systèmes existants présente des avantages, mais qu'il y a lieu d'évaluer plus avant le rapport coûts-bénéfices d'une plateforme d'échange d'informations, de réfléchir à la source du financement et à la manière dont le projet serait dirigé. Cette évaluation devrait également faire intervenir l'agence IT[31].

Les États membres sont invités à:

- passer par Europol, pour les échanges pour lesquels le canal n'est pas légalement défini, en utilisant SIENA, en tant que canal par défaut, à moins que des raisons particulières n'exigent d'utiliser un autre canal;
- préparer des instructions nationales pour le choix du canal;
- en particulier, après la mise en service de SIS II et la fermeture de SISNET, utiliser le canal Europol et l'outil SIENA pour les échanges en matière de coopération policière qui ont lieu actuellement par l'intermédiaire de SISNET;
- créer, s'il n'existe pas déjà, un point de contact unique (PCU) couvrant tous les canaux principaux, disponible 24 heures sur 24 et 7 jours sur 7 et rassemblant tous les services répressifs, avec un accès aux bases de données nationales;
- veiller à ce que les informations échangées par l'intermédiaire des centres de coopération policière et douanière soient, s'il y a lieu, transmises au niveau national et, le cas échéant, à Europol;
- établir une coopération entre les PCU et les centres nationaux de coordination d'EUROSUR.

Le Conseil est invité à:

- modifier les recommandations au niveau de l'UE de manière à tenir compte des orientations relatives au choix du canal proposées ci-dessus.

La Commission:

- participera aux travaux d'évaluation de la faisabilité d'une plateforme d'échange d'informations.

3.3. Garantir la qualité, la sécurité et la protection des données

Les garanties en matière de protection des données contenues dans les instruments existants doivent être scrupuleusement observées. Dans le cadre de la proposition de la Commission du

[31] Agence européenne pour la gestion opérationnelle des systèmes d'information à grande échelle au sein de l'espace de liberté, de sécurité et de justice.

25 janvier 2012 relative à une directive applicable au traitement national des données à caractère personnel à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière[32], les règles en matière de protection des données contenues dans les instruments existants devront être réexaminées afin d'apprécier la nécessité de les mettre en conformité avec la directive.

Un **niveau élevé de sécurité des données** est nécessaire pour protéger l'intégrité des données à caractère personnel échangées et pour garantir la confiance des États membres dans l'échange d'informations. La solidité d'une chaîne dépend de son maillon le plus faible: les États membres et les agences de l'UE doivent garantir que l'échange de données s'effectue par le biais de réseaux hautement sécurisés. La proposition de directive susmentionnée comporte des règles sur la sécurité des données[33], et il existe, au niveau de l'UE, des règles de sécurité détaillées aux fins de la protection des informations classifiées de l'UE[34].

Un **niveau élevé de qualité des données** est tout aussi important. Dans ce contexte, le «processus de travail», c'est-à-dire la façon dont l'échange d'informations s'effectue dans la pratique, est important. Il s'agira notamment, dans la mesure de ce qui est possible et opportun, d'**automatiser certaines tâches**. Par exemple, formuler une demande d'informations émanant d'un autre État membre exige que des données enregistrées sur un système national soient à nouveau saisies dans l'outil de communication utilisé; une procédure manuelle peut entraîner l'introduction d'erreurs et prend du temps. L'automatisation de ce type de tâches sera rendue possible par **UMF II**[35], une autre action relevant de la stratégie de gestion de l'information. Ce projet financé par l'UE et mené par Europol vise à élaborer une norme fixant le format des messages utilisés pour demander des informations et fournir des réponses. Cela permettrait d'automatiser le transfert de données entre différents systèmes, comme par exemple les systèmes de gestion des dossiers nationaux et SIENA. Outre des économies potentielles ou, à tout le moins, une meilleure utilisation des ressources, il y a un double avantage à ne pas re-saisir manuellement les données. Cela libère du personnel qui peut être affecté aux tâches de validation. Par ailleurs, en réduisant les erreurs de saisie et en facilitant l'échange d'informations dans des formats structurés, on améliore la gestion et la protection des données.

L'automatisation des tâches ne signifie pas que chaque fonctionnaire de police de l'UE doit avoir accès à toutes les informations policières de l'UE. Les échanges doivent se limiter à ceux qui sont nécessaires et opportuns, et leur gestion doit garantir qu'ils restent dans ces limites. **Les recherches automatisées, destinées à surmonter les problèmes de capacité, fonctionnent donc dans le cadre des instruments de l'UE existants en matière d'échange d'informations, sur la base d'un système de concordance/non-concordance** (par exemple, SIS, ADN et empreintes digitales relevant de la décision Prüm) ou se limitent à des types de données strictement définis (par exemple, les données sur l'immatriculation des véhicules relevant de la décision Prüm). Certaines tâches ne peuvent pas et ne doivent pas être automatisées, notamment la validation des demandes et des réponses. Ce point est particulièrement important dans le contexte de l'initiative suédoise, qui exige que les demandes soient justifiées.

Pour finir, l'**interopérabilité** entre les différents systèmes et structures administratives nationaux peut présenter des avantages au niveau de la cohérence des procédures, de la

---

32 COM(2012) 10.

33 Articles 27 à 29 de la proposition.

34 Décision 2011/292/UE du Conseil.

35 **U**niversal **M**essage **F**ormat (format universel pour les messages).

brièveté des temps de réponse, de l'amélioration de la qualité des données et de la simplification de la conception et du développement. Le cadre d'interopérabilité européen[36] recense quatre niveaux d'interopérabilité: technique, sémantique, organisationnel et juridique. Le projet UMF II développera le niveau sémantique[37]. La convergence vers des pratiques communes (PCU, choix du canal) renforcera le niveau organisationnel. Toutefois, les informations ne peuvent effectivement être échangées et utilisées que lorsque la législation l'autorise.

Europol et les États membres sont invités à:

- poursuivre le développement de la norme UMF II.

3.4. Améliorer la formation et la sensibilisation

Pour doter les fonctionnaires des services répressifs des connaissances et des compétences nécessaires à une coopération efficace, la Commission prépare actuellement un programme de formation européenne dans le domaine de la répression. Une analyse a montré que les instruments européens d'échange d'informations pertinents sont abordés lors de la formation initiale dans les services de répression, sans pour autant évaluer la qualité de cette formation. Les fonctionnaires spécialisés, tels que ceux qui travaillent dans les PCU, nécessitent une formation plus approfondie. Les échanges de ces personnels sont également reconnus[38] comme étant bénéfiques et doivent être encouragés.

Les États membres sont invités à:

- veiller à ce que tous les fonctionnaires des services répressifs bénéficient d'une formation appropriée en matière d'échange d'informations transfrontière;
- organiser des échanges de personnel travaillant dans les PCU.

La Commission:

- veillera à ce que le programme de formation européenne dans le domaine de la répression comprenne une formation sur l'échange d'informations transfrontière.

3.5. Financement

L'UE a financé, dans le cadre du fonds «Prévenir et combattre la criminalité» (ISEC), des projets dans le domaine de l'échange d'informations, tels que le projet UMF II (830 000 euros), et la mise en œuvre de la décision Prüm (11,9 millions d'euros). Le fonds sera remplacé en 2014-2020 par un fonds européen pour la sécurité intérieure, dont les projets européens dans le domaine de l'échange d'informations pourront également bénéficier.

Une partie du fonds pour la sécurité intérieure sera administrée par les États membres dans le cadre d'une gestion dite «partagée», conformément aux **programmes pluriannuels**. **Ces programmes devraient tenir compte de certaines priorités nationales en matière**

[36] Communication COM(2010) 744 de la Commission.

[37] Le projet UMF II tient compte d'autres travaux sur la sémantique, comme les modèles de données communs développés dans le cadre du programme de l'UE concernant des solutions d'interopérabilité pour les administrations publiques européennes.

[38] 10333/12.

d'échange d'informations, conformément aux recommandations formulées dans la présente communication. La Commission examinera, en parallèle, la façon dont certaines parties du fonds pour la sécurité intérieure qu'elle gère directement peuvent notamment soutenir des projets pilotes, tels que la poursuite du développement du projet UMF II.

En ce qui concerne les dépenses propres aux États membres, d'autres recommandations (à propos des PCU, du projet UMF II) pourraient, comme indiqué précédemment, contribuer à réduire les coûts ou pour le moins à mieux utiliser les ressources.

Les États membres sont invités à:

- tenir compte de certaines priorités en matière d'échange d'informations dans les programmes pluriannuels nationaux au titre du fonds de l'UE pour la sécurité intérieure de 2014-2020.

La Commission:

- intégrera des règles en matière d'échange d'informations dans son dialogue avec les États membres relatif à la programmation du fonds pour la sécurité intérieure;

- lancera un appel à propositions pour le financement direct (par elle) des projets pilotes pertinents.

3.6. Statistiques

Les statistiques actuelles, si elles sont pertinentes dans certains domaines (par exemple, SIS, SIENA), ne sont pas complètes. De meilleures statistiques permettraient de mieux connaître l'utilisation qui est faite de l'initiative suédoise (pour laquelle seuls les chiffres envoyés par l'intermédiaire de SIENA sont connus) et de la décision Prüm.

Le recueil de statistiques peut toutefois mobiliser des ressources considérables, en particulier s'il ne fait pas partie des tâches habituelles. Les exercices ponctuels sont à éviter. Il convient de privilégier une approche progressive, s'appuyant sur des processus déjà engagés, tels que, comme le décrit le rapport Prüm, le recensement des concordances Prüm utiles aux enquêtes. L'utilisation accrue de SIENA pour les demandes relevant de l'initiative suédoise, recommandée précédemment, conduira à une représentation accrue de ces demandes dans les statistiques de SIENA.

Les États membres sont invités à:

- améliorer les statistiques relatives à la décision Prüm.

4. CONCLUSIONS

L'amélioration de l'échange d'informations transfrontière n'est pas une fin en soi. Elle a pour but de lutter plus efficacement contre la criminalité et donc de réduire le préjudice occasionné aux victimes et à l'économie de l'UE.

L'échange d'informations transfrontière fonctionne bien d'une manière générale et, comme l'illustrent les exemples donnés ci-dessus, contribue grandement à lutter contre la grande criminalité et la criminalité transfrontière dans l'UE. Des améliorations sont toutefois

possibles. La législation qui a été convenue doit être pleinement mise en œuvre, par l'ensemble des États membres. À l'avenir, les États membres devraient en particulier tous converger vers une utilisation plus systématique du canal Europol et concevoir des points de contact uniques (PCU) nationaux complets.

La Commission, pour sa part, continuera à suivre la mise en œuvre et l'utilisation des instruments, à apporter le financement de l'UE et à rassembler les différents éléments indispensables à la cohérence d'ensemble. La Commission ne propose pas ici de nouvel instrument. Si elle y est amenée à l'avenir, elle suivra les principes matériels énoncés dans la communication de 2010, à savoir protéger les droits fondamentaux et garantir la nécessité, la subsidiarité et une gestion rigoureuse des risques.

Des efforts conséquents restent à fournir pour garantir le partage des informations pertinentes au sein d'Europol, ce qui permettrait d'avoir une vue d'ensemble de la criminalité transfrontière à l'échelle de l'Union. La proposition de réforme d'Europol qui sera prochainement présentée par la Commission répondra à ce besoin. Toutefois, l'application des recommandations formulées dans la présente communication en faveur d'une utilisation plus systématique du canal Europol et de son outil de communication sécurisé SIENA permettrait d'ores et déjà de faciliter la transmission d'informations à Europol.

Dans le prolongement de la présente communication, la Commission continuera à travailler avec les États membres au titre de la stratégie de gestion de l'information pour la sécurité intérieure de l'UE, et propose que le Conseil organise un débat annuel au sein de son comité de sécurité intérieure. La Commission invite également le Parlement européen à débattre de ses recommandations, y compris au sein de sa commission spéciale sur la criminalité organisée, la corruption et le blanchiment de capitaux.