CONSEIL DE L'UNION EUROPÉENNE

Bruxelles, le 25 novembre 2009 (26.11)
(OR. en)

16637/09

JAI 873
CATS 131
ASIM 137
JUSTCIV 249
JURINFO 145

TRADUCTION NON RÉVISÉE

NOTE POINT "I/A"

du:	Secrétariat général
au:	Coreper/Conseil
n° doc. préc.	15857/09 JAI 825 CATS 121 ASIM 127 JUSTCIV 237 JURINFO 142
Objet:	Projet de conclusions du Conseil concernant une stratégie de gestion de l'information pour la sécurité intérieure de l'UE

1. Le 26 juin 2009, la présidence a présenté au groupe ad hoc sur l'échange d'informations une proposition de stratégie de gestion de l'information. L'objectif de cette stratégie consiste non pas à définir le type d'informations qui devraient être stockées et/ou échangées mais plutôt à fournir une méthodologie (le "comment") permettant de s'assurer que les décisions concernant la nécessité de gérer et d'échanger des données et les décisions relatives aux modes de gestion et d'échange de ces données soient prises de façon cohérente, professionnelle, efficace, rentable, responsable et compréhensible pour les citoyens et les utilisateurs professionnels. Il ne s'agit pas d'un texte juridiquement contraignant.
   Associée aux priorités de l'UE en matière de justice et d'affaires intérieures, et notamment dans le domaine de la sécurité intérieure[1] (le "quoi"), la stratégie de gestion de l'information permettra aux autorités compétentes de mettre en œuvre de manière efficace les évolutions que connaîtra la politique relative à l'échange d'informations.

[1] Un État membre peut décider d'appliquer cette stratégie en adoptant une approche graduelle, par exemple en limitant son application à des secteurs spécifiques de la sécurité intérieure, tels que la répression et la coopération judiciaire en matière pénale. Lorsque cet État membre a constaté que l'approche concernant la stratégie devrait également s'appliquer à d'autres secteurs, il peut décider d'élargir son application.

2. La stratégie est le document central et est par essence axée sur le long terme. Elle pourra être étoffée et mise à jour au rythme des développements ou des changements que connaîtra la vision des choses qui la sous-tend, et elle devrait faire l'objet d'un réexamen pour la fin de 2014. La stratégie de gestion de l'information sera complétée par une liste de mesures ou une feuille de route définissant concrètement les objectifs, les processus, les rôles et les délais.

3. Le groupe ad hoc sur l'échange d'informations a examiné la proposition en détail lors de ses réunions des 7 et 13 juillet, des 26 et 27 septembre et des 15 et 26 octobre; il est parvenu à un accord général sur le texte, abstraction faite de quelques réserves sur le champ d'application du document. Le comité de l'article 36 a examiné la proposition lors de sa réunion des 10 et 11 novembre 2009 et a approuvé le projet de conclusions du Conseil, des réserves ayant néanmoins été émises par CZ, DE, AT et LT.

4. Le Coreper a examiné le projet de conclusions du Conseil lors de sa réunion du 20 novembre 2009 et a invité les délégations concernées à lever leur réserve, ce qu'elles ont fait à la suite de la réunion.

5. **Le Coreper est par conséquent invité à demander au Conseil d'approuver le projet de conclusions du Conseil concernant une stratégie de gestion de l'information pour la sécurité intérieure de l'UE, figurant en annexe.**

6. À la demande de la délégation DE, la déclaration suivante sera inscrite au procès-verbal du Conseil approuvant les conclusions du Conseil:

L'Allemagne soutient et approuve pleinement l'idée énoncée dans le programme de La Haye (doc. 16054/04, partie III, point 2.1) et le plan d'action de La Haye (doc. 9778/2/05 REV 2, point 3.1, lettre k)) en vue d'adopter et de mettre en œuvre une stratégie de l'UE en matière de gestion de l'information. Par conséquent, l'Allemagne soutient et approuve les conclusions du Conseil concernant une stratégie de gestion de l'information adoptées ce jour en ce qui concerne le partage transfrontalier d'informations entre les autorités répressives et judiciaires s'occupant d'affaires pénales dans le cadre juridique existant 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[2], et en particulier son point 2.1 qui invite à améliorer l'échange des informations afin de lutter contre la criminalité et consacre à cet effet le principe de disponibilité,

– le plan d'action du Conseil et de la Commission mettant en œuvre 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 3.1 k), qui invite à définir une politique en vue d'une approche cohérente du développement des technologies de l'information (TI) à l'appui de la collecte, du stockage, du traitement, de l'analyse et de l'échange d'informations,

– le rapport du groupe des ministres sur l'avenir de la politique intérieure ("Groupe du futur"), recommandant la mise en place d'une "stratégie de gestion de l'information" de l'UE pour remédier à la situation actuelle, caractérisée par "un éventail d'instruments et de dispositifs d'information peu cohérents et coordonnés" qui a "induit des coûts et retards au détriment du travail opérationnel", cette stratégie devant dès lors "dépasser l'approche cas par cas et viser une gestion holistique et objective de l'information policière",

– les conclusions du Conseil sur le principe de convergence et la structuration de la sécurité intérieure[4] et la suite à donner aux résultats de la réunion informelle des ministres JAI sur la question des nouvelles technologies et de la sécurité[5],

---

2 Doc. 16504/04 JAI 559.
3 Doc. 9778/2/05 REV 2 JAI 207.
4 Doc. 14069/08 JAI 514 CATS 78.
5 Doc. 10143/09 JAI 324 CATS 55 ASIM 54 ENFOPOL 145 CRIMORG 85.

– la communication de la Commission européenne du 10 juin 2009 intitulée "Un espace de liberté, de sécurité et de justice au service des citoyens" (COM(2009) 262), dans laquelle il est indiqué que la sécurité dans l'Union repose sur des mécanismes performants d'échanges d'informations entre les autorités nationales et les acteurs européens,

– 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,

SE FONDANT SUR

– les travaux des Amis de la présidence[6] sur les modalités techniques de la mise en œuvre du principe de disponibilité,

– la proposition de conclusions[7] du Conseil sur la définition d'une politique pour une approche cohérente du développement des technologies de l'information,

– les conclusions des conférences[8] COPE-2007, COPE-2008 et COPE-2009 et la "vision commune des besoins" (Common Requirements Vision)[9],

---

6 Doc. 13558/1/05 REV 1.
7 Doc. 15478/05 CRIMORG 152 CATS 87 (en anglais uniquement).
8 Doc. 10063/07 CATS 70, 13592/08 CATS 74 et 14033/09 CATS 99 (en anglais uniquement).
9 Doc. 7758/08 CATS 21 (en anglais uniquement).

CONSCIENT DE CE QUI SUIT

un échange transnational effectif et sûr des informations[10] est une condition préalable pour atteindre les objectifs de sécurité intérieure dans l'Union européenne,

il faut pour cela que les bonnes personnes puissent disposer des bonnes informations au bon moment et au bon endroit. Les tâches relatives à la sécurité intérieure sont réparties entre une série d'autorités (les "utilisateurs") et cette répartition diffère d'un État membre à un autre, selon les structures, les compétences et le cadre juridique de chacun. Dans le passé, les décisions relatives à l'échange d'informations ont trop souvent été fonction de motifs organisationnels, rendant impossibles ces différences structurelles entre États membres et donnant lieu à des exigences inutilement compliquées pour l'échange d'informations,

le programme de La Haye a établi le principe de disponibilité comme pierre d'angle de l'échange d'informations dans l'UE et a précisé que, à cette fin, "les méthodes utilisées pour échanger les informations devraient exploiter pleinement les nouvelles technologies et être adaptées à chaque type d'information".
En conséquence, afin de promouvoir les échanges entre États membres et en faciliter les modalités pratiques, les informations voulues devraient être disponibles sous une forme appropriée, de sorte que les décisions nationales devraient tenir compte des politiques de l'UE. Par ailleurs, les États membres et les autorités intervenantes doivent avoir grandement confiance en la manière dont chacun gère les informations de l'autre.
Le principe de disponibilité exige également que les attentes des citoyens en matière de protection de la vie privée soient mises en balance avec leurs attentes en matière de sécurité,

compte tenu de la panoplie d'instruments existant en matière d'échange transnational d'informations, les États membres ont fait état, à plusieurs occasions, d'un besoin de cohérence et de structuration et de la nécessité de mettre en œuvre les instruments et accords existants plutôt que de lancer de nouvelles initiatives. Cela montre qu'il est nécessaire de professionnaliser et de rationaliser la gestion de l'information, y compris la collecte, le stockage, le traitement, l'analyse et l'échange,

---

[10] On entend ici par "informations" les informations et les renseignements en matière pénale 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.

ce besoin de cohérence et de professionnalisation 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,

la stratégie de gestion de l'information 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, abstraction faite des responsabilités des États membres relatives à la protection de leur sécurité nationale. Les autorités concernées seront essentiellement les services répressifs, les services chargés de la gestion des frontières et les services judiciaires s'occupant d'affaires pénales. Toutefois, la nécessité d'échanger des informations avec d'autres autorités et sources sera aussi prise en compte,

il faut clairement opérer une distinction entre les outils méthodologiques utilisés pour gérer efficacement l'information et les objectifs et motifs qui sous-tendent son traitement. Ce dernier aspect ("la vision et les besoins des utilisateurs") découle des priorités politiques établies par le Conseil, notamment dans le programme de Stockholm,

DÉCIDE

1. d'adopter et de mettre en œuvre une stratégie de gestion de l'information en vue de soutenir, de rationaliser et de faciliter la gestion de l'information dont les autorités compétentes ont besoin pour assurer la sécurité intérieure de l'UE, stratégie qui

   a) repose sur les principes suivants:

   – la gestion de l'information est un outil essentiel pour atteindre les objectifs consistant à renforcer la sécurité intérieure de l'UE et à protéger ses citoyens; elle n'est cependant pas un but en soi et reste un moyen axé sur une fin à atteindre. 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 d'atteindre les objectifs susmentionnés;

– 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. Par conséquent, la stratégie européenne de gestion de l'information 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;

– la stratégie fournit des orientations sur la manière d'assurer un échange d'informations approprié, dans le cadre duquel la communication des informations tient compte tant des besoins des utilisateurs que des droits des personnes concernées. Elle définit les conditions préalables du développement et de la gestion de l'échange d'informations, qui doivent être professionnels, axés sur les activités, efficaces et rentables. Elle indique la voie à suivre pour atteindre un échange structuré des informations et constitue une base pour améliorer les processus décisionnels et la gouvernance;

– la stratégie en soi ne crée pas de liens entre différentes bases de données, pas plus qu'elle ne prévoit des types particuliers d'échanges 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;

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

I. Besoins et exigences
   1. les besoins, les exigences et la valeur ajoutée sont évalués avant tout développement;
   2. tout développement est conforme aux flux de données autorisés dans le domaine de l'action répressive et aux formats du renseignement en matière pénale;
   3. tout développement répond à la fois aux exigences de la protection des données et aux besoins opérationnels des utilisateurs;

II. Interopérabilité et rentabilité
   4. l'interopérabilité et la coordination sont assurées entre les activités des utilisateurs et les solutions techniques;
   5. La réutilisation est la règle: ne pas réinventer la roue.

III. Processus de décision et de développement
   6. les États membres sont associés au processus dès le début;
   7. les responsabilités sont clairement partagées entre les différentes parties du processus, garantissant compétence, qualité et efficacité;

IV. Approche multidisciplinaire
8. la coordination multidisciplinaire est assurée au sein du domaine JAI;

2. de prendre les mesures nécessaires pour mettre au point et actualiser au besoin un plan d'action détaillé 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 aux échanges d'informations et au développement des TI pour mettre la stratégie en œuvre;

– le Coreper à charger le groupe ad hoc sur l'échange d'informations d'élaborer une liste de mesures pour la mise en œuvre de la stratégie et à garantir, sur la base des rapports de ce groupe et d'autres groupes, une mise en œuvre cohérente et efficace 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 à prendre la stratégie en considération lors de d'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 guide pour les responsables politiques, les responsables de l'information et autres décideurs au sein de leurs autorités compétentes lorsqu'ils traitent de questions liées aux échanges transnationaux d'informations et au développement des TI ou de questions influencées 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 lors de l'élaboration d'une communication qui aide le Conseil à formuler une vision propre aux utilisateurs pour renforcer l'échange d'informations à des fins répressives et à élaborer un modèle européen d'échange d'informations.

I. BESOINS ET EXIGENCES

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

Cette priorité met en évidence l'exigence de procéder à une évaluation de la valeur ajoutée avant d'instaurer un échange d'informations. Elle reflète aussi le principe de la 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:

a) *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;*

b) *il faut subordonner les idées ou les discussions sur les solutions techniques à l'analyse des besoins et des exigences;*

c) *les travaux relatifs aux instruments législatifs et/ou aux études préalables pour les solutions techniques ne devraient pas commencer avant que les exigences découlant des activités des utilisateurs ne soient établies et justifiées;*

d) *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;*

e) *des critères d'évaluation clairs, étayés par des programmes d'évaluation systématique, devraient être établis;*

f) *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 (procédés) de la coopération transnationale 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 transnationale en matière répressive qui orienteront le développement.

Implications:

a) les travaux consacrés à la "vision commune des besoins" devraient se poursuivre et être complétés par des analyses des exigences fondamentales, effectuées avec et par les autorités nationales;

b) *une "carte de l'information" devrait fournir une vue d'ensemble des activités quotidiennes et des flux d'informations correspondants dans le cadre de la coopération transnationale, de manière à définir sur cette base les niveaux de concertation auxquels une coordination 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, y compris 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 de la part des autorités compétentes dans ces domaines est un tremplin pour arriver à une attitude de partage des données par défaut.

Implications:

a) *les exigences légales assortissant 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 du point de vue technique) soient garantis pour les échanges d'informations et les systèmes TI;*

b) *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;*

c) *la sécurité des données doit être assurée par des moyens organisationnels ainsi que techniques et physiques;*

d) *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; cela réduira le risque de causer des dommages, tout comme le fera une formation consacrée aux outils disponibles et à leur utilisation;*

e) *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;*

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

II. INTEROPÉRABILITÉ ET RENTABILITÉ

4. L'interopérabilité et la coordination sont assurées entre les activités des utilisateurs et les 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 TI 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:

a) 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;

b) il conviendrait de prendre en compte les recommandations formulées dans la stratégie européenne en matière d'interopérabilité;

c) les fonctions actuelles d'accréditation ou de normalisation, définies d'un commun accord, devraient être utilisées;

d) *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;*

e) les mesures de protection des données et de sécurité des données devraient être coordonnées aux niveaux de l'UE et des États membres ainsi qu'entre ces niveaux.

5. La réutilisation est la règle: ne pas réinventer la roue.

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 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:

a) *la "carte de l'information" devrait inclure les flux d'informations, les fonctions et les solutions;*

b) *il faut présenter un mécanisme d'évaluation concret, utile et économe en ressources, qui devrait être fonction des objectifs poursuivis et non des compétences des différents services 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;*

c) *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, notamment le développement de l'échange d'informations, sur sa sécurité intérieure;*

d) *il faudrait élaborer une méthode pour partager et réutiliser les solutions viables en tenant compte des pratiques utilisées au sein de l'UE mais aussi dans les pays tiers;*

e) *une évaluation approfondie des instruments actuellement 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 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:

a) *les stratégies ou politiques nationales de gestion de l'information et celles de l'UE devraient être cohérentes;*
b) *les utilisateurs finaux et les principales parties prenantes devraient être associés au niveau national et à celui de l'UE;*
c) *les autorités des États membres doivent définir et mettre au point leurs propres processus de développement.*

7. Les responsabilités sont clairement partagées entre 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 de technique et d'architecture. Les décisions sur les niveaux de gestion et d'action doivent porter sur les questions correspondant à ce niveau.
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, et également pour garantir une coordination et une cohérence globales.

Implications:

a) *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, etc.);*

b) *il faut définir ou créer des fonctions pour préparer les décisions stratégiques sur la gestion de l'information et le développement des TI;*

c) *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[11]

8. La coordination multidisciplinaire est assurée.

La stratégie de gestion de l'information fait sienne et suit l'approche multidisciplinaire nécessaire pour assurer la sécurité intérieure 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 réduira à son tour les perturbations et les réenregistrements manuels et augmentera la qualité des informations. Elle permet aussi de maintenir et 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.

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.

---

[11] **Réserve d'examen de DE**.

Implications:

a) *il ne faut pas que des questions de compétence fassent obstacle aux échanges d'informations (reconnaissance mutuelle des différentes structures nationales); le cadre juridique applicable à ces échanges doit par ailleurs être strictement respecté;*

b) *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;*

c) *les mesures de protection des données et de sécurité des données devraient être coordonnées entre le niveau de l'UE et les États membres.*