Conseil de
l'Union européenne

Bruxelles, le 24 novembre 2014
(OR. en)

15701/1/14
REV 1

JAI 897
DAPIX 175
CRIMORG 109
ENFOPOL 372

NOTE POINT "I/A"

Origine:	Secrétariat général du Conseil
Destinataire:	Comité des représentants permanents/Conseil
Nº doc. préc.:	11153/2/14 REV 2
Objet:	Projet de conclusions du Conseil concernant une stratégie actualisée de gestion de l'information pour la sécurité intérieure de l'UE

1. Le 30 novembre 2009, le Conseil a approuvé des conclusions concernant une stratégie de gestion de l'information pour la sécurité intérieure de l'UE[1]. La stratégie en tant que telle est axée sur le long terme et pourra être étoffée et actualisée au rythme des développements que connaîtra la vision qui la sous-tend. Elle a donc été approuvée par le Conseil en 2009, étant entendu qu'elle devrait faire l'objet d'un réexamen d'ici la fin de 2014.

2. Cette stratégie vise à soutenir, rationaliser et faciliter la gestion de l'information nécessaire à l'échange transfrontière d'informations approprié entre les services répressifs, les services chargés de la gestion des frontières et les services judiciaires s'occupant d'affaires pénales. Elle fournit des orientations sur les moyens de traduire les besoins des utilisateurs en structures et contenu, et énonçait, sous un certain nombre de domaines prioritaires, les objectifs stratégiques à atteindre.

[1] Doc. 16637/09 JAI 873 CATS 131 ASIM 137 JUSTCIV 249 JURINFO 145.

3. La stratégie était complétée par une liste de mesures ou une feuille de route définissant concrètement les objectifs, les processus, les rôles et les délais. Jusqu'ici, trois listes de mesures d'une durée de dix-huit mois chacune ont été établies. Le deuxième rapport intermédiaire sur la mise en œuvre des listes de mesures de la stratégie[2] présente les objectifs atteints ainsi que les résultats obtenus à ce jour.

4. Le groupe "Échange d'informations et protection des données" s'est penché sur l'évaluation et le réexamen de la stratégie lors de ses réunions du 1er juillet et du 23 septembre. Les délégations ont recommandé qu'il soit établi une nette distinction entre la stratégie en tant que telle, sa mise en œuvre au niveau national ou de l'UE et l'établissement d'autres listes de mesures. Il est ressorti des débats que la stratégie était considérée comme un instrument suffisamment solide qui devrait être réaffirmé moyennant quelques actualisations. Toutefois, en ce qui concerne la mise en œuvre de la stratégie au moyen de listes de mesures, les délégations ont demandé que les acteurs concernés se montrent plus participatifs et que l'accent soit mis sur les résultats concrets et sur les questions opérationnelles et de coordination.

5. La présidence a donc suggéré d'élaborer des conclusions du Conseil concernant une stratégie actualisée de gestion de l'information pour la sécurité intérieure de l'UE qui tiennent compte des travaux réalisés dans ce domaine au cours des cinq dernières années.

6. Le groupe "Échange d'informations et protection des données" a examiné la proposition et est parvenu à un accord sur le projet de conclusions du Conseil lors de sa réunion du 19 novembre, le Royaume-Uni ayant émis une réserve d'examen. Cette réserve a été levée le 24 novembre.

7. Il est donc demandé au Coreper d'inviter le Conseil à approuver le projet de conclusions du Conseil sur une stratégie actualisée de gestion de l'information pour la sécurité intérieure de l'UE, dont le texte figure à l'annexe de la présente note.

---

[2] Doc. 13032/14 JAI 663 DAPIX 111 CRIMORG 76 ENFOPOL 260.

ANNEXE

PROJET DE CONCLUSIONS DU CONSEIL

CONCERNANT UNE STRATÉGIE ACTUALISÉE DE GESTION DE L'INFORMATION

POUR LA SÉCURITÉ INTÉRIEURE DE L'UE

LE CONSEIL DE L'UNION EUROPÉENNE,

RAPPELANT

– le programme de La Haye visant à renforcer la liberté, la sécurité et la justice dans l'Union européenne[3], et en particulier son point 2.1 qui invite à améliorer l'échange d'informations afin de lutter contre la criminalité et consacre à cet effet le principe de disponibilité pour l'échange transfrontière d'informations et précise que "les méthodes utilisées pour échanger les informations devraient exploiter pleinement les nouvelles technologies et être adaptées à chaque type d'information";

– le fait que le Conseil européen relève dans le programme de Stockholm que le développement de la gestion et des échanges d'informations doit se faire de manière cohérente et structurée et qu'il invite à cet effet le Conseil à adopter et à mettre en œuvre une stratégie de l'UE en matière de gestion de l'information reposant sur un développement obéissant à des considérations pragmatiques, un solide système de protection des données, l'interopérabilité des systèmes d'information et une rationalisation des outils, ainsi qu'une coordination, une convergence et une cohérence générales;

– les conclusions du Conseil européen des 26 et 27 juin 2014[4], notamment leur point I sur la liberté, la sécurité et la justice, où il est précisé ce qui suit: "Dans le combat qu'elle mène contre la criminalité et le terrorisme, l'Union devrait mobiliser tous les instruments de la coopération policière et judiciaire pour soutenir les autorités nationales, Europol et Eurojust jouant un rôle accru de coordination, notamment par l'amélioration des échanges d'informations transfrontières, y compris en ce qui concerne les casiers judiciaires.";

---

[3] Doc. 16504/04 JAI 559.

[4] Doc. EUCO 79/14 CO EUR 4 CONCL 2.

COMPTE TENU

– des conclusions du Conseil sur l'accélération de la mise en œuvre des "décisions Prüm" après l'échéance du 26 août 2011[5];
– des conclusions du Conseil sur la mise en œuvre de la décision-cadre 2006/960/JAI du Conseil ("décision-cadre suédoise")[6];
– des conclusions du Conseil intitulées "Améliorer encore l'efficacité de l'échange transfrontalier d'informations en matière répressive"[7];
– de la communication de la Commission européenne du 7 décembre 2012 sur le modèle européen d'échange d'informations (EIXM) et des conclusions du Conseil correspondantes[8], en particulier en ce qui concerne la tâche consistant à poursuivre la discussion sur l'automatisation des processus d'échange de données existants dans le cadre de la stratégie de gestion de l'information;

SOULIGNANT

– que l'objectif stratégique de la future stratégie de sécurité intérieure de l'UE renouvelée qui consiste à renforcer une approche globale et cohérente dans la lutte contre la criminalité transnationale et le terrorisme, notamment par l'accès à l'information, la disponibilité et l'échange d'informations, sera soutenu en visant davantage l'interopérabilité des systèmes ainsi qu'en améliorant et en simplifiant les outils existants dans le domaine de l'échange transfrontière d'informations en matière répressive, en conformité avec la législation existante en matière de protection des données;

---

5 Doc. 17762/11 JAI 892 DAPIX 163 CRIMORG 233 ENFOPOL 441 ENFOCUSTOM 160.
6 Doc. 15277/11 JAI 714 DAPIX 129 CRIMORG 176 ENFOPOL 346 ENFOCUSTOM 115.COMIX 719.
7 Doc. 10333/12 JAI 356 DAPIX 65 CRIMORG 57 ENFOCUSTOM 43 ENFOPOL 147.
8 Doc. 9811/13 JAI 400 DAPIX 82 CRIMORG 76 ENFOCUSTOM 88 ENFOPOL 146.

TENANT COMPTE DE CE QUI SUIT

– les conclusions du Conseil concernant une stratégie de gestion de l'information pour la sécurité intérieure de l'UE[9] ont été approuvées par le Conseil, étant entendu que la stratégie est axée sur le long terme et qu'elle pourra être étoffée et actualisée, et qu'elle devrait donc faire l'objet d'un réexamen d'ici la fin de 2014;

– la stratégie a été complétée à ce jour par trois listes de mesures d'une durée de dix-huit mois chacune, avec des objectifs concrets, des processus, des rôles et des délais bien définis;

– la stratégie a été considérée comme un instrument suffisamment solide qui devrait être réaffirmé moyennant quelques actualisations;

– compte tenu des objectifs et des résultats présentés dans le deuxième rapport intermédiaire sur la mise en œuvre des listes de mesures de la stratégie[10], la poursuite de la mise en œuvre de la stratégie requiert que les acteurs concernés à la fois au niveau national et au niveau de l'UE se montrent plus participatifs et que l'accent soit mis sur les résultats concrets et sur les questions opérationnelles et de coordination;

– l'Agence européenne pour la gestion opérationnelle des systèmes d'information à grande échelle (euLISA) a entamé ses activités le 1er décembre 2012 et vise à fournir des solutions viables à long terme pour la gestion des systèmes d'information à grande échelle et à devenir progressivement un centre d'excellence;

– le volume des échanges transfrontières d'informations a augmenté ces dernières années et les États membres s'attendent à ce que cette tendance perdure, ce qui peut être atténué par l'utilisation efficace de la technologie moderne, comme l'automatisation, ainsi que la rationalisation des tâches courantes et des flux de données;

[9] Doc. 16637/09 JAI 873 CATS 131 ASIM 137 JUSTCIV 249 JURINFO 145.
[10] Doc. 13032/14 JAI 663 DAPIX 111 CRIMORG 76 ENFOPOL 260.

CONSCIENT DE CE QUI SUIT

- un échange transfrontière effectif et sûr des informations[11] est une condition préalable pour atteindre les objectifs de sécurité intérieure dans l'Union européenne;

- les tâches relatives à la sécurité intérieure sont réparties entre une série d'autorités (les "utilisateurs") selon les structures, les compétences et le cadre juridique de chacun, et cette répartition diffère d'un État membre à un autre;

- la gestion de l'information entre les différents secteurs offre l'approche multidisciplinaire nécessaire pour développer un espace de liberté, de sécurité et de justice, et notamment la possibilité d'accroître l'échange d'informations et la coopération entre toutes les parties concernées afin de rendre plus efficace la lutte contre la criminalité transnationale;

- en ce qui concerne l'importante fragmentation de l'échange transfrontière d'informations, les États membres ont mis en évidence à plusieurs reprises le caractère prioritaire d'une mise en œuvre cohérente et consolidée des instruments et arrangements existants par rapport au lancement de nouvelles initiatives;

- le besoin d'une approche transfrontière cohérente et effective est accentué par la mobilité croissante des citoyens, par la nature de plus en plus complexe de la criminalité et donc des mesures que doit prendre l'UE pour y faire face, ainsi que par la nécessité pour l'UE et les États membres d'exploiter de manière optimale leurs ressources;

- il convient de trouver un équilibre approprié entre le respect de la vie privée des citoyens et leurs attentes en matière de sécurité;

---

[11] *On entend ici par "informations" les informations et les renseignements requis par les autorités nationales compétentes et mis à leur disposition en application du cadre réglementaire pertinent dans le but d'améliorer la sécurité intérieure de l'UE au bénéfice de ses citoyens.*

SOULIGNANT CE QUI SUIT

- la stratégie vise à fournir des orientations sur la manière d'assurer une communication des informations qui tienne compte tant des besoins des utilisateurs que des droits des personnes concernées;

- elle vise à définir les conditions préalables du développement et de la gestion des TI, qui doivent avoir un caractère professionnel, être axés sur les activités et être rentables;

- elle a pour objet d'indiquer la voie à suivre pour atteindre un échange structuré des informations et constitue une base pour améliorer les processus décisionnels et la gouvernance;

SALUANT ET ENCOURAGEANT

– les travaux sur les modalités technologiques de l'échange transfrontière d'informations et, en particulier, les progrès réalisés en ce qui concerne le format universel pour les messages (UMF) en vue de renforcer l'échange transfrontière d'informations structuré; et
– le développement plus poussé du format universel pour les messages comme l'un des éléments clés de l'architecture d'échange d'informations de l'UE, tel qu'énoncé dans les conclusions finales de la conférence UMF 2[12],
– les travaux en cours sur l'interopérabilité et une plus grande synergie des systèmes, ainsi que sur l'automatisation de l'échange d'informations;

DÉCIDE

1. de réaffirmer et de poursuivre la mise en œuvre de la stratégie de gestion de l'information afin de soutenir, de rationaliser et de faciliter une gestion de l'information qui

   a) repose sur les principes suivants:

[12] Doc. 10158/14 DAPIX 69.

– la gestion de l'information dans l'espace de liberté, de sécurité et de justice est un outil essentiel pour atteindre les objectifs consistant à renforcer la sécurité intérieure de l'UE et à protéger ses citoyens;
– l'échange transfrontière d'informations en matière répressive doit parvenir à un équilibre entre les besoins des utilisateurs et la protection des droits fondamentaux des citoyens;
– les priorités définies pour la gestion et l'échange de l'information doivent correspondre aux priorités politiques, stratégiques et opérationnelles et à la vision qu'ont les utilisateurs de la manière de mettre en œuvre les objectifs susmentionnés;
– la protection, la sécurité et la qualité des données doivent toujours être respectées;
– le développement et la gestion des TI doivent avoir un caractère professionnel, être axés sur les activités et être rentables;
– la gestion de l'information est définie d'un point de vue fonctionnel, c'est-à-dire qu'elle est fonction de la tâche à exécuter et non des compétences ou de l'organisation;
– la gestion de l'information doit offrir l'approche multidisciplinaire nécessaire pour développer un espace de liberté, de sécurité et de justice;

b) comprend des domaines prioritaires regroupés sous les intitulés suivants et plus amplement décrits en annexe:

I. Besoins et exigences

• Les besoins, les exigences et la valeur ajoutée sont évalués avant tout développement.

• Tout développement est conforme aux flux de données autorisés dans le domaine de l'action répressive et aux formats du renseignement en matière pénale.

• Tout développement répond à la fois aux exigences de la protection des données et aux besoins opérationnels des utilisateurs.

II. Interopérabilité et rentabilité

• L'interopérabilité et la coordination sont assurées au niveau des activités des utilisateurs et des solutions techniques.

• La réutilisation est la règle.

III. Processus de décision et de développement

- Les États membres sont associés au processus dès le tout début.
- Les responsabilités sont clairement établies pour les différentes parties du processus, garantissant compétence, qualité et efficacité.

IV. Approche multidisciplinaire

- La coordination multidisciplinaire est assurée au sein du domaine JAI;

2. de prendre les mesures nécessaires pour mettre au point et actualiser, au besoin, de futurs plans d'action détaillés assortis de calendriers réalistes et axés sur les résultats concrets en vue d'atteindre les buts et objectifs globaux de la stratégie;

INVITE

– les instances préparatoires du Conseil à se pencher sur les questions liées à l'échange d'informations et au développement des TI pour poursuivre la mise en œuvre de la stratégie;
– les agents de l'UE, les représentants des États membres et les experts des structures et agences de l'UE à tenir compte de la stratégie dans leurs travaux de préparation des décisions, notamment en ce qui concerne l'échange d'informations au niveau bilatéral ou régional et avec des pays ou organisations tiers, et lors de l'élaboration et de l'exploitation de programmes et projets axés sur l'échange d'informations et le développement des TI;
– les États membres à soutenir les efforts communs déployés au niveau de l'UE en adoptant la stratégie au niveau national en tant que ligne directrice pour les responsables politiques et autres décideurs au sein de leurs autorités compétentes lorsqu'ils traitent de questions liées à l'échange international d'informations et au développement des TI ou de questions concernées par ces aspects (y compris la "gestion nationale" et les relations avec des pays ou organisations tiers);
– la Commission à appliquer la méthodologie arrêtée dans les présentes conclusions lorsqu'elle poursuivra l'élaboration de son modèle européen d'échange d'informations et à garantir un financement approprié pour les mesures nécessaires à la poursuite de la mise en œuvre de la stratégie;
- la Commission à examiner la possibilité de consolider et d'accroître l'efficacité de la législation existante en matière d'échange d'informations en matière répressive.

I. BESOINS ET EXIGENCES

1. Les besoins, les exigences et la valeur ajoutée sont évalués avant tout développement.

Ce domaine prioritaire met en évidence l'exigence de procéder à une évaluation de la valeur ajoutée avant d'instaurer un nouvel échange d'informations. Il reflète aussi le principe de disponibilité des informations en fonction de la finalité, de la nécessité et de la proportionnalité.

Il faudra donc évaluer les besoins des utilisateurs et les exigences professionnelles et juridiques pour la coopération concernée, y compris la manière dont les solutions seront utilisées ainsi que leur utilité pour renforcer la coopération opérationnelle et les méthodes de travail existantes.

Par conséquent, le développement sera fondé et axé sur les besoins et les exigences des autorités concernées. Une évaluation de l'utilité (y compris une analyse coûts-avantages) contribuera aussi à fixer les priorités pour le développement.

Implications:

Lorsque des initiatives relatives à des échanges d'informations ou à des solutions techniques sont présentées, il faut y associer les utilisateurs finaux et les cadres dans les différents domaines. Sans leur aide, il est impossible d'évaluer l'importance et la valeur d'une initiative. Cette participation sera aussi utile lorsqu'il s'agira de préciser l'équilibre à trouver entre la protection des données et les besoins des utilisateurs.

Il faut subordonner les idées ou les discussions sur les solutions techniques à l'analyse des besoins et des exigences.

Les travaux relatifs aux instruments législatifs et/ou aux études préalables pour les solutions techniques ne devraient pas commencer avant que les exigences des utilisateurs ne soient établies et justifiées.
Toute initiative dans le domaine de l'échange d'informations doit reposer sur une analyse approfondie des solutions existant au niveau de l'UE et dans les États membres, sur la définition des besoins, des exigences et de la valeur ajoutée et sur une évaluation de l'incidence juridique, technique et financière de la nouvelle initiative.

Des critères d'évaluation clairs, étayés par des programmes d'évaluation systématique, devraient être établis.
L'évaluation de l'utilité de développer, par exemple, certains types d'informations devrait découler d'un processus de définition des priorités stratégiques.

2. Tout développement est conforme aux flux de données autorisés et aux formats du renseignement en matière pénale.

L'amélioration de l'échange d'informations dépend étroitement de la contribution apportée par les solutions informatiques. Pour que les TI soient utiles à cet échange, il faut qu'elles soutiennent les activités quotidiennes (processus) de la coopération internationale en matière répressive.

Ces activités doivent permettre de procéder à des échanges rapides, efficaces, simples et économiques d'informations et de renseignements en matière pénale. Les flux de données doivent dès lors être décrits, connus et accessibles. Ils devraient faire partie intégrante des travaux de développement et d'acquisition des systèmes. Cela entraînera une meilleure gestion et une meilleure justification du développement, et ce sont les besoins de la coopération internationale en matière répressive qui orienteront le développement.

Implications:

Les travaux consacrés à la vision commune des besoins devraient être complétés par des analyses des exigences fondamentales, effectuées avec et par les autorités nationales.

Une "carte de l'information" devrait fournir en continu une vue d'ensemble des activités quotidiennes et des flux d'informations correspondants dans le cadre de la coopération internationale, de manière à définir sur cette base les niveaux de concertation auxquels une harmonisation est nécessaire.

3. Tout développement répond à la fois aux exigences de la protection des données et aux besoins opérationnels des utilisateurs.

La coopération à mener en vue d'assurer la sécurité intérieure de l'UE induit des exigences élevées en matière de protection des données et en termes de sécurité des données. Il convient d'assurer à la fois le respect de la vie privée et la sécurité des activités, tout en tenant compte des besoins des utilisateurs en matière d'exploitation et de partage des informations.

Un niveau élevé de sécurité protégera à la fois les intérêts des utilisateurs et la vie privée des citoyens, sans compromettre la disponibilité des informations, de sorte que des informations exactes seront mises à la disposition des utilisateurs autorisés d'une manière identifiable, si cela est nécessaire et autorisé par la législation en vigueur. Un recours adéquat aux technologies modernes, mais aussi l'adaptation des activités quotidiennes et des mesures de protection des données, faciliteront cet équilibre. Une plus grande confiance entre autorités compétentes dans ces domaines est importante pour parvenir à une attitude de partage des données par défaut.

Implications:

Les exigences légales concernant la protection des données à caractère personnel et l'établissement de normes de sécurité doivent être évaluées en même temps que les besoins des utilisateurs à l'égard de l'exploitation et de l'échange des informations, de sorte que les niveaux adéquats de normes de sécurité du point de vue opérationnel et technique soient garantis pour l'échange d'informations et les systèmes TI.

La collecte des données doit être bien ciblée pour protéger la vie privée et éviter que les autorités compétentes ne soient submergées d'informations, ainsi que pour permettre un contrôle efficace des informations.

La sécurité des données est un prérequis de la protection des données et doit être assurée par des moyens organisationnels comme techniques.

Les différents outils, tels que les applications et les outils de soutien, doivent être rationalisés en vue de simplifier le travail des autorités compétentes et des utilisateurs finaux, ce qui réduira le risque de causer des dommages, tout comme le fera une formation consacrée aux outils disponibles et à leur utilisation.

Des mesures adéquates de protection des données doivent prévoir des contrôles opérationnels appropriés et réguliers et garantir que tout manquement fera effectivement l'objet de sanctions adaptées.

Des mécanismes d'évaluation et de contrôle systématiques devraient être élaborés pour évaluer la qualité et l'incidence des mesures de protection des données.

II. INTEROPÉRABILITÉ ET RENTABILITÉ

4. L'interopérabilité et la coordination sont assurées au niveau des activités des utilisateurs et des solutions techniques.

L'interopérabilité concerne de nombreux niveaux, notamment juridique, sémantique, opérationnel et technique. Elle est à la fois une condition préalable et un moyen pour que l'échange d'informations soit efficace. Des solutions et des capacités interopérables reposent sur des initiatives et des propositions qui partent des besoins et des exigences des utilisateurs.

Techniquement, les solutions TI et leurs composantes devraient respecter des normes et des principes définis d'un commun accord. Des solutions standard devraient être utilisées et leur nombre limité.

Leur utilisation donnera davantage de cohérence au développement des solutions et à leur gestion.

Cela favorisera aussi l'interopérabilité et la coordination entre les systèmes. Ainsi, les solutions existantes seront mieux et davantage utilisées, et les systèmes TI seront à même de supporter de plus grandes parties des activités. Il sera moins nécessaire d'avoir recours à un double stockage et à un double enregistrement, et le soutien TI deviendra plus convivial. Grâce à l'application de normes définies d'un commun accord, l'échange d'informations peut être pris en charge par plusieurs fournisseurs et non par quelques-uns seulement, ce qui réduit la dépendance à des fournisseurs particuliers. À long terme, cela réduira également le coût d'adaptation dans les États membres.

Implications:

La "carte de l'information" devrait comprendre un aperçu comparatif de la situation juridique de l'UE et des États membres dans le domaine de l'échange d'informations.

La stratégie européenne en matière d'interopérabilité [proposée] devrait être appliquée.

Les fonctions actuelles d'accréditation ou de normalisation, définies d'un commun accord, devraient être utilisées.

Il faudrait identifier les outils d'intégration, comme des technologies et capacités normalisées, qui facilitent l'intégration et sont conçus pour assurer sécurité, modularité et performance.

Les mesures de protection des données devraient être coordonnées au niveau de l'UE et au niveau national ainsi qu'entre ces niveaux.

5. La réutilisation est la règle.

Le développement implique des coûts élevés et des investissements considérables, mais aussi des frais à long terme de gestion, de maintenance et d'assistance. Généralement, seule une petite partie de l'ensemble des frais sert à la phase de développement. Cela ne concerne pas que le développement technique; il s'agit également de ne pas créer de nouvelles bases juridiques ou modalités pratiques, si celles qui existent peuvent être utilisées ou développées.

Par conséquent, le partage et la réutilisation des solutions viables doivent être une priorité du développement et des améliorations techniques. La réutilisation permet d'éviter les solutions parallèles et de poursuivre le développement des instruments et systèmes existants, de les intégrer davantage et d'accroître leur utilité. Elle entraînera une exploitation accrue des investissements déjà réalisés et une diminution du besoin d'en réaliser de nouveaux. Le temps nécessaire au développement sera également d'autant moins long que le nombre de composantes déjà disponibles sera important.

Pour que la réutilisation soit efficace, il est nécessaire de disposer d'une "carte de l'information" qui fournisse une vue d'ensemble des flux d'informations existants, des fonctions et des composantes. L'utilisation ou la réutilisation efficace des solutions performantes nécessite aussi un processus d'évaluation constant et un mécanisme de suivi permettant d'évaluer la manière dont fonctionne l'échange d'informations.

Implications:

La "carte de l'information" devrait inclure les flux d'informations, les fonctions et les solutions.

Il faut présenter un mécanisme d'évaluation concret, utile et économe en ressources, qui devrait être fonction des objectifs poursuivis et non des compétences et qui ne devrait pas se limiter à certains instruments (juridiques); il convient de veiller à ce que les leçons tirées de l'évaluation puissent être appliquées.

Pour évaluer l'impact de ses travaux, l'UE doit créer des outils qui lui permettent de mesurer non seulement l'activité criminelle mais aussi l'incidence de ses efforts en matière de lutte contre la criminalité.

Il faudrait élaborer une méthode pour partager et réutiliser les solutions viables en tenant compte des pratiques mises en œuvre au sein de l'UE mais aussi dans les pays tiers.

Une évaluation approfondie des instruments existants utilisés pour l'échange d'informations devrait être effectuée pour déterminer leur efficacité afin de permettre une rationalisation, et ce certainement avant d'entamer le développement de nouveaux outils.

III. PROCESSUS DE DÉCISION ET DE DÉVELOPPEMENT

6. Les États membres sont associés au processus dès le tout début.

Les décisions prises au niveau de l'UE concernant la coopération, l'échange d'informations et le développement des TI ont des incidences notables, dans une perspective tant de court terme que de cycle de vie, sur les processus, structures, investissements et budgets relatifs aux activités des États membres. Un résultat final totalement opérationnel demande une coordination intensive au niveau national, ainsi qu'une réciprocité et une interaction entre le niveau national et celui de l'UE.

Les autorités des États membres qui sont responsables de la mise en œuvre, au niveau national, des flux de données, méthodes et développements doivent être associées dès le début aux processus de développement au niveau européen. Pour pouvoir y contribuer pleinement, les États membres devraient améliorer leur propre interopérabilité, au niveau des activités comme sur le plan technique, et arrêter leurs propres processus de développement.

Implications:

Les stratégies ou politiques nationales de gestion de l'information et celles de l'UE devraient être cohérentes.

Les utilisateurs finaux et les principales parties prenantes devraient être associés au niveau national et à celui de l'UE.

Les autorités des États membres doivent définir et mettre au point leurs propres processus de développement.

7. Les responsabilités sont clairement établies pour les différentes parties du processus, garantissant compétence, qualité et efficacité.

Pour mieux guider le processus de développement, il faut préciser les rôles et les responsabilités de ses acteurs. Des compétences particulières sont nécessaires dans différents domaines, comme l'architecture opérationnelle et technique, les méthodes et les modèles, la gestion, les finances et le contrôle. Les discussions sur les solutions (techniques) doivent correspondre au niveau de juste compétence en termes techniques et d'architecture. Les décisions sur les niveaux de gestion et d'action doivent porter sur les questions correspondant à ces niveaux.

Par conséquent, il faut définir les rôles et les responsabilités et créer des structures pour garantir que toutes les parties concernées interviennent au bon niveau et au bon stade du processus, mais également pour garantir une coordination et une cohérence globales.

Implications:

Il faut définir et organiser les rôles et les compétences aux différents niveaux (au sein des autorités nationales, des institutions, instances et agences de l'UE, existantes ou envisagées, etc.).

Il faut définir ou créer des fonctions pour préparer les décisions stratégiques sur la gestion de l'information et le développement des TI.

Il faut mettre en place des fonctions pour la gestion, le développement et l'évaluation des solutions (en termes opérationnels et techniques).

IV. APPROCHE MULTIDISCIPLINAIRE

8. La coordination multidisciplinaire est assurée.

La stratégie de gestion de l'information actuelle vise à soutenir, rationaliser et faciliter la gestion de l'information dont les autorités compétentes ont besoin pour assurer la sécurité intérieure de l'UE. Dans la pratique, les autorités concernées seront essentiellement les services répressifs et les services judiciaires s'occupant d'affaires pénales mais l'échange d'informations avec d'autres autorités et d'autres sources est également nécessaire. La stratégie de gestion de l'information fait sienne et suit cette approche multidisciplinaire pour atteindre les objectifs susmentionnés et faciliter le transfert et la réutilisation des informations, indépendamment de l'instance qui détient ces dernières. La technologie moderne permet d'atteindre le niveau de disponibilité voulu, qui peut à son tour réduire les perturbations et les réenregistrements manuels et augmenter la qualité des informations. Elle permet aussi de maintenir ou de relever le niveau de protection des données, y compris la sécurité des données.

La stratégie vise à faciliter, d'un point de vue fonctionnel et technique, l'échange d'informations entre autorités compétentes si cela est légalement prévu. Dès lors, elle préconise et fournit des moyens d'assurer l'interopérabilité. Elle ne crée pas en soi de liens entre différentes bases de données, pas plus qu'elle ne prévoit des types particuliers d'échange de données, mais elle garantit que, s'il existe des besoins opérationnels et une base juridique, la solution la plus simple, la plus facilement identifiable et la plus rentable sera trouvée.

Cela signifie que les efforts nécessaires pour parvenir à l'interopérabilité nécessitent une interaction entre l'ensemble des autorités et organisations concernées. Ces autorités et organisations seront fonction du besoin particulier auquel il est répondu. La méthodologie exposée dans la présente stratégie et en particulier les domaines prioritaires 1 à 3 permettront de faire en sorte que l'interopérabilité soit assurée en tant que de besoin et de façon proportionnelle au niveau et au-delà des autorités directement responsables de la sécurité intérieure de l'UE, mais aussi qu'elle soit limitée à ces cas.

Implications:

Il ne faut pas que des questions de compétence fassent obstacle à l'échange d'informations (reconnaissance mutuelle des différentes structures nationales).

Le soutien et la normalisation des TI (y compris les principes d'architecture et les modèles d'informations ou de données) doivent être aussi horizontaux que possible et reposer sur des principes communs et une coordination.

Les mesures de protection des données et de sécurité des données devraient être coordonnées entre le niveau de l'UE et celui des États membres.

Une analyse d'impact intersystèmes devrait être prise en compte dans le cadre de cette approche multidisciplinaire.