N° 3695

ASSEMBLÉE NATIONALE

CONSTITUTION DU 4 OCTOBRE 1958

DOUZIÈME LÉGISLATURE

Enregistré à la Présidence de l'Assemblée nationale le 13 février 2007

RAPPORT D'INFORMATION

DÉPOSÉ

PAR LA DÉLÉGATION DE L'ASSEMBLÉE NATIONALE
POUR L'UNION EUROPÉENNE (1),

***sur* les échanges d'informations et la protection des données à caractère personnel dans le cadre de la coopération policière et judiciaire en matière pénale (COM [2005] 475 final/n° E 2977, COM [2005] 490 final/ n° E 2981 et COM [2005] 695 final/n° E 3066)**,

ET PRÉSENTÉ

PAR M. CHRISTIAN PHILIP,

Député.

(1) La composition de cette Délégation figure au verso de la présente page.

La Délégation de l'Assemblée nationale pour l'Union européenne est composée de : M. Pierre Lequiller, *président* ; MM. Jean-Pierre Abelin, Mme Elisabeth Guigou, M. Christian Philip, *vice-présidents* ; MM. François Guillaume, Jean–Claude Lefort, *secrétaires* ; MM. Alfred Almont, François Calvet, Mme Anne-Marie Comparini, MM. Bernard Deflesselles, Michel Delebarre, Bernard Derosier, Nicolas Dupont-Aignan, Jacques Floch, Pierre Forgues, Mme Arlette Franco, MM. Daniel Garrigue, Michel Herbillon, Marc Laffineur, Jérôme Lambert, Robert Lecou, Pierre Lellouche, Guy Lengagne, Louis-Joseph Manscour, Thierry Mariani, Philippe–Armand Martin, Jacques Myard, Christian Paul, Axel Poniatowski, Didier Quentin, André Schneider, Jean-Marie Sermier, Mme Irène Tharin, MM. René-Paul Victoria, Gérard Voisin.

SOMMAIRE

———

Pages

Mesdames, Messieurs,

Depuis les tragiques attentats du 11 septembre 2001, suivis par ceux de Madrid le 11 mars 2004 et de Londres en 2005, l'Union européenne a adopté de nombreuses mesures visant à renforcer la lutte contre le terrorisme. Les échanges d'informations entre les autorités répressives des Etats membres, ainsi qu'entre celles-ci et l'Office européen de police (Europol) et Eurojust, se sont intensifiés et ont été facilités par l'adoption de plusieurs textes.

La directive du 15 mars 2006 sur la conservation des données de communication[(1)], la décision-cadre du 18 décembre 2006 relative à la simplification de l'échange d'informations entre les services répressifs des Etats membres de l'Union européenne[(2)] ou le traité (dit « Schengen Plus ») signé à Prüm le 27 mai 2005 par sept Etats membres en vue d'approfondir la coopération transfrontalière en matière de lutte contre le terrorisme, la criminalité transfrontalière et la migration illégale[(3)], illustrent cette tendance générale au renforcement des échanges d'informations en matière répressive.

Plusieurs propositions en cours d'examen par le Conseil et le Parlement européen, relatives au système d'information Schengen de deuxième génération (SIS), au système d'information sur les visas (VIS) et au principe de disponibilité des informations par exemple, accentueront cette orientation. D'autres projets, pas encore

---

(1) Directive 2006/24/CE du 15 mars 2006 sur la conservation de données générées ou traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public ou de réseaux publics de communications.

(2) Décision-cadre 2006/960/JAI du Conseil du 18 décembre 2006 relative à la simplification de l'échange d'informations et de renseignements entre les services répressifs des Etats membres de l'Union européenne.

(3) Traité entre le Royaume de Belgique, la République fédérale d'Allemagne, le Royaume d'Espagne, la République française, le Grand-duché de Luxembourg, le Royaume des Pays-Bas et la République d'Autriche, relatif à l'approfondissement de la coopération transfrontalière, notamment en vue de lutter contre le terrorisme, la criminalité transfrontalière et la migration illégale.

concrétisés par des propositions législatives, tels que le renforcement de l'interopérabilité des bases de données européennes dans le domaine de la justice et des affaires intérieures[4] (Eurodac – le système d'enregistrement des empreintes digitales des demandeurs d'asile, le système d'information sur les visas et le système d'information Schengen, en particulier), vont dans le même sens.

Cette évolution rend indispensable l'adoption d'un cadre juridique commun, garantissant une protection efficace des données à caractère personnel dans le cadre de la coopération policière et judiciaire pénale européenne.

Le cadre actuel apparaît en effet insuffisant, la directive 95/46/CE ne s'appliquant pas au traitement des données à caractère personnel mis en œuvre pour l'exercice d'activités qui ne relèvent pas du champ d'application du droit communautaire, telles que la coopération policière et pénale, qui relève du « troisième pilier » (Titre VI du traité sur l'Union européenne) et non du « premier pilier » communautaire. Cette situation n'est pas satisfaisante. Le droit de l'Union n'est pas en conformité, sur ce point, avec la Charte des droits fondamentaux de l'Union européenne, dont l'article 8 garantit le droit à la protection des données à caractère personnel de toute personne.

C'est pourquoi la Commission a déposé, le 4 octobre 2005, une proposition de décision-cadre relative à la protection des données à caractère personnel traitées dans le cadre de la coopération policière et judiciaire en matière pénale (I)[5]. Ce texte est étroitement lié à la proposition de décision-cadre relative à l'échange d'informations en vertu du principe de disponibilité[6], dont l'adoption ne saurait être envisagée tant qu'un régime cohérent et efficace de protection des données à caractère personnel dans le domaine policier et répressif n'aura pas été adopté (II).

---

[4] Communication de la Commission européenne du 24 novembre 2005 sur le renforcement de l'efficacité et de l'interopérabilité des bases de données européennes dans le domaine de la justice et des affaires intérieures et sur la création de synergies entre ces bases (COM [2005] 597 final).

[5] Proposition de décision-cadre relative à la protection des données à caractère personnel traitées dans le cadre de la coopération policière et judiciaire en matière pénale (COM [2005] 475 final.

[6] Proposition de décision-cadre relative à l'échange d'informations en vertu du principe de disponibilité (COM [2005] 490 final).

I. LA PROPOSITION DE DECISION-CADRE RELATIVE A LA PROTECTION DES DONNEES A CARACTERE PERSONNEL

Cette proposition de décision-cadre vise à répondre aux insuffisances du cadre juridique actuel applicable à la protection des données à caractère personnel, qui n'inclut pas les données échangées dans le cadre de la coopération policière et judiciaire en matière pénale. L'adoption du texte de la Commission constituerait, de ce point de vue, un « *pas en avant considérable* » pour la protection des données, pour reprendre l'expression du contrôleur européen de la protection des données[(7)], M. Peter Hustinx. Cette adoption est malheureusement retardée par d'importantes divergences de vues entre Etats membres, concernant, en particulier, le champ d'application du texte.

A. Les insuffisances du cadre actuel

Le cadre actuel apparaît insuffisant : la directive 95/46/CE n'inclut en effet pas le traitement des données à caractère personnel à des fins répressives et la convention du Conseil de l'Europe du 28 janvier 1981 est trop générale pour pallier cette lacune. Ces insuffisances ont conduit à la création de plusieurs régimes spécifiques de protection des données pour le système d'information Schengen, Europol, le système d'information des douanes et Eurojust. L'adoption d'un cadre commun apparaît, dans ces conditions, indispensable.

[(7)] Le contrôleur européen de la protection des données (CEPD) est une autorité européenne indépendante chargée de contrôler l'application, par les institutions et organes de l'Union, des dispositions communautaires relatives à la protection des données, conformément à l'article 286 TCE. Il a été mis en place par le règlement 45/2001/CE et son statut est fixé par la décision n° 1247/2002/CE du 1er juillet 2002.

1) La directive 95/46/CE n'inclut pas le traitement des données à des fins répressives

Le régime actuel de protection des données à caractère personnel de l'Union européenne repose sur la directive 95/46/CE du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données. Or l'article 3, paragraphe 2, de la directive 95/46/CE exclut expressément de son champ d'application :

- les traitements « *mis en œuvre pour l'exercice d'activités qui ne relèvent pas du champ d'application du droit communautaire, telles que celles prévues par le titre* […] *VI du traité sur l'Union européenne* » ;

- les traitements « *ayant pour objet* […] *les activités de l'Etat relatives à des domaines du droit pénal* ».

En pratique, la plupart des législations nationales de transposition de la directive ont adopté un champ d'application plus étendu, incluant le traitement des données à des fins répressives. Certaines législations nationales ne s'y appliquent cependant pas et il existe d'importantes disparités, s'agissant du régime prévu, entre les législations couvrant ce domaine.

En France, par exemple, la loi n° 2004-801 du 6 août 2004 modifiant la loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, vise également les traitements mis en œuvre à des fins de prévention et de répression des infractions pénales. Elle a cependant adapté le régime applicable à ces opérations aux exigences spécifiques de la lutte contre la criminalité. Ont ainsi été prévues :

- des dérogations spécifiques à l'interdiction de traitement des données de nature sensible, c'est-à-dire notamment des données relatives aux origines raciales et ethniques des personnes ainsi qu'à leurs opinions politiques, philosophiques ou religieuses (article 8 II et IV) ;

- des dérogations aux obligations d'information incombant aux administrations responsables de ces traitements à l'égard des personnes dont les données sont traitées (article 32 V et VI) ;

- des dérogations à la possibilité pour les personnes dont les données sont traitées d'exercer pour un motif légitime un droit d'opposition à l'inclusion de leurs données dans le traitement (article 38) ;

- des limitations au droit d'accès des personnes aux données les concernant incluses dans le traitement (articles 41 et 42 – le droit d'accès est indirect) ;

- des dérogations au pouvoir de la Commission nationale de l'informatique et des libertés (CNIL) d'interrompre un traitement en cas de nécessité urgente de remédier à une violation des droits et libertés des personnes (article 45) ;

- la possibilité de déroger sous certaines conditions à l'interdiction de transfert des données à caractère personnel vers un Etat n'assurant pas un niveau suffisant de protection des données à caractère personnel (article 69).

2) La convention du Conseil de l'Europe du 28 janvier 1981 ne suffit pas à pallier cette lacune.

La convention n° 108 du Conseil de l'Europe du 28 janvier 1981 relative à la protection des personnes à l'égard du traitement automatisé a été ratifiée par l'ensemble des Etats membres. Entrée en vigueur le 1er octobre 1985, elle constitue le premier instrument international contraignant ayant pour objet de protéger les personnes contre l'usage abusif du traitement automatisé des données à caractère personnel et de règlement des flux transfrontaliers de données.

Outre des garanties prévues en ce qui concerne le traitement automatisé des données à caractère personnel, elle proscrit le traitement des données « sensibles » relatives à l'origine raciale, aux opinions politiques, à la santé, à la religion, à la vie sexuelle, aux condamnations pénales, *etc.*, en l'absence de garanties offertes par le droit interne. La Convention garantit également le droit des

personnes concernées de connaître les informations stockées à leur sujet et d'exiger le cas échéant des rectifications. La seule restriction à ce droit est prévue lorsque les intérêts majeurs de l'Etat (sécurité publique, défense, *etc.*) sont en jeu.

La Convention a été complétée par un protocole additionnel, signé à Strasbourg le 8 novembre 2001. Ce texte, entré en vigueur le 1er juillet 2004, vise à renforcer la portée de la convention de 1981 en la complétant sur deux points : il prévoit l'établissement d'autorités de contrôle chargées d'assurer le respect des lois ou règlements introduits par les Etats en application de la Convention, et il précise que les données à caractère personnel ne pourront être transférées vers des pays ou organisations internationales tiers que si elles bénéficient, dans l'Etat ou l'organisation internationale destinataire, d'un niveau de protection adéquat. Ce protocole est en cours de ratification parlementaire par la France, qui se conforme déjà à ses obligations.

La Cour européenne des droits de l'homme a également contribué, par sa jurisprudence au titre de l'article 8 de la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales, à dessiner les contours et à enrichir le droit de la protection des données en Europe.

La Convention de 1981 a joué un rôle pionnier et a constitué une référence importante lors de l'élaboration du régime communautaire de protection des données. Elle a inspiré de nombreuses législations nationales, ainsi que la directive 95/46/CE. La Convention est cependant moins détaillée que le corpus communautaire existant et ne tient pas compte des aspects spécifiques de l'échange de données par des autorités policières et judiciaires. Il existe, sur ce point, une recommandation du Conseil de l'Europe visant à réglementer l'utilisation des données à caractère personnel dans le secteur de la police[(8)], mais elle n'est pas contraignante pour les Etats membres.

Plusieurs tentatives d'harmonisation des règles relatives à la protection des données dans le troisième pilier n'ont pas abouti. Une proposition de résolution sur les règles de protection des données à caractère personnel dans les instruments du troisième pilier de

[(8)] Recommandation n° R (87) 15 du Conseil des ministres du 17 septembre 1987.

l'Union européenne a ainsi été déposée en 2001, mais n'a pas été adoptée. En juin 2003, la présidence grecque a proposé une série de principes généraux sur cette question, dans une note, dont le Conseil « Justice et affaires intérieures » des 5 et 6 juin 2003 s'est contenté de « prendre acte », sans y donner suite.

3) En l'absence de cadre général, des régimes spécifiques de protection ont dû être mis en place.

En l'absence de cadre général relatif à la protection des données dans le troisième pilier, des régimes particuliers de protection des données à caractère personnel ont dû être mis en place par divers instruments. Trois autorités de contrôle communes (ACC) distinctes ont été créées, ainsi qu'un organe de contrôle commun, au sein desquels siège un représentant de la CNIL.

a) La protection des données du système d'information Schengen

Ainsi, la convention d'application de l'accord de Schengen, signée le 19 juin 1990, comporte des dispositions spécifiques sur la protection des données, applicables au système d'information Schengen (SIS). L'autorité de contrôle commune Schengen a été créée afin d'exercer un contrôle technique du fichier central (C-SIS) installé à Strasbourg et de vérifier le respect par les Etats participants des droits accordés aux personnes.

b) La protection des données d'Europol

La convention Europol du 26 juillet 1995 comporte également des règles relatives à la protection des données à caractère personnel. Elle prévoit que les Etats membres doivent assurer dans leur droit interne un niveau de protection au moins équivalent à celui assuré par la Convention du Conseil de l'Europe du 28 janvier 1981, et que toute personne peut formuler une demande à l'autorité nationale compétente afin d'accéder aux données la concernant.

L'office européen de police doit répondre dans un délai de trois mois à la demande transmise par l'autorité nationale, le droit de toute personne d'accéder à ses données ou de les faire vérifier s'exerçant dans le respect du droit de l'Etat membre où la demande

a été faire. La communication des données peut être refusée dans la mesure où cela est nécessaire pour :

- qu'Europol puisse remplir dûment ses fonctions ;

- protéger la sécurité et l'ordre public des Etats membres ;

- lutter contre les infractions criminelles ;

- protéger les droits et les libertés des tiers.

Toute personne est en droit de demander à Europol de rectifier ou d'effacer des données erronées la concernant. Quand les données erronées ou contraires à la convention Europol ont été introduites directement par les Etats membres, c'est à eux de les rectifier ou de les effacer en liaison avec Europol. Europol informe le requérant qu'il a été procédé à la rectification ou à l'effacement des données le concernant. Si le requérant n'est pas satisfait de la réponse d'Europol ou s'il n'a pas obtenu de réponse dans un délai de trois mois, il peut saisir l'autorité de contrôle commune (ACC) mise en place par la Convention.

Cette autorité de contrôle commune indépendante est chargée de surveiller l'activité d'Europol afin de s'assurer que le stockage, le traitement et l'utilisation des données dont disposent les services d'Europol ne portent pas atteinte aux droits des personnes. L'ACC s'acquitte de cette tâche notamment en effectuant des inspections au sein d'Europol.

A côté de l'autorité de contrôle commune, chaque Etat membre désigne une autorité de contrôle nationale chargée de contrôler, dans l'application du droit national, que l'introduction, la consultation, ainsi que la transmission à Europol de données à caractère personnel par cet Etat membre sont licites. Elle assure que les droits des personnes n'en sont pas lésés. Toute personne a le droit de demander à cette autorité nationale de s'assurer que l'introduction et la transmission des données la concernant ainsi que la consultation des données sont licites. Ce droit est régi par le droit national de l'Etat membre auquel appartient l'autorité de contrôle sollicitée.

c) La protection des données du système d'information douanier

La convention sur l'emploi de l'information dans le domaine des douanes du 26 juillet 1995 a mis en place un système d'information automatisé commun répondant aux besoins des douanes, appelé le système d'information des douanes (SID). La convention comporte des règles spécifiques relatives à la protection des données. Elle prévoit que chaque Etat membre qui a l'intention de recevoir des données à caractère personnel ou d'en introduire dans le système d'information des douanes doit adopter une législation nationale de nature à offrir un niveau de protection des données à caractère personnel au moins égal à celui résultant des principes de la convention de Strasbourg de 1981.

Les droits des personnes, notamment leur droit d'accès, s'exercent conformément aux lois, aux réglementations et aux procédures de l'Etat membre dans lequel elles font valoir ces droits. Chaque Etat membre désigne une ou plusieurs autorités de contrôle nationales chargées de la protection des données à caractère personnel afin qu'elles contrôlent indépendamment les données de ce type introduites dans le système d'information des douanes.

Une autorité de contrôle commune est instituée. Elle se compose de deux représentants de chaque Etat membre provenant de l'autorité ou des autorités nationales indépendantes de contrôle de chacun de ces Etats.

d) La protection des données d'Eurojust

La décision du Conseil du 28 février 2002 comporte elle aussi des règles relatives à la protection des données à caractère personnel (complétées par des dispositions du règlement intérieur d'Eurojust relatives au traitement et à la protection des données à caractère personnel, approuvées par le Conseil le 24 février 2005)[(9)].

Elle précise que l'application des principes de la Convention du Conseil de l'Europe de 1981 sur la protection des données doit être garantie et qu'Eurojust peut seulement traiter les données relatives aux personnes qui font l'objet d'une enquête, aux victimes

[(9)] *Cf.* Rapport d'information n° 2103 de la Délégation de l'Assemblée nationale pour l'Union européenne, p. 77 et s.

et aux témoins. Les types de données qui peuvent être utilisées concernent, entre autres, l'identité de la personne (nom, prénom, date et lieu de naissance, nationalité, résidence, profession, *etc.*) et la nature des faits reprochés (qualification pénale, date et lieu des faits, type d'enquête, *etc*.). Les données susmentionnées ne sont accessibles qu'aux membres nationaux, leurs assistants et le personnel autorisé d'Eurojust, dont l'obligation de confidentialité est maintenue au-delà de la cessation de fonction.

Au sein d'Eurojust, un membre du personnel est spécialement désigné pour la protection des données. Il assure, entre autres, le traitement licite, la conservation d'une trace écrite de la transmission ainsi que de la réception des données.

De manière générale, toute personne peut consulter les données personnelles qui la concernent et en demander la rectification ou l'effacement si les données sont erronées ou incomplètes. La personne qui estime avoir subi un préjudice à cause d'un traitement des données incorrect a le droit de déposer une plainte. Eurojust encourt sa responsabilité conformément au droit national de l'Etat membre où il a fixé son siège, et les Etats membres sont responsables conformément à leur droit national. Des limites à la consultation sont prévues en considération des activités d'Eurojust (par exemple afin d'éviter de compromettre une enquête).

Les données ne sont conservées que pour la période strictement nécessaire à la conclusion de l'activité d'Eurojust. En tout état de cause, une vérification périodique est prévue tous les trois ans. Eurojust et les Etats membres protègent les données, en particulier, contre la destruction, la perte, la divulgation, la modification et l'accès illicite.

Un organe indépendant contrôle toutes les activités d'Eurojust afin d'assurer que les données à caractère personnel sont traitées dans le respect de la décision. L'organe de contrôle commun (OCC) se réunit périodiquement et lorsqu'il est convoqué par son président. Celui-ci est désigné par l'Etat membre qui exerce la présidence du Conseil de l'Union européenne.

4) L'adoption d'un cadre commun spécifique à la coopération policière et pénale est indispensable.

Compte tenu de ces insuffisances, l'adoption de normes communes relatives à la protection des données à caractère personnel dans le cadre de la coopération policière et pénale est indispensable et urgente.

De nombreux praticiens de la protection des données l'ont signalé à plusieurs reprises. Les autorités européennes de protection des données (telles que la CNIL en France) et le contrôleur européen de la protection des données (CEPD) ont ainsi adopté, lors de la conférence de printemps qui s'est tenue à Cracovie les 25 et 26 avril 2005, une déclaration appelant à la création d'un nouveau cadre juridique pour la protection des données applicable aux activités relevant du troisième pilier.

La conférence souligne qu'elle a « *conscience de la nécessité d'une coopération renforcée entre les autorités chargées du respect de la loi, au sein de l'Union européenne et avec les pays tiers* », mais souligne qu'il apparaît, dans le même temps, « *évident que la Convention n° 108 du Conseil de l'Europe relative à la protection des données applicable dans l'Union européenne est trop générale pour garantir de façon efficace la protection des données par les autorités en charge du respect de la loi* ». Elle affirme qu'« *étant donné l'obligation de respecter les droits humains et les libertés fondamentales qui incombe à l'Union, les initiatives visant l'amélioration du respect de la loi, tel que le principe de disponibilité (appliqué aux informations qui peuvent être communiquées entre autorités), ne devraient être introduites que sur la base d'un système approprié de dispositions garantissant un niveau élevé de protection des données* ».

La conférence de 2005 a également défini des principes directeurs pour le traitement des données personnelles dans le troisième pilier. Selon elle, « *les principes de la directive 95/46/CE devraient constituer la base d'une législation européenne générale en matière de protection des données. En particulier, concernant ses dispositions juridiques, le principe de licéité, les droits de la personne concernée, le principe des garanties pour leur mise en œuvre doivent être soulignés, et concernant les dispositions institutionnelles, il convient d'insister sur la nécessité de constituer*

un groupe de travail européen composé de représentants des autorités nationales et européennes en charge de la protection des données agissant de manière indépendante et ayant des missions de coopération, de surveillance et de conseil ».

Ces orientations ont été confirmées par la déclaration adoptée lors de la conférence européenne des autorités de protection des données qui s'est tenue à Budapest les 24 et 25 avril 2006. Cette importante contribution des autorités de protection des données a servi de base aux travaux de la Commission européenne lors de l'élaboration de sa proposition de décision-cadre.

B. Le contenu de la proposition de la Commission : un « *pas en avant considérable* » pour la protection des données

Cette proposition de décision-cadre, fondée sur les articles 30 et 31 du traité sur l'Union européenne, vise à établir des normes communes de traitement et de protection des données à caractère personnel dans le cadre de la coopération policière et judiciaire en matière pénale.

Elle a pour objet d'accompagner la mise en œuvre du principe de disponibilité par l'instauration de règles permettant de renforcer la confiance mutuelle, et de garantir que la circulation accrue d'informations qui résultera de ce principe ne se fasse pas au détriment des droits et libertés. Son adoption marquerait un « *pas en avant considérable* » pour la protection des données[(10)].

Termes clés de la proposition de décision-cadre

Autorité compétente : les forces de police, les autorités douanières, judiciaires et les autres autorités compétentes dans les Etats membres dans le domaine de la coopération policière et judiciaire en matière pénale ;

Données à caractère personnel : toute information concernant une personne physique identifiée ou identifiable (personne concernée) ;

Fichier : tout ensemble structuré de données à caractère personnel accessible selon des critères déterminés ;

[(10)] Avis du contrôleur européen de la protection des données du 19 décembre 2005, *JOUE* C47/27 du 25 février 2006.

Responsable du traitement : la personne physique ou morale, l'autorité publique, le service ou tout autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement de données à caractère personnel ;

Sous-traitant : la personne physique ou morale, l'autorité publique, le service ou tout autre organisme qui traite des données à caractère personnel pour le compte du responsable du traitement ;

Traitement : toute opération ou ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliqués à des données de caractère personnel (enregistrement, conversation, modification, *etc.*).

1) Un champ d'application incluant le traitement des données dans un cadre strictement national

La décision-cadre s'appliquerait au transfert de données entre Etats mais également aux traitements de données dans un cadre strictement national. Ce point constitue l'une des principales difficultés soulevées par le texte (*cf. infra*).

Les régimes de protection des données existants pour Europol, Eurojust et le système d'information des douanes ne seraient en revanche pas concernés. Le texte ne vise que les traitements réalisés aux fins de prévention et de détection des infractions pénales, ainsi qu'aux fins d'enquête et de poursuite en la matière. Cela signifie que les données collectées à d'autres fins (par exemple fiscales) n'entreraient pas dans son champ d'application.

2) Conditions générales de licéité du traitement des données

La proposition comporte des règles générales sur le traitement des données à caractère personnel. Les Etats membres doivent assurer, entre autres, que les données à caractère personnel sont traitées de façon loyale et licite, et qu'elles sont collectées à des fins déterminées, explicites et légitimes. Elles doivent être exactes et conservées sous une forme permettant l'identification de la personne concernée pendant la durée nécessaire à la réalisation des finalités pour lesquelles elles ont été collectées.

Le responsable du traitement tient un registre des traitements ou séries de traitements qui poursuivent une même finalité ou des finalités liées. Les Etats membres doivent distinguer clairement les données à caractère personnel, entre autres, si une personne :

- est soupçonnée d'être l'auteur d'une infraction pénale ;

- est condamnée pour une infraction pénale ;

- laisse croire qu'elle commettra une infraction pénale ;

- est susceptible de témoigner ;

- est une victime d'une infraction, *etc.*

Le traitement de données à caractère personnel qui révèlent l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques, l'appartenance syndicale, ainsi que le traitement des données relatives à la santé et à la vie sexuelle sont, en principe, interdits. Le traitement de ces données est possible lorsqu'il est prévu par un texte de loi et absolument nécessaire pour l'accomplissement des tâches légitimes de l'autorité concernée aux fins de prévention et de détection des infractions pénales. Il en est de même si les Etats membres prévoient des garanties spécifiques, par exemple l'accès aux données uniquement par le personnel chargé de l'accomplissement des tâches légitimes.

3) Les droits de la personne concernée

Afin d'assurer les droits de la personne concernée, la proposition prévoit des autorités de contrôle ainsi qu'un groupe de protection des personnes à l'égard du traitement des données à caractère personnel. En principe, la personne concernée doit être informée sur le traitement de ses données. Les Etats membres doivent en outre assurer des recours juridictionnels en cas de violation de droits garantis par le droit national applicable au traitement de données en vertu de la décision-cadre.

a) Une autorité de contrôle dans tous les Etats membres

Les Etats membres assurent qu'une ou plusieurs autorités publiques indépendantes sont chargées de contrôler l'application, sur leur territoire, des dispositions adoptées selon la présente décision-cadre. Il s'agirait naturellement, en France, de la CNIL. Ces autorités exercent leur mission en toute indépendance et leurs décisions peuvent faire l'objet d'un recours juridictionnel.

Les autorités de contrôle sont consultées lors de l'élaboration des mesures réglementaires ou administratives relatives aux droits et libertés des personnes à l'égard du traitement de données en matière pénale. En plus, ces autorités doivent disposer :

- de pouvoirs d'investigation, tels que le pouvoir d'accéder aux données faisant l'objet d'un traitement ;

- de pouvoirs effectifs d'intervention, tels que l'effacement ou la destruction de données ;

- du pouvoir d'ester en justice en cas de violation de dispositions nationales prises en application de la décision-cadre ou du pouvoir de porter ces violations à la connaissance de l'autorité judiciaire.

b) Un groupe de protection des personnes

La proposition prévoit la création d'un groupe de protection des personnes à l'égard des données à caractère personnel, inspiré du groupe mis en place, dans le premier pilier communautaire, par l'article 29 de la directive 95/46/CE, dit « groupe de l'article 29 ». Ce groupe aurait, entre autres, pour mission :

- d'examiner toute question portant sur la mise en œuvre des dispositions nationales prises en application de la présente décision-cadre ;

- de donner un avis sur le niveau de protection dans les Etats membres, dans les pays tiers et dans les instances internationales ;

- de conseiller la Commission et les Etats membres sur tout projet de modification de la décision-cadre.

Composé d'un représentant de l'autorité ou des autorités de contrôle des Etats membres, d'un représentant du contrôleur européen de la protection de données et d'un représentant de la Commission, le groupe a un statut consultatif et agit en toute indépendance.

c) L'information de la personne concernée

Le responsable du traitement des données fournit gratuitement à la personne concernée :

- l'identité du responsable du traitement ou de son représentant ;

- les finalités du traitement des données ;

- la base juridique du traitement ;

- les destinataires des données ;

- le caractère obligatoire ou facultatif de la réponse aux questions ou d'autres formes de coopération, y compris les conséquences éventuelles.

La fourniture de ces informations peut être refusée ou limitée, entre autres, pour permettre au responsable du traitement d'accomplir ses tâches légales de manière satisfaisante ou pour protéger la sécurité et l'ordre public dans un Etat membre. En cas de refus ou limitation de la fourniture des informations, le responsable du traitement informe la personne concernée qu'elle peut introduire un recours devant l'autorité de contrôle. Cette dernière examine si les données ont été traitées correctement et, dans la négative, si toutes les corrections nécessaires ont été apportées. Le recours devant l'autorité de contrôle se fait sans préjudice d'éventuels recours juridictionnels et procédures pénales nationales.

Quand les données ne sont pas collectées auprès de la personne concernée ou ont été obtenues à son insu, le responsable du traitement fournit à cette personne les finalités du traitement, la base

juridique, l'existence d'un droit d'accès aux données, *etc*. Le responsable du traitement communique ces informations dès l'enregistrement des données ou, si une communication de données à un tiers est envisagée, dans un délai raisonnable après la première communication de données. Les informations ne sont pas fournies lorsque la personne concernée dispose déjà de ces informations, ou si la fourniture d'informations se révèle impossible, implique un effort disproportionné ou compromet les enquêtes en cours.

d) Les recours juridictionnels

Les Etats membres assurent que les personnes concernées disposent d'un recours juridictionnel en cas de violation de droits garantis par le droit national applicable au traitement de données en vertu de la présente proposition de décision-cadre. Les personnes qui ont subi un dommage du fait d'un traitement illicite de leurs données ont droit d'obtenir du responsable du traitement de données réparation du préjudice subi. Le responsable du traitement peut être exonéré de sa responsabilité s'il prouve que le fait qui a provoqué le dommage ne lui est pas imputable.

Une autorité compétente qui a reçu des données à caractère personnel de l'autorité compétente d'un autre Etat membre est responsable à l'égard de la personne lésée des dommages causés en raison de l'utilisation de données inexactes ou obsolètes. L'autorité réceptrice des données inexactes transmises par une autre autorité peut recourir à ce dernier pour le remboursement de la totalité du montant payé à titre de dommages et intérêts à la personne lésée.

Les Etats membres prennent les mesures appropriées pour assurer des sanctions effectives, proportionnées et dissuasives à appliquer en cas de violation des dispositions prises en application de la présente décision-cadre.

4) La transmission de données aux autres Etats membres

Les données à caractère personnel ne sont transmises ou mises à la disposition des autres Etats membres que si cela est nécessaire pour l'accomplissement des tâches légitimes de l'autorité émettrice ou réceptrice aux fins de prévention et de détection des infractions

pénales, et d'enquêtes et de poursuites en la matière. Les Etats membres veillent à la qualité et à l'exactitude des données. Chaque transmission et chaque réception automatisée des données à caractère personnel, en particulier par accès direct automatisé, doivent être enregistrées dans un journal (« journalisation ») afin de permettre la vérification ultérieure des motifs justifiant la transmission.

Les données à caractère personnel reçues ou mises à disposition par les autorités compétentes des autres Etats membres ne peuvent faire l'objet d'un traitement ultérieur que pour :

- la finalité spécifique pour laquelle elles ont été transmises ou mises à disposition (auquel cas le consentement préalable de l'Etat ayant transmis n'étant pas requis) ;

- la prévention ou la détection des infractions pénales, ou d'enquêtes ou de poursuites en la matière, avec le consentement préalable de l'Etat émetteur ;

- la prévention de menaces à l'encontre de la sécurité publique ou d'une personne (le consentement de l'Etat émetteur est également requis dans ce cas).

La proposition prévoit également des restrictions en cas de transmission à d'autres autorités compétentes, à des autorités autres que les autorités compétentes et à des personnes privées.

5) La transmission de données aux pays tiers

L'efficacité de la coopération policière et judiciaire à l'intérieur de l'Union dépend de plus en plus de la coopération avec des pays tiers ou des organisations internationales. Il s'agit d'une question délicate, comme l'attestent les difficultés soulevées par la conclusion de l'accord sur la transmission des données relatives aux passagers, dites « PNR », avec les Etats-Unis[(11)].

[(11)] Un premier accord, signé le 28 mai 2004, a été annulé par la Cour de justice européenne car il avait été conclu sur le fondement de l'article 95 du traité instituant la Communauté européenne et de la directive 95/46/CE, alors qu'il relève de la lutte contre le terrorisme, donc du troisième pilier (CJCE, 30 mai 2006, aff. C-317/04 et 318/04). Un nouvel accord provisoire a été conclu le 5 octobre 2006 sur le fondement des articles 24 et 38 du traité sur l'Union européenne (*cf.* rapport d'information n° 3332, pp. 115 et s.).

La proposition précise les conditions dans lesquelles des données à caractère personnel reçues d'un autre Etat membre peuvent être transmises aux autorités compétentes de pays tiers ou à des organisations internationales.

Un tel transfert n'est autorisé que si :

- le transfert fait l'objet d'un obligation ou d'une autorisation légale ;

- le transfert est nécessaire pour atteindre la finalité pour laquelle les données concernées ont été transmises ou mises à disposition, ou à des fins de prévention ou de détection des infractions pénales, ou d'enquêtes ou de poursuites en la matière, ou à des fins de prévention de menaces à l'encontre de la sécurité publique ou d'une personne, sauf lorsque la nécessité de protéger les intérêts ou les droits fondamentaux de la personne concernées l'emporte sur ce type de considérations ;

- l'autorité compétente d'un autre Etat membre ayant transmis les données concernées à l'autorité compétente qui entend ensuite les transmettre, ou les ayant mises à la disposition de celle-ci a donné son consentement préalable à leur transfert ultérieur ;

- le pays tiers ou l'organisation internationale en question assure un « *niveau de protection adéquat* » pour les données transférées. Le transfert peut cependant intervenir, même en l'absence de ce niveau adéquat de protection, à titre exceptionnel et en cas d'absolue nécessité afin de sauvegarder les intérêts essentiels d'un Etat membre ou à des fins de prévention de menaces imminentes graves à l'encontre de la sécurité publique ou d'une ou de plusieurs personnes.

Le « *niveau adéquat* » de protection assuré par un pays tiers est déterminé par la Commission, assistée d'un comité composé de représentants des Etats membres et présidé par un représentant de la Commission. En cas d'avis négatif du comité sur la proposition de la Commission, celle-ci doit soumettre son texte au Conseil, qui peut statuer à la majorité qualifiée dans un délai de deux mois (le Conseil étant réputé approuver la mesure s'il n'a pas statué dans ce délai). Cette procédure s'inspire de celle prévue par la directive

95/46/CE pour le transfert de données à caractère personnel vers des pays tiers.

6) Confidentialité et sécurité du traitement

Toute personne agissant sous l'autorité du responsable du traitement ou du sous-traitant (ou le sous-traitant lui-même), qui accède à des données de caractère personnel les traite seulement sur l'instruction du responsable du traitement, sauf en vertu d'obligations légales. Le responsable du traitement utilise les mesures techniques et d'organisation appropriées pour protéger les données contre la destruction, l'altération, la diffusion ou l'accès non autorisé. En ce qui concerne le traitement automatisé de données, les Etats membres veillent, entre autres, à :

- interdire à toute personne non autorisée d'accéder aux installations utilisées ;

- empêcher que des supports de données ne puissent être lus, copiés, modifiés ou enlevés par une personne non autorisée ;

- empêcher l'introduction non autorisée dans le fichier ainsi que toute prise de connaissance, toute modification ou tout effacement non autorisé des données.

C. Une adoption urgente, retardée par d'importantes divergences de vues entre Etats membres

Les discussions sur la proposition de décision-cadre, déposée par la Commission le 4 octobre 2005, progressent difficilement et la perspective d'un accord semble encore lointaine. La première date butoir pour l'adoption du texte, fixée par le Conseil européen des 15 et 16 juin 2006, à la fin 2006, n'a pas été tenue en dépit des efforts de la présidence finlandaise. Les deux passages du texte au Conseil « justice et affaires intérieures », en avril 2006 sous présidence autrichienne, et en décembre 2006 sous présidence finlandaise, n'ont pas permis de progrès notables. Des divergences de vues entre les Etats membres sur des points aussi essentiels que le champ d'application du texte subsistent en effet, rendant un accord sous présidence allemande peu probable. Plus de

250 réserves des Etats membres restent inscrites dans le projet actuel.

Les principales difficultés soulevées concernent le champ d'application du texte, la transmission des données à caractère personnel aux pays tiers, le traitement ultérieur de données reçues d'un autre Etat membre et la fusion des autorités de contrôle communes (Schengen, Europol, SID et Eurojust) existantes en une autorité de contrôle unique compétente pour l'ensemble du troisième pilier de l'Union.

Les autorités européennes de protection des données ont émis un avis globalement favorable sur le texte, lors de la conférence européenne qu'elles ont tenue à Bruxelles le 24 janvier 2006, mais appellent cependant à la clarification de certaines dispositions. Elles estiment notamment qu'un trop grand nombre d'exemptions sont possibles pour les Etats membres, ce qui va à l'encontre d'une réelle harmonisation de la protection des données dans l'Union, et déplorent que la protection de base puisse être mise de côté exceptionnellement voire simplement pour « *l'accomplissement de tâches légitimes* » des autorités répressives. Elles considèrent également que les mesures de sauvegarde sont insuffisantes pour le traitement des fichiers ADN et des données biométriques, et que les dérogations à l'obligation d'informer les personnes concernées sont trop larges.

1) La décision-cadre devrait-elle se limiter à la transmission transfrontalière de données ou s'étendre aux données recueillies et utilisées dans un contexte strictement national ?

La Commission européenne a opté, dans sa proposition, pour un champ d'application large incluant aussi bien le traitement des données au niveau national que le traitement transfrontière (c'est-à-dire de données échangées entre les Etats membres). La solution retenue sur ce point est similaire à celle figurant dans la directive 95/46/CE, qui s'applique aussi à des données collectées et utilisées dans un contexte national.

De nombreuses délégations, dont la France, soutiennent cette approche et font valoir le caractère artificiel, impraticable et

politiquement inopportun de la distinction entre données nationales et données de coopération internationale. Elles estiment, à juste titre, que toute donnée collectée dans le cadre d'une enquête nationale pourrait, à un stade ultérieur, être échangée avec des autorités d'un autre Etat.

Plusieurs Etats membres (le Danemark, la République tchèque, l'Irlande, le Royaume-Uni et la Suède notamment) s'opposent à l'inclusion dans le champ d'application de la décision-cadre des données traitées dans un contexte purement national. Ils estiment qu'il n'existe pas de base juridique dans le traité sur l'Union européenne autorisant l'Union à légiférer en ce qui concerne la protection des données dans des cas strictement nationaux. A titre subsidiaire, ils estiment que même si une telle base juridique existait, l'intervention de l'Union sur ce sujet serait contraire aux principes de subsidiarité et de proportionnalité.

Le service juridique du Conseil, consulté, a rendu un avis sur cette question le 9 mars 2006.

Il estime, en premier lieu, que les articles 30, 31 et 34 du traité sur l'Union européenne constituent une base juridique suffisante pour adopter une décision-cadre sur la protection des données à caractère personnel applicable également au traitement des données dans un contexte purement national. Ces articles ne sauraient en effet être interprétés dans un sens qui restreindrait leur portée, à savoir le renforcement de la coopération policière et judiciaire, à la réglementation des données à caractère personnel qui sont effectivement échangées entre les autorités compétentes des Etats membres. La compétence de l'Union doit être interprétée, selon le service juridique, à la lumière des objectifs généraux de la coopération policière et judiciaire pénale tels qu'ils sont énoncés à l'article 29 du traité sur l'Union européenne, c'est-à-dire « *offrir aux citoyens un niveau élevé de protection dans un espace de liberté, de sécurité et de justice, en élaborant une action en commun* ».

Le service juridique considère, en second lieu, que l'examen de la conformité de la décision-cadre proposée avec les principes de subsidiarité et de proportionnalité doit être effectué par le Conseil et fait partie intégrante de l'examen global de la proposition. Le service juridique souligne, en particulier, que le principe de subsidiarité est essentiellement un principe politique et subjectif, qui

implique un jugement de valeur. Il rappelle, à l'appui de sa démonstration, que la Cour de justice, qui contrôle le respect du principe dans le cadre du traité instituant la Communauté européenne, n'a jamais annulé un acte pour violation de ce principe.

Cet avis n'a cependant pas convaincu les délégations opposées à l'inclusion du traitement des données à caractère personnel traitées dans un cadre purement national. Le blocage sur ce point reste entier, en dépit des prises de position favorables à l'inclusion de ces données du contrôleur européen de la protection des données, dans son avis du 19 décembre 2005, de la CNIL et de ses homologues européens dans l'avis, précité, du 24 janvier 2006, et du Parlement européen (avec lequel ce texte est adopté en consultation), qui s'est prononcé dans une résolution du 27 septembre 2006 adopté sur le rapport de Mme Martine Roure (PSE, France).

Le rapporteur est favorable à l'inclusion des données à caractère personnel traitées dans un cadre purement national, pour des raisons pragmatiques. Les interrogations de certains Etats membres au sujet du respect des principes de subsidiarité et de proportionnalité sont, certes, légitimes, mais il est difficile, voire impossible, de distinguer, en pratique, les données qui sont susceptibles de faire l'objet à un stade ultérieur d'une transmission transfrontière de celles qui ne le sont pas. Il serait en tout état de cause très complexe et coûteux de mettre en place deux régimes différents de protection des données. Ces deux régimes coexisteraient pour des informations contenues dans un même fichier ou utilisées dans le cadre d'une même enquête ou des mêmes poursuites, ce qui serait difficilement gérable.

2) Le transfert de données à des pays tiers

Cette question très sensible fait également l'objet de fortes divergences entre les Etats membres. Certaines délégations, ainsi que la précédente présidence finlandaise, souhaitent étendre les conditions restrictives posées au transfert de données vers des pays tiers (existence d'une obligation légale, niveau adéquat de protection, respect du principe de finalité, consentement préalable de l'Etat membre ayant transmis) à toutes les données, y compris aux données strictement nationales.

La majorité des Etats membres aimerait, au contraire, que ces conditions ne s'appliquent qu'au transfert de données reçues d'un autre Etat membre, comme le suggérait la Commission dans sa proposition initiale.

Enfin, un troisième groupe d'Etats membres (dont l'Allemagne et les Pays-Bas) voudrait que la question du transfert aux pays tiers ne soit même pas mentionné dans la décision-cadre, afin de préserver la marge de manœuvre des Etats membres sur ce point, en fonction des accords bilatéraux ou multilatéraux auxquels ils sont parties.

A titre de compromis, la présidence allemande a proposé, en janvier 2007, que la décision-cadre se contente de permettre à l'Etat membre qui communique des données à un autre Etat membre de subordonner tout transfert ultérieur à son consentement préalable ou au respect de certaines conditions. En revanche, la décision-cadre ne devrait comporter aucune disposition sur ce point ayant des conséquences sur la conclusion d'accords entre les Etats membres et les Etats tiers, ou sur des accords en vigueur.

Le rapporteur estime que le compromis proposé n'est pas satisfaisant, car l'harmonisation apportée sur ce point essentiel serait minimale. Or, comme le souligne le contrôleur européen de la protection des données dans son avis du 19 décembre 2005, les règles régissant le transfert des données à des pays tiers constituent « *un des principes fondamentaux de la législation en matière de protection des données* ». Tant la directive 95/46/CE que le protocole additionnel à la convention du Conseil de l'Europe de 1981 encadrent strictement ces transferts. De manière similaire, les règles encadrant le transfert à des pays tiers prévues par la décision-cadre devraient englober toutes les catégories de données, y compris nationales, et les conditions posées doivent être exigeantes, afin de s'assurer que les pays tiers destinataires assurent un niveau de protection adéquat.

Le recours à une procédure inspirée de la « comitologie », similaire à celle prévue par la directive 95/46/CE, pour la détermination du « niveau adéquat » de protection assuré par un pays tiers a été supprimé, la plupart des délégations estimant que le recours à une procédure de ce type n'avait pas sa place dans le troisième pilier.

3) Le traitement ultérieur de données reçues d'un autre Etat membre

La Commission propose de ne permettre le traitement ultérieur des données reçues d'un autre Etat membre que pour la finalité spécifique pour laquelle elles ont été transmises ou mises à disposition, ou, si l'Etat émetteur y consent, pour la prévention ou la détection des infractions pénales, ou d'enquêtes ou de poursuites en la matière, ou la prévention de menaces à l'encontre de la sécurité publique ou d'une personne.

Plusieurs Etats membres ont souhaité restreindre les possibilités de traitement ultérieur des données échangées entre les Etats membres. D'autres s'y opposent et souhaitent que les règles s'y appliquant soient les mêmes que celles applicables au niveau national. Les discussions semblent s'orienter vers un compromis :

- ayant étendu la liste des finalités pour lesquelles un traitement ultérieur est autorisé sans le consentement de l'Etat émetteur, selon un libellé inspiré de l'article 23 de la convention du 29 mai 2000 relative à l'entraide judiciaire en matière pénale entre les Etats membres[(12)] ;

- permettant un traitement ultérieur pour toute autre finalité, avec l'accord préalable de l'Etat émetteur ;

- prévoyant que dans les cas revêtant un caractère exceptionnellement sensible, l'Etat émetteur peut exiger que son consentement préalable soit recueilli pour le traitement des données transmises à toute autre fin que celles pour lesquelles elles ont été transmises.

[(12)] Article 23 : Protection des données à caractère personnel : 1. Les données à caractère personnel communiquées au titre de la présente convention peuvent être utilisées par l'Etat membre auquel elles ont été transmises : a) aux fins des procédures auxquelles la présente convention s'applique ; b) aux fins d'autres procédures judiciaires ou administratives directement liées aux procédures visées au point a) ; c) pour prévenir un danger immédiat et sérieux pour la sécurité publique ; d) pour toute autre fin, uniquement après consentement préalable de l'Etat membre qui a transmis les données, sauf si l'Etat membre concerné a obtenu l'accord de la personne concernée. 2. Le présent article s'applique aussi aux données à caractère personnel qui n'ont pas été communiquées mais obtenues d'une autre manière en application de la présente convention. 3. Selon le cas d'espèce, l'Etat membre qui a transmis les données à caractère personnel peut demander à l'Etat membre auquel les données ont été transmises de l'informer de l'utilisation qui en a été faite. […].

4) La fusion des autorités de contrôle communes

La délégation allemande a plaidé, tout au cours des négociations, en faveur d'une fusion des autorités de contrôle communes compétentes, respectivement, pour le système d'information Schengen, Europol, Eurojust et le système d'information douanier. Elle estime que l'existence parallèle de ces organismes de contrôle est synonyme de bureaucratie inutile et empêche les effets de synergie en matière de contrôle de la protection des données. Elle souhaiterait qu'une autorité de contrôle unique soit créée pour le troisième pilier de l'Union européenne, auquel un rôle consultatif pourrait être confié. La décision-cadre couvrirait ainsi l'ensemble du troisième pilier de l'Union.

L'Allemagne a repris cette proposition, en tant que présidence, en la présentant, de manière quelque peu surprenante comme consensuelle, alors que certaines délégations semblent défavorables à cette suggestion.

Le rapporteur est favorable à cette initiative, qui entraînerait une clarification bienvenue, sous réserve que cet ajout ne retarde pas exagérément l'adoption de la décision-cadre.

II. LA PROPOSITION DE DECISION-CADRE RELATIVE AU PRINCIPE DE DISPONIBILITE

Le principe de disponibilité des informations est un nouveau principe juridique, selon lequel les informations nécessaires à la lutte contre la criminalité doivent pouvoir traverser sans entrave les frontières intérieures de l'Union européenne. Ce principe a été affirmé par le programme de la Haye, qui fixe les orientations pour l'espace de liberté, de sécurité et de justice pour la période 2005-2010, adopté par le Conseil européen des 4 et 5 novembre 2004.

Le Conseil européen l'a défini comme signifiant que « *dans l'ensemble de l'Union, tout agent des services répressifs d'un Etat membre qui a besoin de certaines informations dans l'exercice de ses fonctions peut les obtenir d'un autre Etat membre, l'administration répressive de l'autre Etat membre qui détient ces informations les mettant à sa disposition aux fins indiquées et en tenant compte des exigences des enquêtes en cours dans cet autre Etat* ».

Le postulat fondant ce principe est que la prévention de la criminalité grave et la lutte contre celle-ci seraient plus efficaces si les informations collectées par les autorités répressives dans un Etat membre étaient mises plus facilement, plus rapidement et plus directement à la disposition de tous les autres Etats membres.

La mise en œuvre du principe de disponibilité permettrait d'aller au-delà du cadre communautaire actuel applicable aux échanges d'informations entre services répressifs. La proposition de décision-cadre de la Commission apparaît ambitieuse, mais son examen n'a guère progressé en raison des débats relatifs au traité de Prüm, qui traite pour partie des mêmes questions et dont l'intégration dans le cadre de l'Union européenne est envisagée.

A. Le cadre actuel des échanges d'informations reste perfectible.

L'Union européenne a déjà adopté de nombreux textes visant à améliorer les échanges d'informations entre les services répressifs des Etats membres et avec Europol. Ce corpus a en outre été récemment complété par le traité de Prüm (dit « Schengen plus »), signé entre sept Etats membres. Des obstacles subsistent cependant et ce cadre reste perfectible.

1) La convention d'application de l'accord de Schengen ne prévoit pas d'échanges directs.

La convention d'application de l'accord de Schengen du 19 juin 1990 prévoit, en son article 39, que les services de police des Etats parties s'accordent, dans le respect de la législation nationale et de leurs compétences, l'assistance aux fins de la prévention et de la recherche de faits punissables. Elle autorise les échanges d'informations entre les services de police qui en font la demande, mais elle n'oblige pas les Etats membres à répondre à une telle demande. En outre, les demandes et les réponses transitent par les autorités centrales, et les échanges directs entre les agents concernés demeurent exceptionnels.

2) Europol reste insuffisamment alimenté en informations par les services des Etats membres.

La valeur ajoutée de l'office européen de police créé par la Convention Europol du 26 juillet 1995 dépend de la quantité et de la qualité des informations qui doivent lui être transmises par les services compétents des Etats membres.

Le constat dressé par le rapporteur, en mars 2005, dans son rapport sur l'Union européenne et la lutte contre le terrorisme[(13)], selon lequel la contribution d'Europol à la lutte contre le terrorisme reste limitée en raison de la réticence des services à l'alimenter en informations, reste malheureusement d'actualité, en dépit d'une augmentation sensible du nombre de messages échangés entre

[(13)] Rapport d'information n° 2123, *L'Europe face au terrorisme. Quelle valeur ajoutée ?*, mars 2005.

Europol et les services (+ 19,7 % en 2005, avec 180 920 messages échangés) et de la mise en service du système d'information Europol en octobre 2005. La mise en œuvre du principe de disponibilité contribuerait dès lors à renforcer l'efficacité d'Europol.

3) La décision-cadre relative à la simplification de l'échange d'informations ne permet pas un accès en ligne.

La décision-cadre 2006/960/JAI du 18 décembre 2006 relative à la simplification de l'échange d'informations et de renseignements entre les services répressifs des Etats membres est issue d'une initiative suédoise. Cette initiative a fait l'objet d'une présentation détaillée dans le rapport d'information sur l'Union européenne et la lutte contre le terrorisme, précité.

Le texte adopté apporte une réelle plus value, car il harmonise le cadre légal dans lequel s'opère les échanges de données, fixe des délais de réponse impératifs (huit heures en cas d'urgence, une semaine pour les 32 infractions graves figurant à l'article 2, paragraphe 2, de la décision-cadre relative au mandat d'arrêt européen, et 14 jours dans les autres cas) et limite les motifs de refus à trois (atteinte aux intérêt vitaux ou au bon déroulement d'une enquête ou d'une opération de renseignement ou demande clairement disproportionnée ou sans objet au regard des finalités pour lesquelles elles a été demandée).

Il ne va cependant pas aussi loin que la proposition de décision-cadre relative au principe de disponibilité, car il ne prévoit pas un accès en ligne aux informations disponibles et aux données d'index renvoyant à des informations non accessibles en ligne (*cf. infra*), ce qui oblige l'Etat émettant la demande à rechercher partout les informations nécessaires, sans savoir si et où elles sont disponibles avant d'émettre sa demande.

4) La décision du 20 septembre 2005 relative à l'échange d'informations concernant les infractions terroristes

Il convient enfin de signaler la décision 2005/671/JAI du Conseil du 20 septembre 2005 relative à l'échange d'informations concernant les infractions terroristes, qui a été adoptée à la suite des

attentats de Madrid et de Londres. Elle dispose que les Etats membres doivent transmettre à Europol et à Eurojust les informations relatives aux enquêtes, aux poursuites et aux condamnations pénales pour infractions terroristes. Cette décision prévoit également que les Etats membres doivent veiller à ce que les informations en rapport avec des infractions terroristes soient rendues accessibles aux autres Etats membres intéressés.

Ce texte n'inclut pas les services de sécurité et de renseignement dans son champ d'application. C'est pourquoi la Commission a déposé, le 22 décembre 2005, une proposition de décision visant à modifier cette décision[(14)]. Les discussions sur ce texte, sensible pour les Etats membres, n'ont cependant pas encore débuté.

Ce bref panorama démontre que des progrès importants ont été réalisés au cours des dernières années en matière d'échange de données, mais que le cadre juridique actuel reste perfectible, des obstacles subsistant dans ce domaine.

B. Une proposition ambitieuse qui simplifierait considérablement les échanges entre Etats membres.

La proposition de décision-cadre impose aux Etats membres de faire en sorte que les informations utiles à l'action répressive soient partagées avec les autorités compétentes équivalentes des autres Etats membres et à Europol. Son champ d'application est étendu ; elle prévoit un accès direct aux données et limite strictement les motifs de refus.

1) Un champ d'application étendu

La finalité de l'instrument est large, car elle englobe non seulement la détection d'infractions pénales, mais aussi la prévention de telles infractions et les enquêtes relatives à ces infractions.

[(14)] Proposition de décision du Conseil relative à la transmission d'informations résultant des activités des services de sécurité et de renseignement en ce qui concerne les infractions terroristes, (COM [2005] 695 final /n° E 3066).

Six types d'informations sont visés : les données ADN, les empreintes digitales, la balistique, les informations relatives à l'immatriculation des véhicules, les numéros de téléphone et les autres données relatives aux communications (à l'exclusion des données sur le contenu des communications et des données relatives au trafic, à moins que ces dernières ne soient contrôlées par une autorité désignée), et les données d'identification des personnes figurant dans les registres de l'état civil. Les informations extraites des casiers judiciaires des Etats membres ne sont pas visées, car elles font l'objet de la décision 2005/876/JAI du Conseil du 21 novembre 2005[(15)], qui devrait être prochainement remplacée par une décision-cadre[(16)].

2) Un accès direct en ligne aux données

Le texte prévoit que les autorités équivalentes des autres Etats membres auront un accès en ligne aux informations contenues dans les bases de données électroniques auxquelles les autorités compétentes correspondantes de l'Etat membre concerné ont un tel accès.

Pour les autres données, auxquelles un accès direct en ligne n'est pas possible, les Etats membres devront prévoir un accès via un index permettant au pays requérant de savoir si une information l'intéressant existe et de formuler ainsi une demande d'informations complémentaire. L'autorité détenant les informations demandées devra répondre dans un délai de douze heures à compter de la réception de la demande. Elle peut assortir, le cas échéant, la transmission des directives d'utilisation nécessaires pour éviter de compromettre une enquête en cours, protéger une source d'information ou l'intégrité physique d'une personne, ou préserver la confidentialité des informations à tous les stades du traitement. Si une autorisation préalable est nécessaire, elle devra être délivrée dans un délai de douze heures également.

---

(15) *Cf.* rapport d'information n° 2103 de la Délégation pour l'Union européenne, p. 67 et s.

(16) Proposition de décision-cadre du Conseil relative à l'organisation et au contenu des échanges d'informations extraites du casier judiciaire entre les Etats membres, (COM [2005] 690 final).

3) Des motifs de refus limités

Les refus sont strictement limités à quatre motifs :

- éviter de compromettre les enquêtes en cours ;

- protéger une source d'information ou l'intégrité d'une personne physique ;

- préserver la confidentialité des informations à tous les stades du traitement ;

- protéger les droits fondamentaux des personnes dont les données sont traitées.

La proposition prévoit, par ailleurs, une traçabilité de toutes informations, un droit d'accès des personnes concerné à la demande d'informations la concernant, ainsi que la création d'un comité composé de représentants des Etats membres et présidé par un représentant de la Commission.

C. Une articulation à clarifier avec le traité de Prüm

La Commission européenne a souhaité « geler » les discussions relatives à la proposition de décision-cadre en raison de l'intégration, projetée par la présidence allemande, du traité de Prüm dans le cadre de l'Union européenne, celui-ci traitant pour partie des mêmes questions.

1) Des dispositions novatrices en matière d'échanges de données

Le traité signé à Prüm le 27 mai 2005 par sept Etats membres (auquel huit autres Etats membres ont adhéré ou ont annoncé l'intention d'adhérer)[(17)] comporte des dispositions particulièrement

[(17)] Traité entre le Royaume de Belgique, la République fédérale d'Allemagne, le Royaume d'Espagne, la République française, le Grand-duché de Luxembourg, le Royaume des Pays-Bas et la République d'Autriche, relatif à l'approfondissement de la coopération transfrontalière, notamment en vue de lutter contre le terrorisme, la criminalité transfrontalière et la migration illégale. Six autres Etats membres (la Finlande, l'Italie, le Portugal, la Roumanie, la Slovénie et la Suède) ont signé le traité et deux autres (Bulgarie et Grèce) ont annoncé leur intention d'y adhérer.

novatrices en matière d'échanges d'informations, relatives notamment à l'ADN, aux empreintes digitales (données dactyloscopiques) et aux plaques d'immatriculation des véhicules, pour lesquelles un accès automatisé à certains fichiers nationaux est prévu.

Ce traité, dit « Schengen Plus », a été ratifié par l'Allemagne, l'Autriche, l'Espagne et le Luxembourg et est en cours de ratification en France (le projet de loi autorisant sa ratification a été déposé au Sénat le 10 janvier dernier). Un accès mutuel direct et en ligne est prévu pour les registres d'immatriculation des véhicules, tandis que l'accès est indirect, selon une procédure dite « connu/inconnu » (« *hit/no hit* »), qui permet au service ayant lancé une consultation de savoir s'il existe ou non une concordance dans le fichier du partenaire.

L'Autriche et l'Allemagne ont ainsi engagé le premier croisement d'informations automatisé et peuvent, depuis décembre 2006, croiser leurs données ADN respectives. Au cours des six premières semaines, le croisement des données allemandes avec les données autrichiennes a révélé plus de 1 500 concordances, et le croisement réalisé en Autriche avec les données allemandes en a donné 1 400. Dans de nombreuses enquêtes, ces résultats permettront de mettre en relation des traces relevées sur le lieu d'un crime et jusqu'ici non attribuées avec des personnes désormais identifiées.

2) Vers une intégration dans le cadre de l'Union ?

Cette coopération se développe hors du cadre communautaire, et son champ géographique est plus étroit que celui de l'Union. Le traité lui-même prévoit d'ailleurs qu'au plus tard trois ans après son entrée en vigueur, une initiative sera présentée afin de transcrire ses dispositions dans l'ordre juridique de l'Union européenne.

Cette intégration des éléments clés du traité dans le cadre juridique de l'Union européenne (comme cela a été fait pour l'acquis Schengen, par le biais d'un protocole annexé au traité d'Amsterdam) pourrait intervenir plus rapidement. Elle est en effet envisagée par la présidence allemande, dont la suggestion a été bien accueillie par les Etats membres lors du Conseil « justice et affaires intérieures » informel qui s'est tenu à Dresde le 15 janvier 2007.

Certains Etats membres (le Royaume-Uni, la République tchèque, la Pologne et l'Irlande) ont cependant émis des réserves concernant les coûts inhérents à la mise en place de cet accès mutuel. Le ministre allemand de l'Intérieur, M. Schäuble, a souligné que la mise en œuvre du traité en Allemagne a coûté environ 930 000 euros, soit un coût supportable compte tenu des avantages découlant de cet accès mutuel en termes de sécurité. La ventilation des dispositions du traité entre le premier pilier communautaire et le troisième pilier soulèvera également sans doute des difficultés.

Une discussion formelle sur l'intégration du traité de Prüm devrait avoir lieu lors du Conseil « Justice et affaires intérieures » des 15 et 16 février 2007.

3) Un champ cependant moins étendu que la proposition de décision-cadre

Les dispositions du traité de Prüm relatives aux échanges de données ne vont cependant pas aussi loin que celles proposées par la Commission dans la proposition de décision-cadre.

Le mode de consultation prévu, en premier lieu, ne permet un accès direct aux données que pour les registres d'immatriculation des véhicules, les autres données ne pouvant faire l'objet que d'une consultation indirecte du type « connu/inconnu ».

Une deuxième limite est relative au type d'informations concerné, qui se limite aux données ADN, dactyloscopiques et à l'immatriculation des véhicules, alors que la proposition de décision-cadre vise un type de données beaucoup plus large, puisqu'elle englobe aussi la balistique, les numéros de téléphone et les autres données relatives aux communications et les données d'identification des personnes figurant dans les registres de l'état civil.

Il conviendrait de fixer un niveau d'ambition aussi élevé sur ces points que dans la décision-cadre, lors de l'intégration des éléments clés du traité de Prüm dans le cadre de l'Union.

Compte tenu du caractère voisin des questions traitées par ces deux instruments, un « gel » au moins provisoire des discussions sur

la décision-cadre était opportun, afin de clarifier l'articulation des deux instruments.

CONCLUSION

Le développement des échanges d'informations entre les services répressifs des Etats membres est indispensable pour renforcer l'efficacité de la lutte contre le terrorisme et la criminalité organisée. L'échange d'informations est au cœur de la coopération policière et son amélioration est la clé d'une meilleure coopération.

Dans une Union qui se veut une « Communauté de droit », cette intensification des échanges d'informations ne peut cependant se faire que si elle s'accompagne de normes communes en matière de protection des données à caractère personnel.

Les lacunes du cadre juridique actuel, découlant de l'exclusion du troisième pilier de l'Union du champ d'application de la directive 95/46/CE, doivent être comblées au plus vite pour répondre aux exigences de l'article 8 de la Charte des droits fondamentaux de l'Union européenne, selon lequel « *toute personne a droit à la protection des données à caractère personnel la concernant* ».

Il serait regrettable que les divergences de vues des Etats membres au sujet de la proposition de décision-cadre relative à la protection des données conduisent à un texte purement déclaratoire, fondé sur le plus petit dénominateur commun et sans réelle valeur ajoutée, alors qu'il s'agit d'un sujet sensible pour les droits et les libertés des citoyens.

TRAVAUX DE LA DELEGATION

La Délégation s'est réunie le mardi 13 février 2007, sous la présidence de M. Christian Philip, Vice-président, pour examiner le présent rapport d'information.

L'exposé du rapporteur a été suivi d'un débat.

M. Jacques Floch a relevé que ce rapport vient à point pour rappeler combien il est difficile de faire travailler ensemble les services qui ont pour mission de protéger les citoyens. Cela fait pourtant des années que l'on essaie, notamment, de faire travailler les autorités nationales avec Europol. Un précédent rapport d'information de la Délégation, également présenté par M. Christian Philip, avait montré qu'Europol est insuffisamment utilisé. Auparavant, un rapport sur Europol présenté par M. Jacques Floch lui-même avait constaté la méfiance dont faisaient preuve les policiers français à l'égard d'Europol ; quant à l'éventualité d'échanger avec Europol des informations, les policiers français craignaient une certaine « perte en ligne », ne sachant pas si les informations transmises seraient utilisées à bon escient, tandis que la collaboration avec Interpol, basé à Lyon et en français, ne posait pas ce problème.

M. Jacques Floch a souligné qu'il convient, comme le montre le rapport présenté, de faire preuve de vigilance en cette matière. La grande criminalité ignore les frontières et échange des informations en se passant de règles. En revanche, les législateurs se doivent d'encadrer les échanges d'informations car les libertés fondamentales et les libertés individuelles sont en cause : comment les citoyens européens peuvent-ils savoir s'ils sont « référencés » par différents organismes et, si c'est le cas, en quels termes et pour quel usage ?

La presse a révélé des cas d'individus qui, ayant été « fichés » à leur insu, se sont rendus compte à l'occasion de contrôles dans un Etat de l'Union européenne ou dans un Etat tiers (les Etats-Unis en l'occurrence), que ces informations les concernant avaient été transmises à un Etat autre que leur Etat d'origine ; ils se sont alors trouvés, sur la base de ces données, refoulés, questionnés, voire arrêtés. Il y a donc bien un problème de transmission des informations à des Etats tiers. On

sait qu'actuellement les Etats-Unis, depuis les attentats du 11 septembre 2001, sont très sensibles à cette question et ont mis en place des contrôles très stricts à leurs frontières. Ceci pourrait créer des problèmes si un contrôle européen n'est pas mis en place afin de savoir quelles informations ont été diffusées et pour quel usage.

Or les législateurs européens n'ont pour l'heure pas instauré de règles. Si le texte proposé n'est pas adopté, c'est la Cour de justice qui « fera le droit ». Il faut donc effectivement inciter le législateur communautaire et les législateurs nationaux à écrire le droit. On peut espérer que l'Assemblée nationale, lors de la prochaine législature, pourra se prononcer sur ces sujets importants. M. Jacques Floch a conclu que le rapport présenté est d'une grande utilité pour l'information qu'il apporte à la fois sur le problème et sur les solutions préconisées.

M. Jérôme Lambert a indiqué que des données nombreuses circulent, sans que les citoyens en aient une connaissance suffisante. Paradoxalement, aucune distinction n'est faite, notamment, entre auteurs et victimes d'infractions : il suffit parfois d'être la victime dans une affaire criminelle pour que des données personnelles se trouvent enregistrées et diffusées. Et s'agissant de la circulation des données relatives au casier judiciaire, qui peuvent comporter la mention de telle ou telle condamnation, que se passe-t-il le cas échéant lorsqu'une amnistie vient effacer cette mention en France ? La mention de la condamnation est-elle alors également effacée ailleurs ? Quels sont les moyens pour le citoyen concerné de le vérifier dans les 27 pays membres, sachant qu'il est déjà difficile de le faire en France ? Or ceci peut avoir des conséquences graves.

M. Jérôme Lambert a indiqué qu'il partage l'objectif de rendre plus efficace le travail des services de justice et de police contre la criminalité transfrontalière, mais qu'il faut se garder de créer une situation qui rendrait le citoyen complètement démuni face à la toute-puissance de systèmes d'information dont il ne maîtrise ni le flux ni le contenu.

M. Jacques Floch a demandé que les références du texte relatif aux échanges d'informations liées au casier judiciaire soient mentionnées dans le rapport d'information présenté par M. Christian Philip.

Sur proposition du **rapporteur**, la Délégation a ensuite *adopté* les conclusions dont le texte figure ci-après.

CONCLUSIONS ADOPTEES PAR LA DELEGATION

La Délégation pour l'Union européenne,

Vu la proposition de décision-cadre relative à la protection des données à caractère personnel traitées dans le cadre de la coopération policière et judiciaire en matière pénale (COM [2005] 475 final/n° E 2977),

Vu la proposition de décision-cadre relative à l'échange d'informations en vertu du principe de disponibilité (COM [2005] 490 final/n° E 2981),

1. Considère que les avancées réalisées ou envisagées en matière d'échanges d'informations entre les services répressifs des Etats membres doivent s'accompagner des garanties nécessaires en matière de protection des données à caractère personnel ;

<u>I. En ce qui concerne la proposition de décision-cadre relative à la protection des données à caractère personnel</u> :

2. Souhaite l'adoption rapide de la proposition de décision-cadre, car un cadre juridique commun applicable à la protection des données à caractère personnel dans le cadre de coopération policière et judiciaire en matière pénale est indispensable ;

3. Estime que la décision-cadre devrait inclure les données traitées dans un cadre strictement national, sans se limiter aux seules données transférées entre Etats membres, car la distinction entre ces deux types de données serait difficile à mettre en œuvre, toute donnée collectée dans le cadre d'une enquête nationale pouvant être, à un stade ultérieur, échangée avec un autre Etat membre ;

4. Souligne que la décision-cadre devrait encadrer strictement le transfert des données à caractère personnel, y compris nationales,

aux pays tiers, comme l'ont souligné le contrôleur européen de la protection des données et les autorités européennes de protection des données ;

5. Est favorable à la fusion des autorités de contrôle communes en une autorité de contrôle unique compétente pour l'ensemble du troisième pilier de l'Union européenne ;

II. En ce qui concerne la proposition de décision-cadre relative à l'échange d'informations en vertu du principe de disponibilité :

6. Soutient la mise en œuvre du principe de disponibilité, selon lequel les informations nécessaires à la lutte contre la criminalité doivent pouvoir circuler sans entrave au sein de l'Union européenne, sous réserve qu'il s'accompagne d'un cadre juridique commun relatif à la protection des données ;

7. Souhaite que l'articulation de la proposition de décision-cadre avec les dispositions du traité de Prüm relatives aux échanges d'informations soit clarifiée.