E 3259

ASSEMBLÉE NATIONALE

DOUZIÈME LÉGISLATURE

SÉNAT

SESSION ORDINAIRE DE 2006-2007

Reçu à la Présidence de l'Assemblée nationale le 11/10/2006

Enregistré à la Présidence du Sénat le 11/10/2006

TEXTE SOUMIS EN APPLICATION DE L'ARTICLE 88-4 DE LA CONSTITUTION

PAR LE GOUVERNEMENT,

À L'ASSEMBLÉE NATIONALE ET AU SÉNAT

Livre Vert sur les technologies de détection dans le travail des services répressifs, des douanes et d'autres services de sécurité.

COM(2006) 0474 final

CONSEIL DE L'UNION EUROPÉENNE

Bruxelles, le 25 septembre 2006

13183/06

JAI 464
ENFOPOL 160
MI 166

NOTE DE TRANSMISSION

Origine:	Pour le Secrétaire général de la Commission européenne, Monsieur Jordi AYET PUIGARNAU, Directeur
Date de réception:	4 septembre 2006
Destinataire:	Monsieur Javier SOLANA, Secrétaire général/Haut Représentant
Objet:	Livre Vert sur les technologies de détection dans le travail des services répressifs, des douanes et d'autres services de sécurité

Les délégations trouveront ci-joint le document de la Commission COM(2006) 474 final.

p.j. : COM(2006) 474 final

COMMISSION DES COMMUNAUTÉS EUROPÉENNES

Bruxelles, le 1.9.2006
COM(2006) 474 final

LIVRE VERT

sur les technologies de détection dans le travail des services répressifs, des douanes et d'autres services de sécurité

(présenté par la Commission)

TABLE DES MATIÈRES

LIVRE VERT

sur les technologies de détection dans le travail des services répressifs, des douanes et d'autres services de sécurité

(Texte présentant de l'intérêt pour l'EEE)

INTRODUCTION

La sécurité est un élément fondamental de la politique de la Commission. La lutte contre la criminalité et le terrorisme est une dimension essentielle de la politique de sécurité. Dans sa communication *«Attaques terroristes: prévention, préparation et réponse»* d'octobre 2004, la Commission a exposé sa politique antiterroriste. Cette communication souligne l'importance du *Dialogue entre les secteurs privé et public sur les questions de sécurité* en tant qu'instrument permettant d'engager entre ces secteurs une concertation fructueuse au sujet des besoins de l'Europe en matière de sécurité. Le *«Programme de La Haye: renforcer la liberté, la sécurité et la justice dans l'Union européenne»*, adopté par le Conseil européen en novembre 2004, qui constitue à l'heure actuelle le programme politique de l'Union en matière de justice et d'affaires intérieures, souligne lui aussi l'importance de l'interaction public-privé dans la lutte contre le crime organisé et le terrorisme. Le présent Livre vert vise à fournir les éléments nécessaires à l'engagement d'un tel dialogue dans le domaine des technologies de détection.

Dans leur travail quotidien, les services de sécurité s'appuient de plus en plus sur les technologies de détection pour combattre le terrorisme et d'autres formes de criminalité. Ces technologies sont largement utilisées pour la protection des passagers des lignes aériennes et des supporters qui assistent à des événements sportifs, ainsi que pour la détection de substances dangereuses dans l'air, l'eau ou les aliments. Les services de sécurité emploient également ces technologies pour protéger nos frontières et contrôler les marchandises qui entrent sur le territoire de l'Union européenne. Les technologies de détection sont, en outre, essentielles à la surveillance des biens privés et des infrastructures critiques. Le présent Livre vert vise à définir le rôle que pourrait jouer l'Union européenne pour encourager le développement des technologies de détection au service de la sécurité de ses citoyens. Par ailleurs, les technologies de détection représentent par définition une ingérence dans la sphère privée ou peuvent porter atteinte à certains droits et libertés. Dès lors, chaque fois que l'amélioration et l'utilisation des technologies de détection sont envisagées, il y a lieu d'analyser avec soin cet aspect ainsi que la question fondamentale des limites de cette ingérence. La Commission entend contribuer à l'étude de ces deux problèmes par la présente initiative.

Les 28 et 29 novembre 2005, la Commission a organisé à Bruxelles une conférence intitulée *Dialogue public-privé sur les questions de sécurité: Technologies de détection et technologies associées dans la lutte contre le terrorisme*[1]. La participation de plus d'une centaine de représentants de grandes associations professionnelles européennes et du secteur public atteste

[1] Pour plus d'information, voir la partie I de l'annexe.

de l'intérêt des parties prenantes à la conduite d'une politique dans ce domaine. Des membres des services répressifs, douaniers et de sécurité représentaient le secteur public.

Le rôle de l'Europe dans des domaines tels que la recherche ou la normalisation en matière de sécurité est clairement établi. Bien qu'un travail considérable ait été accompli dans certains domaines en étroite collaboration avec les États membres, l'industrie et d'autres parties intéressées, la politique européenne en matière de technologies de détection, en tant que telle, peut encore être améliorée. S'agissant de la sûreté aérienne, les deux règlements (CE) n° 2320/2002 et n° 622/2003[2] prévoient des dispositions détaillées en ce qui concerne les critères de performance des équipements d'inspection/filtrage à utiliser et leur mode d'utilisation. Dans ce domaine, des normes et des protocoles d'essais ont été établis en étroite collaboration avec la Conférence européenne de l'aviation civile qui regroupe des experts issus des services compétents des États membres et d'autres États européens. La Commission entretient en outre des contacts réguliers avec l'industrie et d'autres parties intéressées (groupe consultatif des parties intéressées à la sûreté aérienne – groupe SAGAS).

En vue de renforcer l'approche commune des technologies de détection, la Commission a pris la présente initiative, afin d'améliorer encore l'interaction entre les secteurs public et privé, et de concentrer l'investissement sur la normalisation, la recherche, la certification et l'interopérabilité des systèmes de détection et de convertir les résultats de la recherche en outils utiles et adéquats. Il convient de créer un cercle vertueux dans lequel le secteur privé est guidé dans ses efforts de recherche et ses dépenses par un secteur public conscient de ses besoins et de ce que le secteur privé est en mesure de proposer. Cela devrait contribuer à la mise en place d'un marché moderne des produits de détection et des dispositifs de sécurité, qui devrait déboucher à son tour sur une plus grande disponibilité de ces produits et services à moindre coût.

Pour atteindre cet objectif, il faut une action commune, une meilleure coordination et un échange d'informations plus intensif de la part de toutes les parties concernées en Europe. Il est nécessaire de définir plus précisément les besoins, et de trouver des solutions technologiquement et économiquement viables. Le présent Livre vert **n'a certainement pas pour but de faire double emploi avec d'autres activités menées au niveau national ou européen**. La Commission ne veut pas réinventer la roue, mais dresser l'inventaire des bonnes approches et pratiques existantes, de les soutenir et de les diffuser dans toute l'Union.

La Commission souhaite que le présent Livre vert suscite le plus possible de réponses stimulantes et de propositions concrètes de mesures futures. **Une large participation des États membres, du secteur privé et d'autres parties intéressées est donc indispensable**. La Commission est néanmoins consciente des besoins de confidentialité, tant dans le secteur public que dans le secteur privé, pour des raisons de sécurité et commerciales. Il est donc demandé aux répondants de signaler les réponses ayant un caractère trop sensible pour être partagées et de proposer une autre approche afin de tenir compte de ces problèmes particuliers.

---

[2] Règlement (CE) n° 2320/2002 du Parlement européen et du Conseil du 16 décembre 2002 relatif à l'instauration de règles communes dans le domaine de la sûreté de l'aviation civile, JO L 355 du 30.12.2002, p. 1 et règlement (CE) n° 622/2003 de la Commission du 4 avril 2003 fixant les mesures pour la mise en œuvre des règles communes dans le domaine de la sûreté aérienne, JO L 89 du 5.4.2003, p. 9.

Les politiques concernant les technologies de détection et les technologies connexes doivent respecter pleinement le cadre juridique existant, notamment la Charte des droits fondamentaux de l'Union européenne, la Convention européenne des droits de l'homme ainsi que les principes et règles de protection des données énoncés dans la directive 95/46/CE. Dans ce contexte, la Commission souligne qu'il est impératif que la conception, la fabrication et l'utilisation des systèmes de détection et des systèmes connexes, de même que toutes dispositions législatives ou autres visant à les réglementer ou à les promouvoir, **respectent pleinement les droits fondamentaux** consacrés dans la Charte des droits fondamentaux de l'Union et la Convention européenne des droits de l'homme. À cet égard, il y a lieu d'accorder une attention particulière au respect de la protection des données à caractère personnel et du droit à la vie privée. En effet, le recours aux technologies de détection supposant généralement une ingérence dans les droits fondamentaux à la vie privée et à la protection des données à caractère personnel, il doit impérativement respecter la Convention européenne des droits de l'homme; il doit notamment être prévu par la loi, constituer une mesure nécessaire dans une société démocratique à la protection d'un intérêt public important et être proportionné à l'intérêt public poursuivi.

I. NORMALISATION ET RECHERCHE EN MATIÈRE DE SÉCURITÉ

1. NORMALISATION

Il existe une très large gamme de possibilités technologiques dans les domaines des technologies de détection et des technologies connexes et du travail des services de sécurité. Des normes minimales sont donc indispensables. Toutefois, vu l'étendue de cette gamme, il convient d'assigner des priorités à ce processus de normalisation, ce qui n'est possible qu'au moyen d'une interaction adéquate entre le secteur public (besoins) et le secteur privé (solutions). Au niveau européen, les secteurs public et privé s'accordent à dire que cette interaction est insuffisante. Par ailleurs, de nombreuses activités positives voient le jour aux niveaux national et européen. La vision d'ensemble des initiatives existantes qui est nécessaire pour éviter les doubles emplois et mieux définir les priorités fait cependant défaut. Il est évident que des raisons de sécurité s'opposent à ce que l'élaboration de normes soit débattue publiquement. La discussion portera donc principalement sur l'opportunité de disposer de normes communes.

L'utilisation et le traitement des données et informations recueillies par les instruments de détection, par exemple comme preuves devant un tribunal, sont aussi étroitement liés à la normalisation. Le recensement et l'échange des meilleures pratiques en la matière pourraient présenter des avantages pour les autorités compétentes. Il convient également d'envisager l'élaboration de normes techniques pour faire en sorte que les données recueillies soient conformes aux dispositions légales qui régissent leur utilisation dans les procédures judiciaires.[3]

Questions

Des normes communes sont-elles nécessaires pour les technologies de détection et les technologies connexes utilisées dans le travail des services de sécurité? Quelles sont selon vous les normes à arrêter en priorité?

Dans la phase de préhomologation, quelles sont les normes qui ne reçoivent pas de soutien financier insuffisant?

Pour éviter les doubles emplois et améliorer la transparence, serait-il utile de disposer d'une liste/d'un manuel/d'une base de données consultable, régulièrement mis à jour et recensant les efforts de normalisation passés, actuels et prévus dans les domaines de la détection et des technologies connexes, aux niveaux national et européen?

Seriez-vous intéressé par le recensement et l'échange des meilleures pratiques d'utilisation et de traitement des données et des informations recueillies par des instruments de détection dans le but de respecter pleinement la réglementation régissant l'utilisation des preuves dans les procédures judiciaires?

Quel serait selon vous le meilleur moyen de recenser et d'échanger ces pratiques?

[3] Pour les dispositions légales régissant l'échange des données à caractère personnel, veuillez consulter la partie II de l'annexe.

2. RECHERCHE EN MATIERE DE SECURITE

La recherche en matière de sécurité est un autre domaine essentiel pour la mise au point de nouveaux produits et solutions en matière de sécurité à l'usage des services de sécurité des États membres. Dans ce contexte, il y a lieu de souligner le rôle joué par le Comité consultatif européen pour la recherche dans le domaine de la sécurité (CCERS). Le CCERS adopte une vaste perspective d'ensemble dans ce domaine et conseille la Commission sur le contenu et la mise en œuvre des activités de recherche à réaliser, ainsi que sur les mécanismes de suivi des évolutions intéressantes enregistrées dans d'autres programmes.

Un certain nombre d'activités de recherche sur la sécurité sont en cours au niveau européen et dans les États membres. Il n'existe toutefois aucun mécanisme d'agrégation et de diffusion d'informations sur les activités de recherche passées, actuelles et prévues dans le domaine de la sécurité aux niveaux européen, national, et en dernière analyse, du secteur privé. Un tel mécanisme permettrait d'éviter un gaspillage de ressources limitées dû à la duplication et au chevauchement des projets. Par ailleurs, s'il est jugé nécessaire un mécanisme séparé de diffusion des activités de recherche en matière de sécurité classées secrètes pourrait être mis au point afin de limiter l'accès à ces informations aux seules personnes autorisées.

Après plus d'une année de travail, le CCERS est en train de finaliser son rapport qui sera publié en septembre 2006. Ce rapport recense quelque 120 capacités de sécurité et une centaine de technologies clés qui nécessitent un effort supplémentaire de recherche & développement au niveau de l'UE, alors que diverses autres technologies sont ou seront traitées au niveau national.

Questions

Comment les informations sur la recherche en matière de sécurité en Europe doivent-elles être diffusées pour stimuler la compétitivité tout en évitant le gaspillage de ressources limitées?

II. BESOINS ET SOLUTIONS

1. BESOINS ET SOLUTIONS TECHNOLOGIQUES

La mise au point de solutions et de produits de qualité, efficaces et exploitables suppose que les concepteurs de ces solutions et produits disposent d'informations suffisantes sur les besoins réels des utilisateurs finals. Or, au niveau européen, il semble qu'une plus grande interaction soit nécessaire entre la demande (c'est-à-dire les services de sécurité compétents) et l'offre de solutions technologiques. Toute interaction de cette nature doit également chercher à définir les besoins, à court, moyen et long termes. Par ailleurs, ceux qui proposent les solutions doivent également indiquer dans quel délai elles seront disponibles.

Le dialogue entre concepteurs et utilisateurs doit en outre poser et chercher à résoudre des questions plus fondamentales concernant la nature de nos sociétés et le rôle des technologies de détection. Un tel débat est également important pour défendre les valeurs et la nature de nos sociétés.

Questions

Un débat élargi sur le rôle des technologies de détection et l'influence potentielle de leur utilisation sur les sociétés européennes présente-t-il, selon vous, un intérêt?

Dans quels domaines spécifiques les services de sécurité compétents ont-ils besoin d'améliorations technologiques? Veuillez préciser l'ordre de priorité attribué à ces besoins spécifiques?

Existe-t-il un fossé entre les besoins de capacités de détection et les solutions technologiques actuellement disponibles sur le marché? Quelles sont selon vous les solutions éventuelles pour le combler?

Dans quels domaines spécifiques le secteur privé offre-t-il déjà ou prévoit-il d'offrir des solutions technologiques? Veuillez préciser dans quel délai ces solutions seront disponibles en présentant un bon rapport coût-efficacité?

Considérez-vous qu'il soit utile de créer une liste/base de données consultable à l'échelle de l'Europe énumérant les domaines spécifiques dans lesquels les services de sécurité compétents éprouvent des besoins ainsi que les solutions offertes par le secteur privé?

Dans la négative, quelles autres solutions proposez-vous pour améliorer le flux d'informations entre l'offre et la demande de solutions technologiques?

1.1 Solutions flexibles

Les menaces que représentent actuellement la criminalité et le terrorisme, sont multiples, en évolution constante et se manifestent sous des formes, dans des situations et à des niveaux différents. Elles appellent donc des niveaux de protection et de réaction variables dans le temps, c'est-à-dire des solutions flexibles.

Question

Quels sont les instruments et équipements existants dont l'applicabilité et l'efficacité pourraient être améliorées par un accroissement de leur flexibilité?

Quels sont les besoins de nouveaux instruments et équipements flexibles?

1.2 Solutions portables et mobiles

La menace que représentent le terrorisme et la criminalité non seulement évolue avec le temps, mais devient aussi de plus en plus mobile, d'où la nécessité de solutions portables pour les services de sécurité. Ce type de solutions peut améliorer le rapport coût-efficacité et être facilement transférable d'un lieu à l'autre, en fonction des besoins, car il est tout bonnement impossible de couvrir avec le même niveau de sécurité chaque point d'entrée ou point sensible. De plus, les solutions portables et mobiles peuvent permettre de nouvelles approches opérationnelles.

Question

Quels instruments et équipements existants pourraient être utilisés mieux et plus efficacement dans le travail des services de sécurité concernés s'ils étaient mobiles et portables?

Quels sont les besoins d'instruments et équipements portables et mobiles?

2. INTEROPERABILITE DES SYSTEMES[4]

Les États membres et leurs services compétents disposent déjà de plusieurs systèmes utiles de lutte contre la criminalité et le terrorisme. Toutefois, il arrive souvent que ces systèmes ne soient pas en mesure de communiquer entre eux, ce qui risque d'entraver les efforts communs déployés dans la lutte contre la criminalité et le terrorisme aux niveaux national et européen. Les systèmes doivent par ailleurs être conformes aux cadres juridiques existants et autres règles (par exemple la protection des données, atteintes à la vie privée causées par les systèmes de détection).

Question

Quels sont les systèmes pour lesquels une amélioration de l'interopérabilité est nécessaire?

Une étude sur les contraintes juridiques et autres qui font obstacle à l'interopérabilité des systèmes dans l'UE serait-elle utile pour déterminer quelles sont les limitations?

3. INTEGRATION D'INFORMATIONS PROVENANT DE DIFFERENTES TECHNOLOGIES DE DETECTION ET ANALYSE AMELIOREE DES DONNEES

L'intégration des données provenant de différentes technologies de détection en un système unique d'analyse de données pourrait rendre les systèmes de détection plus efficaces. Toute mesure adoptée en cette matière doit être conforme aux règles de protection des données.

---

[4] Il faut également prendre en considération d'autres systèmes que les systèmes d'information.

Question

Dans quels domaines pensez-vous que l'intégration des informations provenant de différentes technologies de détection améliorerait les performances globales ?

Dans quels domaines de meilleures techniques d'analyse des données sont-elles nécessaires ?

III. UTILISATION ET CERTIFICATION DES ÉQUIPEMENTS ET OUTILS

1. MEILLEURES PRATIQUES ET UTILISATION DES OUTILS ET EQUIPEMENTS EXISTANTS

Des solutions technologiques entièrement nouvelles ne sont pas toujours nécessaires pour combattre efficacement les menaces existantes ou nouvelles et il arrive fréquemment que le secteur public ne dispose pas des moyens financiers nécessaires à leur acquisition. Il convient donc d'examiner comment les instruments existants et acquis précédemment peuvent être utilisés plus efficacement ou améliorés, ce qui peut être un moyen économique d'améliorer l'efficacité, d'accroître la fiabilité et de réduire le nombre de fausses alarmes.

Il n'existe pas de mécanisme d'échange d'expériences concernant ces questions entre les autorités compétentes des différents États membres. Il pourrait par exemple y avoir un partage d'informations au sujet des progrès obtenus au moyen de modifications du mode d'utilisation ou d'améliorations peu coûteuses.

Questions

Quel serait le meilleur moyen de recenser et d'échanger les meilleures pratiques dans ce domaine?

Recensement des meilleures pratiques

Devrait-il s'appuyer sur une évaluation par les pairs ou sur des questionnaires adressés aux États membres?

Diffusion des meilleures pratiques

Devrait-elle s'opérer au moyen d'une base de données sécurisée et consultable, ou par le biais de réunions et séminaires?

Pouvez-vous suggérer d'autres moyens de recenser et de diffuser les meilleures pratiques dans ce domaine?

Au cas où l'amélioration d'un instrument ou d'un équipement serait jugée nécessaire et où aucune des autorités d'autres États membres n'y aurait procédé, une consultation du secteur privé à ce sujet serait-elle acceptable?

2. RECENSEMENT ET DIFFUSION DES MEILLEURES PRATIQUES ET UTILISATION DE NOUVEAUX OUTILS ET EQUIPEMENTS

Les autorités nationales pourraient également être assistées dans leur travail par un système qui faciliterait l'échange d'informations sur l'utilisation de nouveaux instruments et équipements et leur permettrait de s'instruire mutuellement et de mettre à profit l'expérience acquise par d'autres. Ces échanges d'informations, d'expériences et de meilleures pratiques au sujet des instruments et équipements peuvent aider les autorités à déterminer les équipements qui répondent à leurs besoins particuliers.

En outre, les essais des équipements nouveaux ou expérimentaux pourraient être favorisés par un cofinancement communautaire et/ou du secteur privé. Des essais à plus grande échelle portant sur les équipements nouveaux ou expérimentaux pourraient aider l'industrie européenne à convertir les résultats de la recherche en matière de sécurité en produits efficaces et compétitifs.

Questions

Quel serait le meilleur moyen de recenser et d'échanger les informations et les meilleures pratiques dans ce domaine?

Recensement des meilleures pratiques

Devrait-il s'appuyer sur une évaluation par les pairs ou sur des questionnaires adressés aux États membres?

Diffusion des informations et des meilleures pratiques

Devrait-elle s'opérer au moyen d'une base de données sécurisée et consultable, ou par le biais de réunions et séminaires à admission restreinte?

Avez-vous d'autres suggestions au sujet des moyens de recenser les meilleures pratiques dans ce domaine et de les diffuser efficacement?

Instruments nouveaux et expérimentaux

Des essais sur les équipements et instruments nouveaux ou expérimentaux présentent-ils un intérêt pour vous?

Dans l'affirmative/la négative, veuillez préciser pourquoi.

Un financement partiel des essais d'instruments et équipements nouveaux ou expérimentaux par la Communauté et/ou le secteur privé présente-t-il un intérêt?

3. UTILISATION D'INSTRUMENTS DE FOUILLE DE DONNEES ET DE TEXTES

Les services de sécurité nationaux ou européens sont confrontés à une augmentation constante du volume de la documentation et des informations à traiter. Pour y faire face plus efficacement, il existe des logiciels modernes permettant de réaliser des fouilles de données et de textes. Cette technologie permet d'extraire des informations pertinentes à partir d'une très grande quantité de documents. Il est, par exemple, possible de filtrer intelligemment des textes et documents pour faciliter la navigation (groupage de documents), pour l'autocatégorisation (canalisation et prioritisation du flux de documents au sein des équipes d'enquête) et pour le contrôle de la validité des codes utilisés. Les objectifs sont les suivants:

- repérage rapide des entités clés dans des ensembles de documents,
- prétraitement pour la recherche ciblée de documents,
- classement des documents selon leur contenu afin de focaliser les analyses ultérieures,

- analyse automatisée des informations provenant de sources diverses.

Le potentiel de ces outils modernes n'est pas suffisamment exploité dans les États membres. Cependant, parallèlement à la promotion de l'utilisation de ces technologies, il ne faut pas perdre de vue que leur utilisation dans certaines applications, telles que le contrôle des courriers électroniques, constitue en soi une atteinte au droit fondamental des citoyens à la vie privée. Le courrier électronique est une forme de correspondance et est couvert en tant que tel par le droit à la confidentialité des communications consacré dans la Convention européenne des droits de l'homme. L'utilisation de toute technique de fouille de données et de textes doit par conséquent être prévue par la loi, constituer une mesure nécessaire dans une société démocratique à la protection d'un intérêt public important et être proportionnée à l'intérêt public poursuivi. L'adhésion au respect des droits fondamentaux et des principes relatifs à la protection des données devrait être inhérente à ces outils et à leur utilisation. Enfin, il importe que ces activités soient réalisées sous le contrôle et la supervision des autorités publiques compétentes.

Questions

Exercice de sensibilisation

Les États membres et les organes européens concernés seraient-ils intéressés par le partage des meilleures pratiques et par les avantages potentiels de l'utilisation d'instruments de fouille de données et de textes?

Les autorités des États membres utilisant ces technologies seraient-elles disposées à partager leur expérience avec leurs pairs?

L'organisation de séminaires à admission restreinte sur ce sujet par les États membres, Europol ou l'OLAF serait-elle utile?

Renforcement de la capacité de fouille de données et de textes de l'UE

Un centre d'excellence au niveau européen accessible à tous les États membres et aux autorités concernées contribuerait-il à exploiter concrètement le potentiel de ces instruments?

Dans la négative, quelles autres options proposez-vous pour maximiser le potentiel de ces outils?

Recensement et diffusion des meilleures pratiques

Une évaluation par les pairs ou un questionnaire adressé aux États membres seraient-ils utiles pour recenser les meilleures pratiques d'utilisation de ces outils?

Dans la négative, quelles autres approches proposez-vous pour recenser les meilleures pratiques dans ce domaine?

Renforcement de la capacité régionale de fouilles de données et de textes

Les États membres et les organes européens disposent-ils d'une capacité inutilisée leur permettant d'aider les États membres qui ne possèdent pas cette technologie à traiter leurs documents?

En l'absence de cette capacité ou en cas de capacité limitée, un accroissement de capacité dans les États membres ou au niveau européen financé par l'Union européenne serait-il utile et gérable?

Les États membres dont la capacité de fouille de données et de textes est insuffisante seraient-ils disposés à utiliser les outils d'autres organes, s'ils étaient mis à leur disposition?

Serait-il possible de créer des centres européens ou régionaux de fouille de données et de textes que plusieurs États membres et leurs autorités pourraient utiliser pour la fouille de données et de textes?

Les outils existants de fouille de données et de textes traitent-ils suffisamment les différentes langues présentes en Europe?

Existe-t-il des outils suffisants pour aider les autorités qui traitent des textes et des documents dans d'autres langues?

Autres

Si vous n'êtes pas d'accord avec l'une des options présentées ci-dessus, comment traiteriez-vous les problèmes abordés dans ce point?

5. ESSAIS ET CERTIFICATION DES EQUIPEMENTS ET OUTILS

Le marché offre déjà un certain nombre de produits de détection. Il est cependant très souvent difficile de déterminer quels outils et produits sont les meilleurs, ou du moins répondent à certaines exigences minimales. Ce déficit pourrait être comblé au moyen d'un système européen de certification et d'étalonnage de la qualité des outils destiné à simplifier le processus de détermination des outils ou équipements qui répondent aux besoins particuliers d'une autorité donnée. Cela devrait permettre aux autorités nationales de prendre plus facilement leurs décisions d'achat d'équipements et outils et d'optimiser ainsi l'utilisation de ressources peu abondantes.

Un réseau d'autorités *nationales* de certification partageant leurs expériences et connaissances pourrait être établi pour remédier à cette absence d'un système d'évaluation de la qualité des outils. Ces autorités conviendraient également de normes d'étalonnage et de certification des solutions technologiques de qualité. Ce type de certification pourrait être utilisé non seulement pour aider les autorités nationales à évaluer la qualité d'un outil, mais aussi pour promouvoir des solutions européennes sur d'autres marchés. Il est évident que des raisons de sécurité s'opposent à ce que l'élaboration de protocoles d'essais soit publiquement débattue.

Question

La création d'un réseau d'autorités nationales de certification partageant leurs expériences et connaissances, parallèlement à un système de certification de la qualité et d'étalonnage, serait-elle utile?

Dans la négative, quelle autre solution préconisez-vous pour résoudre le problème exposé?

Des normes communes de certification et d'étalonnage seraient-elles utiles?

Dans la négative, comment garantiriez-vous la transparence de ce processus et l'employabilité des résultats dans toute l'UE?

IV. ÉTUDES[5]

Les participants à la conférence ont recensé différents thèmes qui demandent des études complémentaires. La Commission propose donc de réaliser des études sur:

(1) les technologies et la protection des événements de masse;

(2) les obstacles à la coopération et au partage d'informations entre laboratoires médico-légaux et établissements de recherche en matière de sécurité;

(3) les dispositions légales régissant l'utilisation de technologies de détection spécifiques;

(4) l'utilisation concrète de technologies de détection spécifiques;

(5) le cadre juridique régissant l'utilisation de la détection des personnes (y compris la surveillance) dans l'UE;

(6) les niveaux d'acceptation de la détection des personnes (y compris la surveillance et l'utilisation des données biométriques) dans l'UE.

En général, ces études doivent servir à améliorer les connaissances des parties intéressées et à garantir le respect des cadres juridiques existants lors de l'élaboration ou de l'utilisation de technologies de détection. Dans d'autres cas, ces études peuvent servir à l'examen des options politiques et au choix d'autres mesures concrètes.

Question

Souhaiteriez-vous recevoir des études sur ces thèmes fondées sur les informations de base présentées dans l'annexe?

Dans la négative, veuillez expliquer pourquoi et proposer d'autres façons d'aborder les problèmes exposés.

[5] Pour une plus ample description de la justification de ces études, voir partie III de l'annexe.

V. APPLICATION DES RÉSULTATS DE LA CONSULTATION

1. DIALOGUE SPECIFIQUE PUBLIC-PRIVE RENFORCE SUR LES TECHNOLOGIES DE DETECTION ET LES TECHNOLOGIES CONNEXES

Le présent Livre vert expose un certain nombre d'activités envisageables pouvant contribuer à améliorer l'interaction entre le secteur privé et le secteur public dans le domaine des technologies de détection, et aider ainsi les services de sécurité des États membres à accéder aux meilleurs instruments, solutions et pratiques disponibles. Par ailleurs, ces activités peuvent permettre au secteur privé de concentrer ses investissements sur les besoins du secteur public. Il est cependant évident qu'il faut pour cela une coopération intense entre les secteurs public et privé, d'où la nécessité d'un dialogue spécifique public/privé renforcé dans ce domaine. Ce dialogue pourrait revêtir diverses formes, dont la création d'un organe spécifique ou la mise en place d'un groupe spécifique dans le cadre d'exercices horizontaux de partenariat public/privé en matière de sécurité qui devraient être lancés dans un proche avenir.

L'objectif de cette activité ne serait pas de faire concurrence aux organes existants, mais plutôt de combler les lacunes de l'interaction entre le secteur privé et le secteur public par la participation des services de sécurité compétents au niveau européen. La structure de dialogue ne devrait pas non plus être permanente: elle aurait des objectifs clairement définis, mais cesserait d'exister une fois qu'ils seraient atteints. Elle servirait de forum aux experts issus du secteur privé et du secteur public pour contribuer à la solution des problèmes évoqués dans le présent document ou des nouveaux défis qui pourraient se présenter dans la mise en œuvre des résultats de la consultation publique sur le présent document.

Par ailleurs, il va de soi qu'un certain nombre d'actions envisageables et proposées dans le présent document requièrent une action des États membres sans intervention du secteur privé. En outre, la définition des tâches relevant de cette coopération ferait l'objet d'un accord entre le secteur public et le secteur privé, ce qui permettrait aux États membres d'en influencer le rôle et les thèmes. Le dialogue devrait également porter sur la question du partage d'informations confidentielles entre le secteur public et le secteur privé, bien qu'il faille souligner que le secteur public n'est pas le seul dépositaire d'informations sensibles.

Question

Un instrument tel qu'un dialogue spécifique public/privé renforcé dans le domaine de la détection et des technologies connexes serait-il utile pour appliquer les résultats de la consultation publique sur le présent document?

Dans l'affirmative, adhérez-vous aux propositions présentées ci-dessus ou avez-vous d'autres idées?

Dans la négative, quels autres mécanismes préconisez-vous pour donner suite aux résultats de la consultation publique sur le présent document?

Souhaiteriez-vous contribuer aux travaux de la structure concernée ou y participer directement?

2. PLAN D'ACTION

Les plans d'action aux niveaux national et européen se sont révélés utiles pour superviser l'action dans des domaines complexes tels que la lutte contre le terrorisme ou la criminalité. La conférence, tout comme le présent document, soulèvent de nombreuses questions au sujet des technologies de détection et des technologies connexes dans le travail des services de sécurité compétents. Pour suivre les progrès dans ce domaine et fixer des objectifs, un plan d'action fondé sur les réponses à ces questions et, si nécessaire, sur d'autres consultations pourrait être établi.

Question
Un plan d'action serait-il un instrument utile pour mettre en œuvre les mesures proposées dans les réponses au présent document?

Remarque finale

Les réponses au présent document sont à envoyer avant le 10 janvier 2007 par courrier électronique à l'adresse suivante: **JLS-D1-Detection@ec.europa.eu**. Toutes les réponses, qu'elles émanent du secteur public ou du secteur public, seront publiées sur le site Internet de la Commission, à moins que les répondants ne déclarent expressément que certaines informations doivent rester confidentielles.

ANNEXE

I. INFORMATION DE BASE AU SUJET DE L'ELABORATION DU LIVRE VERT

Le présent Livre vert est fondé sur les résultats de la conférence et évoque des thèmes et des questions qui ont occupé une place prépondérante dans les discussions (par exemple, normalisation, recherche en matière de sécurité, amélioration de solutions technologiques, protection de la vie privée, cadre juridique et autres règles que les technologies doivent respecter, etc.). Plus d'une centaine de participants venus des entreprises et du secteur public ont participé au débat. Le secteur public était représenté par des membres des services de police, des douanes et de sécurité, par la Commission et par des représentants des États membres. Quoique le titre de la conférence donne à penser qu'elle était axée sur la lutte contre le terrorisme, il est cependant apparu dès le départ qu'une approche plus large était indispensable pour éviter que d'importants problèmes de sécurité ne soient négligés. Cette approche élargie a été confirmée par la décision du Conseil de décembre 2005 de fonder la protection des infrastructures critiques européennes sur une approche tenant compte de tous les risques. En outre, la conférence a adopté une approche globale en réunissant des acteurs appartenant à différents domaines d'expertise pour débattre des sujets suivants:

- Les technologies de détection dans la protection des infrastructures
- Les technologies de détection des personnes et les données biométriques
- La détection des explosifs et des substances chimiques, biologiques, radiologiques et nucléaires (CBRN).

Tous les thèmes étaient centrés sur le travail des services de police, de sécurité et des douanes. Cette approche a permis à la conférence de cerner de nombreux domaines présentant un intérêt commun pour le secteur public et le secteur privé (par exemple, l'interaction entre ceux qui proposent des solutions et ceux qui ont besoin de solutions dans le secteur public). Cette préoccupation se reflète dans l'ensemble du document.

Définition des technologies de détection et catégories pertinentes

Aux fins de la consultation, le terme 'technologie de détection' est employé au sens le plus large possible. Les technologies de détection peuvent être "in situ" ou extérieures et le moyen le plus perfectionné de faire face à certains problèmes de sécurité dans différents scénarios est sans doute d'intégrer ces technologies à un système complexe (tel que le système de transport). Une technologie de détection peut être pratiquement tout dispositif utilisé pour détecter quelque chose dans un contexte de sûreté ou de sécurité dans une optique policière, douanière ou de sécurité. Il est possible de distinguer plusieurs catégories[6] dont la prise en considération pour répondre aux questions posées dans le présent document peut accroître la pertinence des réponses:

- Détecteurs portatifs
- Portiques de sécurité

[6] La liste qui suit n'est pas exhaustive.

- Dispositifs de surveillance
- Détection des caractéristiques biométriques
- Outils de fouille de données et de textes
- Autres outils de détection fondés sur des logiciels, etc.

Pour répondre aux questions, les répondants devraient également tenir compte des technologies connexes car les technologies qui permettent aux êtres humains d'interpréter les données rassemblées par les détecteurs sont également importantes pour que les dispositifs soient efficaces. Il faut une technologie pour intégrer les solutions et assurer l'interopérabilité des systèmes. Les répondants ne doivent pas se sentir limités par la liste ci-dessus et sont encouragés à aller au-delà des catégories énumérées.

II. NORMALISATION ET ECHANGE DE DONNEES A CARACTERE PERSONNEL

La Commission signale, à propos du traitement de données à caractère personnel, que la directive 95/46/CE fournit déjà le cadre juridique de l'échange d'informations contenant des données à caractère personnel dans le cadre d'activités relevant du «premier pilier». En ce qui concerne l'échange d'informations dans le cadre de la coopération judiciaire et pénale, et, en vertu du principe de disponibilité des informations, la Commission a déposé une proposition législative, qui est actuellement en discussion.

III. ÉTUDES

1. Protection des événements de masse

Chaque année, les États membres de l'UE organisent diverses grandes manifestations publiques d'importance nationale, européenne, mais aussi internationale. Dans les conditions de sécurité actuelles, les coûts de sécurité lors de ces manifestations peuvent représenter une part importante des budgets qui y sont affectés. Tous les États membres pourraient tirer profit d'une approche commune de ce problème.

Afin de préparer le terrain pour l'adoption d'éventuelles mesures dans ce domaine, la Commission propose d'organiser une étude sur la protection des événements de masse. Cette étude examinerait quels outils, équipements et expertises en matière de sécurité utilisés dans la protection des grandes manifestations sont transférables d'un événement/d'un site à un autre. Elle examinerait également les possibilités pratiques et les implications d'équipements appartenant à la Communauté, d'équipements partagés à l'échelle de la Communauté, de l'élaboration d'un modèle commercial pour la fourniture de services par le secteur privé ou d'une combinaison de ces trois approches. Cette partie de l'étude devrait déterminer quelle solution:

- présente le meilleur rapport coût-efficacité et une flexibilité suffisante pour répondre à divers besoins des États membres ;
- est accessible à tous les États membres avec un partage approprié des coûts entre eux.

Lorsque les résultats de l'étude seront prêts, la Commission envisagera de nouvelles mesures dans ce domaine, en concertation avec les États membres et d'autres acteurs concernés.

2. Coopération et partage d'informations entre laboratoires médico-légaux et établissements de recherche en matière de sécurité

Les participants à la conférence ont souligné l'existence au niveau national d'obstacles juridiques et autres qui empêchent une coopération et un partage d'informations effectifs entre établissements médico-légaux nationaux au niveau européen. Aussi la Commission propose-t-elle de mener une étude à ce sujet qui pourrait également examiner les moyens de remédier à cette situation.

Le même problème a été évoqué à propos de la coopération et de l'échange d'informations entre établissements de recherche en matière de sécurité. Une étude distincte à ce sujet pourrait également être réalisée.

3. Le droit et les technologies de détection spécifiques

Les services de police, des douanes et autres services de sécurité font souvent l'objet d'un contrôle afin de vérifier s'ils respectent les règles de droit applicables. Même si une technologie en tant que telle n'enfreint pas les règles de droit, son mode d'utilisation peut être source de préoccupations. En conséquence, le rappel du cadre juridique qui régit l'utilisation des solutions technologiques et en fixe les limites pourrait contribuer à sensibiliser le secteur public et le secteur privé et faciliter le respect des normes existantes. Le secteur privé pourrait également mettre à profit une telle étude pour concevoir et proposer des solutions et services technologiques à l'intention du secteur public.

4. Les technologies de détection spécifiques et leur utilisation concrète

Les orientations et meilleures pratiques dans l'utilisation des technologies, et particulièrement des technologies de détection, doivent également tenir compte de la façon dont leurs utilisateurs les emploient effectivement dans la pratique et dont ils agissent envers les personnes soumises à la détection. Une technologie spécifique peut être conforme aux règles de droit, mais son utilisation concrète peut être source de préoccupations. Par ailleurs, le développement de nouvelles technologies ou une utilisation différente de technologies existantes peuvent engendrer des situations dans lesquelles leur usage n'est pas réglementé par une loi. De même, un usage particulier d'une technologie peut, sans enfreindre la loi, aller à l'encontre de meilleures pratiques ou de codes de conduite élaborés pour compléter les dispositions légales. La connaissance des réglementations (instruments) dans ce domaine peut fournir des indications au sujet de leur conformité avec le cadre juridique (en particulier les droits fondamentaux et la protection des données) et de ce qui est acceptable or non dans une situation où les dispositions légales font encore défaut.

5. Les technologies de détection des personnes et les données biométriques

Comme la détection des personnes (y compris la surveillance) et les données biométriques sont des questions qui touchent directement les personnes, l'utilisation de ces outils pour améliorer la sécurité en Europe fait actuellement l'objet d'un débat politique sensible. La Commission suggère qu'une étude soit entreprise pour déterminer le cadre juridique régissant les technologies de détection des personnes et l'emploi de données biométriques. Cette étude analyserait les systèmes juridiques des États membres et de l'UE et recenserait ainsi les règles

régissant actuellement la détection des personnes et l'emploi des données biométriques. Une étude de cette nature revêt une importance particulière pour garantir la légalité des solutions technologiques proposées par le secteur privé. Pour le dire simplement, elle aiderait le secteur privé à comprendre les contraintes juridiques et autres auxquelles doivent obéir les solutions technologiques qu'il met au point.

Des études spéciales pourraient également porter sur les niveaux d'acceptation de la surveillance et de l'emploi des données biométriques par la population dans les États membres et dans l'Union. La méthode employée pour réaliser ces études devrait faire en sorte d'éviter toute confusion entre les deux sujets – surveillance et emploi de données biométriques. De telles études pourraient aider l'UE et les gouvernements nationaux à déployer des stratégies de communication adéquates sur ces questions. Sur un plan général, ces deux études apporteraient une contribution supplémentaire au débat politique en Europe sur ces questions importantes.