CONTRÔLEUR EUROPÉEN DE LA PROTECTION DES DONNÉES

Avis du Contrôleur européen de la protection des données sur

— la proposition de décision du Conseil sur l'établissement, le fonctionnement et l'utilisation du système d'information Schengen de deuxième génération (SIS II) (COM(2005)230 final),

— la proposition de règlement du Parlement européen et du Conseil sur l'établissement, le fonctionnement et l'utilisation du système d'information Schengen de deuxième génération (SIS II) (COM(2005) 236 final) et

— la proposition de règlement du Parlement européen et du Conseil sur l'accès des services des États membres chargés de l'immatriculation des véhicules au système d'information Schengen de deuxième génération (SIS II) (COM(2005) 237 final)

(2006/C 91/11)

LE CONTRÔLEUR EUROPÉEN DE LA PROTECTION DES DONNÉES,

vu le traité instituant la Communauté européenne, et notamment son article 286,

vu la Charte des droits fondamentaux de l'Union européenne, et notamment son article 8,

vu la directive 95/46/CE du Parlement européen et du Conseil 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,

vu le règlement (CE) n° 45/2001 du Parlement européen et du Conseil du 18 décembre 2000 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions et organes communautaires et à la libre circulation de ces données, et notamment son article 41,

vu la demande d'avis formulée par la Commission conformément à l'article 28, paragraphe 2, du règlement (CE) n° 45/2001, reçue le 17 juin 2005,

A ADOPTÉ L'AVIS SUIVANT:

1. INTRODUCTION

1.1. Historique

Le système d'information Schengen (SIS) est un système informatique européen à grande échelle créé pour compenser la suppression des contrôles aux frontières intérieures de l'espace Schengen. Le SIS permet aux autorités compétentes des États membres d'échanger des informations aux fins du contrôle des personnes et des objets aux frontières extérieures ou à l'intérieur du territoire, ainsi que pour la délivrance de visas et de permis de séjour.

La convention de Schengen, qui est un accord intergouvernemental, est entrée en vigueur en 1995. Le SIS prévu par la convention de Schengen a été intégré ultérieurement dans le cadre de l'UE par le traité d'Amsterdam.

Un nouveau système d'information Schengen «de deuxième génération» (SIS II) remplacera le système actuel et permettra d'élargir l'espace Schengen aux nouveaux États membres de l'UE. Ce système comportera en outre de nouvelles fonctionnalités. Les dispositions Schengen, élaborées sous la forme d'un cadre intergouvernemental, seront entièrement transformées en instruments juridiques européens classiques.

Le 1er juin 2005, la Commission européenne a présenté trois propositions en vue de l'établissement du SIS II. Il s'agit des trois propositions suivantes:

— une proposition de règlement fondé sur le titre IV du traité CE (visas, asile, immigration et autres politiques liées à la libre circulation des personnes) qui réglementera les aspects du SIS II relevant du premier pilier (immigration), dénommée ci-après «la proposition de règlement»;

— une proposition de décision fondée sur le titre VI du traité UE (coopération policière et judiciaire en matière pénale) qui réglementera l'utilisation du SIS à des fins relevant du troisième pilier, dénommée ci-après «la proposition de décision»;

— une proposition de règlement fondé sur le titre V (transports) concernant spécifiquement l'accès des services chargés de l'immatriculation des véhicules aux données du SIS; cette proposition sera examinée séparément (cf. point 4.6 ci-dessous).

Il est à noter dans ce contexte que la Commission présentera dans les prochains mois une communication relative à l'interopérabilité et aux synergies renforcées entre les systèmes d'information de l'UE (SIS, VIS, Eurodac).

Le SIS II consiste en une base de données centrale appelée le «système central d'information Schengen» (CS-SIS), dont la Commission assurera la gestion opérationnelle, connectée aux points d'accès nationaux définis par chaque État membre (NI-SIS). Les autorités SIRENE assureront l'échange de toutes les informations supplémentaires (informations rattachées à des signalements introduits dans le SIS II mais non stockées dans celui-ci).

Les États membres alimenteront le SIS II en données relatives à des personnes recherchées en vue de leur arrestation, de leur remise ou de leur extradition, à des personnes recherchées dans le cadre de procédures judiciaires, à des personnes devant faire l'objet d'une surveillance discrète ou d'un contrôle spécifique, à des personnes auxquelles l'entrée doit être refusée à la frontière extérieure et à des objets perdus ou volés. Les «signalements», à savoir des ensembles de données introduites dans le SIS, visent à permettre aux autorités compétentes d'identifier une personne ou un objet.

Le SIS II présente de nouvelles caractéristiques telles qu'un accès élargi (Europol, Eurojust, procureurs nationaux, services chargés de l'immatriculation des véhicules), la mise en relation des signalements, l'ajout de nouvelles catégories de données, y compris les données biométriques (empreintes digitales et photographies), ainsi qu'une plate-forme technique commune avec le Système d'information sur les visas. Ces ajouts ont alimenté pendant des années les discussions sur le changement de finalité du SIS qui, d'outil de contrôle, se muerait en un système d'information et d'enquête.

1.2. **Évaluation générale des propositions**

1. Le CEPD note avec satisfaction qu'il est consulté sur la base de l'article 28, paragraphe 2, du règlement (CE) n° 45/2001. Cependant, vu le caractère contraignant de cette disposition, le présent avis devrait être mentionné dans le préambule des textes.

2. Le CEPD se félicite de ces propositions pour plusieurs raisons. La transformation d'une structure intergouvernementale en instruments du droit européen entraîne plusieurs conséquences positives: la force juridique des dispositions réglementant le SIS II sera précisée, la Cour de justice sera compétente pour interpréter l'instrument relevant du premier pilier et le Parlement européen sera associé au moins partiellement (mais un peu tardivement) au processus.

3. En outre, en ce qui concerne le fond, les propositions contiennent un important volet consacré à la protection des données, avec notamment des améliorations bienvenues par rapport à la situation actuelle. On notera en particulier les mesures en faveur des victimes d'une usurpation d'identité, l'extension du règlement (CE) n° 45/2001 aux opérations de traitement de données réalisées par la Commission dans le cadre des activités relevant du titre VI et une meilleure définition des motifs justifiant l'introduction de signalements de personnes aux fins de non-admission.

4. Il est par ailleurs manifeste qu'un grand soin a été apporté à la rédaction des propositions, dont la complexité reflète la complexité inhérente au système qu'elles réglementent. La plupart des observations formulées dans le présent avis visent à clarifier ou à compléter des dispositions, sans nécessiter un remaniement de l'ensemble.

Néanmoins, malgré cette appréciation globalement positive, il y a lieu de formuler les réserves suivantes:

1. Il est souvent difficile de percevoir l'intention qui motive le texte; l'absence d'un exposé des motifs est très regrettable. Compte tenu de la grande complexité de ces documents, un exposé des motifs aurait été indispensable. Son absence ne laisse parfois d'autre choix au lecteur que de se lancer dans des suppositions.

2. De plus, on ne peut que regretter l'absence d'une analyse d'impact. Le fait que la première version du système soit déjà en place ne justifie pas cette omission, compte tenu des différences considérables entre les deux versions. Il aurait notamment fallu réfléchir davantage aux conséquences de l'introduction de données biométriques.

3. Le cadre juridique de la protection des données est un domaine très complexe qui se fonde sur l'application combinée de la *lex generalis* et de la *lex specialis*. Il faudrait garantir que, même si une législation spécifique est élaborée, le cadre juridique de la protection des données déjà prévu dans la directive 95/46/CE et le règlement (CE) n° 45/2001 reste pleinement applicable. L'application combinée de différents instruments juridiques ne doit pas non plus entraîner de divergences entre les régimes nationaux sur les aspects fondamentaux, ni de dilution du niveau actuel de protection des données.

4. L'extension de l'accès à de nombreuses autorités qui ne poursuivent pas l'objectif initial d'un «contrôle sur les personnes et les objets» devrait s'assortir de garanties plus strictes.

5. Les propositions sont pour une part importante fondées sur d'autres instruments juridiques encore en voie d'élaboration (voire pas encore proposés). Le CEPD, s'il comprend les difficultés que pose l'élaboration d'une législation dans un environnement complexe et en évolution constante tel que celui-ci, juge cette situation inacceptable compte tenu de ses conséquences pour les personnes concernées et de l'insécurité juridique qu'elle génère.

6. La répartition des compétences entre les États membres et la Commission est quelque peu confuse. La clarté à cet égard est indispensable non seulement au bon fonctionnement du système, mais également au contrôle de l'ensemble de celui-ci.

1.3. **Structure de l'avis**

Le présent avis est structuré de la manière exposée ci-après: Pour commencer, le cadre juridique applicable au SIS II est précisé. Ensuite, la finalité du SIS II est définie et les éléments présentant des différences sensibles par rapport au système actuel sont examinés. Le point 5 contient des observations sur les rôles respectifs de la Commission et des États membres en ce qui concerne le fonctionnement du SIS II. Le point 6 traite des droits des personnes concernées par les données. Le point 7 porte sur le contrôle assuré au niveau national et par le CEPD, ainsi que sur la coopération entre les contrôleurs. Le point 8 contient quelques observations et propose des modifications relatives à la sécurité. Les points 9 et 10 traitent respectivement de la comitologie et de l'interopérabilité. Enfin, un résumé des conclusions reprend les principales conclusions relatives à chaque point.

2. CADRE JURIDIQUE APPLICABLE

2.1. Cadre juridique applicable en matière de protection des données du SIS II

Les propositions font référence à la directive 95/46/CE, à la convention 108 du Conseil de l'Europe et au règlement (CE) nº 45/2001 en tant que cadre juridique de la protection des données. Il y a également lieu de tenir compte d'autres instruments.

Afin de clarifier ce cadre et les principaux éléments sur lesquels se fonde le présent avis, il est utile de rappeler ce qui suit:

— Le respect de la vie privée est garanti en Europe depuis l'adoption par le Conseil de l'Europe, en 1950, de la Convention de sauvegarde des droits de l'homme et des libertés fondamentales (dénommée ci-après «CEDH»), dont l'article 8 consacre le «droit au respect de la vie privée et familiale».

  Aux termes de l'article 8, paragraphe 2, de la CEDH, «il ne peut y avoir ingérence d'une autorité publique dans l'exercice de ce droit que pour autant que cette ingérence est prévue par la loi et qu'elle constitue une mesure qui, dans une société démocratique, est nécessaire» à la protection d'intérêts importants. Selon la jurisprudence de la Cour européenne des droits de l'homme, le respect de ces conditions implique des exigences supplémentaires en ce qui concerne la qualité de la base juridique de l'ingérence, la proportionnalité des mesures et la nécessité de garanties adéquates contre les abus.

— Le droit au respect de la vie privée et la protection des données à caractère personnel ont été consacrés plus récemment dans les articles 7 et 8 de la Charte des droits fondamentaux de l'Union européenne. L'article 52 de cette charte prévoit que ces droits peuvent faire l'objet de limitations, étant entendu que des conditions similaires à celles qui sont prévues à l'article 8 de la CEDH doivent être remplies.

— Aux termes de l'article 6, paragraphe 2, du traité UE, l'Union respecte les droits fondamentaux, tels qu'ils sont garantis par la CEDH.

Les trois textes explicitement applicables aux propositions relatives au SIS II sont les suivants:

— La convention nº 108 du Conseil de l'Europe du 28 janvier 1981 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (dénommée ci-après *«convention 108»*) énonce des principes fondamentaux en matière de protection des personnes à l'égard du traitement des données à caractère personnel. Tous les États membres ont ratifié cette convention, qui s'applique également aux activités réalisées dans les domaines policier et judiciaire. La convention 108 est le régime de protection des données qui s'applique actuellement à la convention de Schengen, avec la recommandation R (87) 15 du 17 septembre 1987 du comité des ministres du Conseil de l'Europe visant à réglementer l'utilisation des données à caractère personnel dans le secteur de la police.

— La directive 95/46/CE du Parlement européen et du Conseil 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 (JO L 281, p. 31), dénommée ci-après *«directive 95/46/CE»*. Il convient de noter que dans la plupart des États membres, la législation nationale mettant en œuvre la directive couvre également les opérations de traitement de données réalisées dans les domaines policier et judiciaire.

— Le règlement (CE) nº 45/2001 du Parlement européen et du Conseil du 18 décembre 2000 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions et organes communautaires et à la libre circulation de ces données (JO L 8, p. 1), dénommé ci-après *«règlement (CE) nº 45/2001»*.

L'interprétation de la directive 95/46/CE et du règlement nº 45/2001 est en partie guidée par la jurisprudence pertinente de la Cour européenne des droits de l'homme, conformément à la Convention de sauvegarde des droits de l'homme et des libertés fondamentales de 1950 (CEDH). En d'autres termes, la directive et le règlement, dans la mesure où ils portent sur un traitement de données à caractère personnel susceptible de porter atteinte aux libertés fondamentales et, en particulier, au droit à la vie privée, doivent être interprétés à la lumière des droits fondamentaux. C'est également ce qui ressort de la jurisprudence de la Cour de justice ([1]).

([1]) À cet égard, il est utile de citer l'arrêt de la Cour du 20 mai 2003 rendu en séance plénière dans les affaires jointes C-465/00, C-138/01 et C-139/01, Österreichischer Rundfunk et autres, Recueil 2003, p. I-4989. La Cour y examine une loi autrichienne prévoyant la transmission à la Cour des comptes autrichienne d'informations concernant les revenus des employés du secteur public ainsi que leur publication ultérieure. La Cour fixe un certain nombre de critères, fondés sur l'article 8 de la Convention européenne des droits de l'homme, qu'il convient d'appliquer lors de la mise en œuvre de la directive 95/46/CE, dans la mesure où celle-ci autorise certaines limitations au droit à la vie privée.

Le 4 octobre 2005, la Commission a présenté une «proposition de décision-cadre du Conseil relative à la protection des données à caractère personnel traitées dans le cadre de la coopération policière et judiciaire en matière pénale» [1] (dénommée ci-après *«projet de décision-cadre»*). Cette décision-cadre vise à remplacer la convention 108 en tant que texte de référence pour le projet de décision relative au SIS II, ce qui est susceptible d'avoir une incidence sur le régime de protection des données dans ce contexte (cf. point 2.2.5 ci-dessous).

2.2. **Régime juridique de protection des données du SIS II**

2.2.1. *Observation à caractère général*

La base législative requise pour régir le SIS II comporte des instruments distincts; toutefois, comme rappelé dans les considérants, cela «n'affecte pas le principe selon lequel le SIS II constitue un système d'information unique qui doit fonctionner en tant que tel. Certaines dispositions de ces instruments doivent par conséquent être identiques.»

Les deux documents sont fondamentalement structurés de la même manière, les chapitres I à III étant pratiquement identiques dans les deux textes. Le fait que le SIS II doit être considéré comme un système d'information unique doté de deux bases juridiques différentes se traduit également dans le régime, plutôt complexe, de protection des données.

Le régime relatif de protection des données est partiellement déterminé dans les propositions elles-mêmes: il s'agit d'une «*lex specialis*», complétée par une législation de référence («*lex generalis*») différente pour chaque secteur (Commission, États membres dans le cadre du premier pilier et États membres dans le cadre du troisième pilier).

Compte tenu de cette structure, il importe de déterminer la relation entre règles particulières et règle générale. Dans le cas présent, le CEPD considère la règle particulière comme une application de la règle générale. Il en résulte que la *lex specialis* doit toujours être conforme à la *lex generalis*; elle développe la *lex generalis* (en la précisant ou en la complétant), mais elle n'est pas conçue comme une exception à celle-ci.

Quant à la question de savoir quelle règle il convient d'appliquer dans chaque cas précis, le principe veut que la *lex specialis* s'applique en priorité mais que, lorsqu'elle est muette ou imprécise, il faille se référer à la *lex generalis*.

Cette structure donne lieu à trois combinaisons différentes entre *lex generalis* et *lex specialis*, qui pourraient se résumer comme suit.

2.2.2. *Régime applicable pour la Commission*

Lorsque la Commission est concernée, le règlement (CE) nº 45/2001 s'applique, y compris pour ce qui est de l'intervention du CEPD, que les activités soient menées dans le cadre du premier pilier (proposition de règlement) ou du troisième pilier (proposition de décision). Le considérant 21 de la proposition de décision établit que: «Le règlement (CE) nº 45/2001 (…) s'applique au traitement par la Commission des données à caractère personnel, dans la mesure où ce traitement est mis en œuvre pour l'exercice d'activités qui relèvent en tout ou en partie du champ d'application du droit communautaire. Une partie du traitement des données à caractère personnel du SIS II relève effectivement du champ d'application du droit communautaire.»

Cela s'explique par des raisons pratiques: il serait extrêmement difficile, en ce qui concerne la Commission, d'établir si les données sont traitées dans le cadre d'activités relevant du premier ou du troisième pilier.

En outre, il est non seulement plus logique, d'un point de vue pratique, d'appliquer un seul instrument juridique à toutes les activités menées par la Commission dans le cadre du SIS II, mais cela améliore aussi la cohérence (garantissant, d'après le considérant 21 de la proposition de décision: «une application cohérente et homogène des règles de protection des libertés et droits fondamentaux des personnes à l'égard du traitement des données à caractère personnel»). Par conséquent, le CEPD se félicite que la Commission considère que le règlement (CE) nº 45/2001 s'applique à toutes les activités de traitement de données qu'elle mène dans le SIS II.

2.2.3. *Régime applicable pour les États membres*

La situation est plus complexe en ce qui concerne les États membres. Le traitement des données à caractère personnel en application de la proposition de règlement est régi par celle-ci, ainsi que par la directive 95/46/CE. Le texte du considérant 14 de la proposition de règlement stipule très clairement que la directive doit être considérée comme la *lex generalis*, tandis que le règlement «SIS II» sera la *lex specialis*. Cela entraîne un certain nombre de conséquences qui seront détaillées ci-après.

Pour ce qui est de la proposition de décision, l'instrument juridique de référence (*lex generalis*) en matière de protection des données est la convention 108, ce qui peut signifier une différence importante sur certains points entre les régimes de protection des données applicables dans le premier et dans le troisième pilier.

2.2.4. *Incidence sur le niveau de protection des données*

Le CEPD formule les observations générales ci-après quant à l'architecture ainsi prévue pour la protection des données:

— L'application de la proposition de règlement en tant que *lex specialis* de la directive 95/46/CE (et, de même, celle de la proposition de décision en tant que *lex specialis* de la convention 108) ne devrait jamais conduire à une diminution du niveau de protection des données garanti au titre de la directive ou de la convention. Le CEPD fera des recommandations à cet effet (voir, par exemple, le droit de recours).

[1] Doc. COM (2005) 475 final.

— De même, l'application conjuguée d'instruments juridiques ne peut avoir pour effet d'abaisser le niveau de protection des données garanti dans le cadre de l'actuelle Convention de Schengen (voir, par exemple, les observations formulées ci-après au sujet de l'article 13 de la directive 95/46/CE).

— L'application de deux instruments différents, si elle est nécessaire en raison du droit communautaire, ne devrait pas conduire à des disparités injustifiées dans la protection des données des personnes concernées en fonction du type de données traitées. Cela doit être évité dans toute la mesure du possible. Les recommandations formulées ci-dessous viseront également à améliorer le plus possible la cohérence (voir, par exemple, les pouvoirs des autorités de contrôle nationales).

— Le cadre juridique est à ce point complexe qu'il engendrera très probablement une certaine confusion au niveau de son application pratique. Dans certains cas, il est difficile de distinguer comment la *lex generalis* et la *lex specialis* interagissent, et il serait utile de clarifier cela dans les propositions. En outre, dans cette situation juridique complexe, le CEPD juge très intéressante la suggestion formulée par l'ACC Schengen dans son «avis sur la base juridique proposée pour le SIS II» (27 septembre 2005), qui consisterait à élaborer un vade-mecum énumérant tous les droits existant en relation avec le SIS II et établissant une hiérarchie claire de la législation applicable.

En conclusion, le présent avis s'emploiera à assurer un niveau élevé de protection des données, de cohérence et de clarté afin d'offrir aux personnes concernées la sécurité juridique nécessaire.

2.2.5. *Incidence du projet de décision-cadre sur la protection des données dans le troisième pilier*

La décision-cadre relative à la protection des données dans le troisième pilier remplacera la convention 108 comme instrument de référence pour la protection des données dans le projet de décision SIS II ([1]). Cela n'est pas mentionné dans la proposition, mais découle de la proposition de décision-cadre. Son article 34, paragraphe 2, stipule que «Toute référence à la convention nº 108 du 28 janvier 1981 du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel doit être interprétée comme étant une référence à la présente décision-cadre.». Étant donné qu'il rendra un avis sur le projet de décision-cadre dans les prochaines semaines, le CEPD n'analysera pas son contenu en détail dans le présent avis. Toutefois, chaque fois que l'application de la décision-cadre est susceptible d'avoir une incidence notable sur le régime de protection des données du SIS II, cela sera mentionné.

([1]) Elle remplacera également le régime général de protection des données de la convention de Schengen (articles 126 à 130 de la convention de Schengen). Ce régime ne s'applique pas au SIS.

2.2.6. *Application de l'article 13 de la directive 95/46/CE et de l'article 9 de la convention 108*

L'article 13 de la directive 95/46/CE et l'article 9 de la convention 108 prévoient que les États membres peuvent prendre des mesures législatives visant à limiter la portée des obligations et des droits prévus par ces instruments lorsqu'une telle limitation constitue une mesure nécessaire pour sauvegarder leurs intérêts supérieurs (tels que la sûreté de l'État, la défense, la sécurité publique, etc.) ([2]).

Tous les considérants de la proposition de règlement ainsi que ceux de la proposition de décision indiquent que les États membres pourraient utiliser cette possibilité lors de la mise en œuvre de ces textes au niveau national. Il faudrait dans ce cas imposer une double condition: la mise en œuvre de l'article 13 de la directive 95/46/CE doit être conforme à l'article 8 de la CEDH et elle ne devrait pas conduire à un affaiblissement du régime actuel de protection des données.

Cela est d'autant plus essentiel dans le cas du SIS II, puisque le système doit être prévisible. Étant donné que les États membres partagent leurs données, ils doivent pouvoir savoir avec suffisamment de certitude comment elles seront traitées au niveau national.

Il existe un motif particulier d'inquiétude à cet égard, celui de voir les propositions conduire à une réduction du niveau actuel de protection des données. L'article 102 de la Convention de Schengen prévoit un système dans lequel l'utilisation des données est strictement réglementée et restreinte, même dans le droit national («Toute utilisation de données non conforme aux paragraphes 1 à 4 sera considérée comme détournement de finalité au regard du droit national de chaque partie contractante»). Tant la directive 95/46/CE que la convention 108 prévoient toutefois la possibilité d'inclure dans le droit national des exceptions au principe de limitation de la finalité du traitement des données. Dans ce cas, on s'écarterait du régime actuel de la Convention de Schengen, qui prévoit que la législation nationale ne peut déroger au principe central de limitation de l'objet du traitement des données et de leur utilisation.

L'adoption de la décision-cadre ne changerait rien à ce constat: il s'agit beaucoup plus fondamentalement de préserver strictement le principe de limitation de la finalité du traitement des données du SIS que de veiller à ce que les données soient traitées dans le respect de la décision-cadre.

([2]) Un État membre recourant à cette possibilité de limiter les droits ne peut le faire que dans le respect de l'article 8 de la CEDH, comme indiqué précédemment.

Le CEPD suggère de faire figurer dans les propositions relatives au SIS II (à savoir à l'article 21 de la proposition de règlement et à l'article 40 de la proposition de décision) une disposition ayant le même effet que l'actuel article 102, paragraphe 4, de la Convention de Schengen, visant à limiter la possibilité laissée aux États membres d'autoriser une utilisation des données qui ne soit pas prévue dans les textes sur le SIS II. Une autre solution serait de restreindre explicitement, dans les propositions de décision et de règlement, la portée des exceptions autorisées au titre de l'article 13 de la directive ou de l'article 9 de la convention en disposant, par exemple, que les États membres ne peuvent restreindre que les droits d'accès et à l'information, et non les principes ayant trait à la qualité des données.

3. OBJECTIF

Conformément à l'article 1er des deux documents («établissement et objectif général du SIS II»), le SIS II est institué afin de «permettre aux autorités compétentes des États membres de coopérer en échangeant des informations aux fins de l'exercice de contrôles sur les personnes et les objets» et «contribue à la préservation d'un niveau élevé de sécurité dans un espace sans contrôles aux frontières intérieures entre les États membres».

L'objectif du SIS II est formulé en des termes assez généraux, les dispositions mentionnées ci-dessus ne précisant pas, elles-mêmes, ce que cet objectif recouvre.

L'objectif du SIS II semble bien plus large que celui du SIS actuel tel qu'il est énoncé à l'article 92 de la Convention de Schengen, lequel mentionne expressément l'accès à des «signalements de personnes et d'objets, à l'occasion de contrôles de frontière et de vérifications et autres contrôles de police et de douanes (…)», ainsi que (pour la catégorie de signalement visée à l'article 96) «aux fins de la procédure de délivrance de visas, de la délivrance des titres de séjour et de l'administration des étrangers (…)».

Cet objectif élargi résulte également de l'adjonction au SIS II de nouvelles fonctionnalités et de nouveaux accès qui ne correspondent pas à l'objectif initial des contrôles sur les personnes et les objets, mais correspondent davantage à celui d'un outil d'investigation. En particulier, l'accès est prévu pour des autorités qui utiliseront les données du SIS II en vue de la réalisation de leurs propres objectifs, et non des objectifs du SIS II (voir ci-dessous). En outre l'interconnexion des signalements sera généralisée bien qu'elle constitue une caractéristique typique d'un outil d'investigation policière.

Des questions se posent également au sujet du moteur de recherche biométrique qui devra être mis au point au cours des prochaines années et permettra d'effectuer, dans le système, des recherches qui dépassent les besoins d'un système de contrôle.

En conclusion, les propositions ont une portée bien plus large que le cadre actuel, ce qui nécessite des garanties supplémentaires. À cet égard, le CEPD concentrera son analyse sur les fonctionnalités et les autres éléments constitutifs du SIS II, plutôt que sur la définition large figurant à l'article premier.

4. MODIFICATIONS IMPORTANTES APPORTÉES DANS LE SIS II

Le présent chapitre portera d'abord sur les éléments nouveaux apportés par le SIS II, à savoir l'introduction de la biométrie, la nouvelle conception de l'accès — une attention particulière étant accordée à l'accès d'Europol, d'Eurojust et des services chargés de l'immatriculation des véhicules — la mise en relation des signalements et l'accès des différentes autorités aux données d'immigration.

4.1. Biométrie

Les propositions relatives au SIS II introduisent la possibilité de traiter une nouvelle catégorie de données qui méritent une attention particulière, à savoir les données biométriques. Comme le CEPD l'a déjà souligné dans son avis concernant le système d'information sur les visas [1], le caractère par définition sensible des données biométriques nécessite des garanties spécifiques qui n'ont pas été introduites dans les propositions relatives au SIS II.

D'une manière générale, la tendance à recourir aux données biométriques dans les systèmes d'information à l'échelle de l'UE (VIS, EURODAC, le futur système européen sur les permis de conduire, etc.) s'accroît constamment, sans pour autant s'accompagner d'un examen attentif des risques encourus et des garanties requises.

La résolution sur la biométrie, diffusée récemment par la Conférence internationale des Commissaires à la protection des données et à la vie privée, qui s'est tenue à Montreux [2], a également insisté sur la nécessité d'approfondir la réflexion à cet égard. Jusqu'à présent, l'accent a été uniquement mis sur le fait que la mise au point de normes permettait d'accroître l'interopérabilité entre les systèmes et non d'accroître la qualité des procédés biométriques.

---

[1] Avis du contrôleur européen de la protection des données sur la proposition de règlement du Parlement européen et du Conseil concernant le système d'information sur les visas (VIS) et l'échange de données entre les États membres sur les visas de court séjour, 23 mars 2005, point 3.4.2.

[2] 27ème Conférence internationale des Commissaires à la protection des données et à la vie privée, Montreux, 16 septembre 2005, résolution sur l'utilisation de la biométrie dans les passeports, cartes d'identité et documents de voyage.

Il serait utile d'établir un ensemble d'obligations ou d'exigences communes liées à la spécificité de ces données, ainsi qu'une méthodologie commune concernant leur mise en œuvre. Ces exigences communes pourraient notamment comporter les éléments suivants (dont la nécessité est mise en évidence par les propositions relatives au SIS II):

— **Analyse d'impact ciblée:** il convient de souligner que les propositions n'ont pas fait l'objet d'une analyse d'impact en ce qui concerne l'utilisation de la biométrie ([1]).

— **Importance accordée à la procédure d'enrôlement:** l'origine des données biométriques et la manière dont elles seront recueillies ne sont pas décrites en détail. L'enrôlement est une étape essentielle dans l'ensemble de la procédure d'identification biométrique et on ne peut se limiter à la définir par le biais d'annexes ou de nouvelles discussions au sein de sous-groupes, car elle conditionne directement le résultat final de la procédure, à savoir le niveau du taux de faux rejets ou du taux de fausses acceptations.

— **Accent mis sur le niveau de précision**: l'utilisation de la biométrie à des fins d'identification (comparaison entre un élément et de nombreux autres), qui est présentée dans la proposition comme la mise en œuvre d'un «moteur de recherche des données biométriques» est plus délicate, car les résultats de ce procédé sont moins précis que ceux qui résultent de l'utilisation des données à des fins d'authentification ou de contrôle (comparaison entre deux éléments). L'identification biométrique ne devrait donc pas constituer l'unique procédé d'identification ou l'unique clé d'accès à d'autres informations.

— **Procédure de secours**: des procédures de secours facilement accessibles seront mises en œuvre afin de respecter la dignité des personnes qui auraient pu être identifiées par erreur et d'éviter de leur faire supporter la charge des imperfections du système.

L'utilisation de données biométriques sans une évaluation préalable correcte indique également que l'on surestime la fiabilité de la biométrie. Les données biométriques sont des données «vivantes»qui évoluent avec le temps; les échantillons qui sont stockés dans la base de données ne constituent qu'un cliché instantané d'un élément dynamique. Leur permanence n'est pas absolue et doit être vérifiée. La précision de la biométrie doit toujours être mise en perspective avec d'autres éléments, car elle ne sera jamais absolue.

([1]) L'analyse pourrait être fondée sur ce qu'il est convenu d'appeler les sept piliers de la sagesse en matière de biométrie, cités dans «Biométrie aux frontières: évaluation des impacts sur la société» IPTS, DG-JRC, EUR 21585 EN, point 1.2, page 32.

L'utilisation éventuelle des données du SIS II à des fins d'investigation présente de graves risques pour les personnes concernées si l'on donne une importance accrue ou exagérée aux preuves biométriques, comme l'ont déjà démontré certaines affaires ([2]).

Par conséquent, les propositions devraient tenir compte des capacités réelles de la biométrie à des fins d'identification et attirer l'attention sur celles-ci.

4.2. **Accès aux données du SIS II**

4.2.1. *Une nouvelle conception de l'accès*

Les autorités qui ont accès aux données du SIS sont précisées pour chaque signalement. En principe, une double condition doit être remplie pour accorder l'accès aux données du SIS: l'accès doit être accordé aux autorités dans le respect intégral de l'objectif général du SIS et de l'objectif spécifique de chaque signalement.

Cela résulte de la définition du signalement figurant dans la proposition de règlement et dans la proposition de décision (l'article 3, paragraphe 1, point a, chacun de ces instruments dispose que: «*on entend par* (…) *"signalement", un ensemble de données introduites dans le SIS II pour permettre aux autorités compétentes d'identifier une personne ou un objet en vue de tenir une conduite particulière à son égard*»). L'article 39, paragraphe 2, de la proposition de décision, confirme ce point: «*les données visées au paragraphe 1 ne sont utilisées que pour identifier une personne en vue de l'exécution de la conduite particulière à tenir conformément à la présente décision*». À cet égard, le SIS II conserve les caractéristiques d'un système «hit — no hit» dans lequel chaque signalement est introduit en vue d'un objectif particulier (remise, non-admission, etc.).

Les autorités qui ont accès aux données du SIS sont de facto limitées quant à l'utilisation de ces données, car elles n'y ont en principe accès qu'en vue de tenir une conduite particulière.

Toutefois, certains accès prévus dans les nouvelles propositions rompent avec cette logique, car ils visent à fournir aux autorités des informations, et non à leur permettre d'identifier une personne en vue de tenir une conduite particulière prévue dans le signalement.

([2]) En juin 2004, un avocat de Portland (États-Unis) a été emprisonné pendant deux semaines parce que le FBI avait établi que ses empreintes digitales correspondaient à des empreintes trouvées dans le cadre des attentats de Madrid (sur un sac plastique ayant contenu le détonateur). Il a finalement été établi que la technique de comparaison était défaillante et avait entraîné une erreur d'interprétation.

Il s'agit plus précisément des accès suivants:

— l'accès des autorités compétentes en matière d'asile aux données d'immigration,

— l'accès des autorités habilitées à octroyer le statut de réfugié aux données d'immigration,

— l'accès d'Europol aux signalements concernant l'extradition, la surveillance discrète et les documents volés aux fins de saisie,

— l'accès d'Eurojust aux données concernant l'extradition et la localisation.

Toutes ces autorités présentent les mêmes caractéristiques en ce qui concerne les données du SIS II:

elles ne sont pas en mesure de tenir la conduite particulière visée dans la définition du signalement. L'accès leur est accordé pour leur permettre d'obtenir des informations servant leurs propres objectifs.

Même entre ces autorités, il convient d'établir une distinction entre celles qui ont un accès à des fins qui leur sont propres, mais dans un objectif particulier, et celles pour lesquelles il n'existe aucune précision quant à l'objectif de l'accès (à savoir Europol et Eurojust). Les autorités compétentes en matière d'asile, par exemple, ont un accès en vue d'un objectif particulier, même si ce n'est pas celui qui est mentionné dans le signalement. Elles peuvent avoir accès aux données d'immigration «en vue de déterminer si un demandeur d'asile a séjourné illégalement dans un autre État membre». En revanche, Europol et Eurojust ont accès aux données, contenues dans certaines catégories de signalements, qui sont «nécessaires à l'accomplissement de leur mission».

En résumé, l'accès aux données du SIS II est accordé dans trois cas:

— en vue de donner suite à un signalement,

— pour un objectif ne relevant pas du SIS II, mais bien délimité dans les propositions,

— pour un objectif ne relevant pas du SIS II, mais non précisément défini.

Le CEPD estime que plus l'objectif de l'accès est général, plus les garanties à mettre en œuvre doivent être rigoureuses. On précisera ci-dessous les garanties générales, avant d'aborder la situation particulière d'Europol et d'Eurojust.

4.2.2. *Conditions d'octroi de l'accès*

1. L'accès ne peut, en tout état de cause, être accordé que s'il est compatible avec l'objectif général du SIS II et conforme à sa base juridique.

   En pratique, cela signifie que l'accès aux données d'immigration, dans le cadre de la proposition de règlement, doit viser à soutenir la mise en œuvre des politiques qui sont rattachées à la libre circulation des personnes et font partie de l'acquis de Schengen.

   De même, l'accès aux signalements prévu par la décision doit viser à soutenir la coopération opérationnelle en matière pénale entre les services de police et les autorités judiciaires.

   À cet égard, le CEPD attire l'attention sur le chapitre concernant l'accès au SIS II par les services chargés de délivrer les certificats d'immatriculation (voir point 4.6 ci-dessous).

2. Il faut prouver la nécessité d'accéder aux données du SIS II, et démontrer qu'il est impossible ou très difficile d'obtenir les données par d'autres moyens, moins intrusifs. Ce point aurait dû être mentionné dans un exposé des motifs, dont l'absence est, le CEPD le répète, très regrettable.

3. L'utilisation qui sera faite des données doit être définie de manière explicite et restrictive.

   Par exemple, les autorités compétentes en matière d'asile ont accès aux données d'immigration «en vue de déterminer si un demandeur d'asile a séjourné illégalement dans un autre État membre». En revanche, Europol et Eurojust ont accès aux données, contenues dans certaines catégories de signalements, qui sont «nécessaires à l'accomplissement de leur mission», formulation qui n'est suffisamment précise (voir ci-dessous).

4. Les conditions d'accès doivent être correctement définies et délimitées. En particulier, seuls les services directement concernés au sein des organisations appelées à traiter les données du SIS II devraient y avoir accès. Cette obligation énoncée à l'article 40 de la proposition de décision et à l'article 21, paragraphe 2, de la proposition de règlement devrait être complétée par l'obligation faite aux autorités nationales de conserver une liste actualisée des personnes autorisées à accéder au SIS II. La même règle devrait s'appliquer à Europol et Eurojust.

5. Le fait que ces autorités disposent d'un accès aux données du SIS II ne saurait en aucun cas justifier que soient introduites ou conservées dans le système des données qui ne sont pas utiles pour le signalement particulier dont elles font partie. De nouvelles catégories de données ne peuvent être ajoutées au motif qu'elles seraient utiles à d'autres systèmes d'information. Par exemple, l'article 39 de la proposition de décision prévoit l'introduction, dans les signalements, de données concernant l'autorité signalante. Ces données ne sont pas nécessaires pour tenir une conduite particulière (arrestation, surveillance,…), et la seule raison qui expliquerait leur introduction est probablement qu'elles intéresseraient Europol ou Eurojust. Il faut que le traitement de ces données soit clairement motivé.

6. La durée de conservation des données ne peut être prolongée lorsque cela n'est pas nécessaire en vue de l'objectif pour lequel les données ont été introduites. Cela signifie que même si Europol et Eurojust ont accès à ces données, ce n'est pas un motif suffisant pour les conserver dans le système (par exemple, lorsqu'une personne recherchée a été extradée, les données devraient être supprimées, même si elles pourraient être utiles à Europol). Ici encore, un contrôle attentif sera nécessaire pour garantir le respect de cette règle par les autorités nationales.

4.2.3. *Accès d'Europol et d'Eurojust*

a) *Motifs de l'accès*

L'accès par Europol et Eurojust à certaines données du SIS a déjà fait l'objet de discussions avant qu'il ne soit instauré par la décision du Conseil du 24 février 2005 ([1]). Par rapport à toutes les autres autorités disposant d'un accès en vue de leurs propres objectifs, l'accès leur est octroyé dans des termes particulièrement généraux. Même si l'utilisation des données est définie au chapitre XII de la décision, les motifs justifiant au départ l'attribution d'un accès ne sont pas suffisamment détaillés. Cela est d'autant plus vrai qu'il est probable que les missions d'Europol et d'Eurojust évoluent avec le temps.

Le CEPD insiste pour que la Commission définisse de manière restrictive les missions pour l'accomplissement desquelles l'accès d'Europol et d'Eurojust serait justifié.

b) *Limitation concernant les données*

Afin d'éviter une «pêche aux données» de la part d'Europol et d'Eurojust et de garantir qu'ils n'ont accès qu'aux données «nécessaires à l'accomplissement de leur mission», l'Autorité de contrôle commune de Schengen a suggéré, dans son avis du 27 septembre 2005 concernant les propositions relatives au SIS II, de limiter l'accès d'Europol et d'Eurojust aux données relatives à des personnes dont les noms figurent déjà dans leurs fichiers. On aurait ainsi la garantie qu'Europol et Eurojust ne consultent que les signalements qui les concernent. Le CEPD appuie cette recommandation.

c) *Aspects relatifs à la sécurité*

Le CEPD accueille favorablement l'obligation de tenir un journal de l'ensemble des transactions réalisées par Europol et Eurojust dans le cadre de connexions, ainsi que l'interdiction de copier ou de télécharger des parties du système.

L'article 56 de la proposition de décision prévoit qu'Europol et Eurojust définissent chacun «un ou deux» points d'accès au SIS II. Si l'on pourrait comprendre qu'un État membre ait besoin de plusieurs points d'accès en raison de la décentralisation de ses autorités compétentes, le statut et les activités d'Europol et d'Eurojust ne justifient pas cette demande. Il convient par ailleurs de souligner que, du point de vue de la sécurité, la multiplication des points d'accès accroît le risque d'abus et devrait par conséquent être justifié par des éléments plus probants. Dès lors, en l'absence d'arguments convaincants, le CEPD suggère de n'accorder qu'un point d'accès à Europol et à Eurojust.

4.3. **Mise en relation des signalements**

L'article 26 du règlement et l'article 46 de la décision prévoient que les États membres peuvent mettre en relation des signalements, conformément à leur législation nationale, afin d'établir un lien entre deux ou plusieurs signalements.

Même s'il peut sûrement s'avérer utile de relier des signalements à des fins de contrôle (un mandat d'arrêt concernant un voleur d'automobile peut, par exemple, être lié à un véhicule volé), l'interconnexion des signalements est une caractéristique typique d'un outil d'investigation policière.

La mise en relation de signalements peut avoir des répercussions importantes sur les droits des personnes concernées, ces personnes n'étant plus «évaluées» sur la base de données qui portent uniquement sur elles, mais sur la base de leur association éventuelle avec d'autres personnes. Les personnes dont les données sont mises en relation avec celles de criminels ou de personnes recherchées sont susceptibles d'être traitées avec davantage de suspicion que les autres. En outre, la mise en relation de signalements constitue une extension des fonctions d'investigation du SIS, car cela permettra l'enregistrement de bandes ou de réseaux présumés (par exemple, si des données concernant des immigrés clandestins sont liées à des données relatives à des passeurs). Enfin, puisque l'établissement de liens relève de la législation nationale, il pourra advenir que des liens illégaux dans un État membre soient établis dans un autre, ce qui alimenterait le système en données «illégales».

([1]) Décision 2005/211/JAI du Conseil du 24 février 2005 concernant l'attribution de certaines fonctions nouvelles au Système d'information Schengen, y compris dans le cadre de la lutte contre le terrorisme, JO L 68 du 15.3.2005, p. 44.

Dans les conclusions du Conseil du 14 juin 2004 relatives aux exigences fonctionnelles concernant le SIS II, il est précisé que chaque lien doit avoir des exigences fonctionnelles claires, être en accord avec le principe de proportionnalité et reposer sur une relation définie avec précision. En outre, un lien ne peut porter atteinte aux droits d'accès. En tout état de cause, puisque la mise en relation des signalements constitue une opération de traitement, elle doit être conforme aux dispositions de la législation nationale mettant en œuvre la directive 95/46/CE et/ou la Convention 108.

Les propositions rappellent que l'existence de liens ne doit avoir aucun effet sur les droits d'accès (faute de quoi l'accès serait accordé à des données dont le traitement ne serait pas autorisé par la législation nationale, en violation de l'article 6 de la directive).

Le CEPD souligne qu'il importe d'interpréter strictement l'article 26 de la proposition de règlement, ainsi que l'article 46 de la proposition de décision, ce qui peut notamment être réalisé en précisant que les autorités ne disposant d'aucun droit d'accès à certaines catégories de données ne peuvent accéder aux liens vers ces catégories, mais aussi qu'elles ne doivent même pas avoir connaissance de l'existence de ces liens. La visualisation des liens doit être impossible en l'absence de droit d'accès aux données associées aux liens.

En outre, le CEPD souhaiterait être consulté sur les mesures techniques permettant de s'en assurer.

4.4. **Signalements aux fins de non-admission**

4.4.1. *Motifs d'introduction*

L'utilisation de «signalements de ressortissants de pays tiers aux fins de non-admission» (article 15 du règlement) a des répercussions importantes sur les libertés individuelles. En effet, un individu signalé en vertu de cette disposition se voit interdire l'accès à l'espace Schengen pendant plusieurs années. Jusqu'à présent, ces signalements sont ceux qui ont été le plus souvent utilisés, en termes de nombre de personnes signalées. Au regard des conséquences de ces signalements et du nombre de personnes concernées, il convient d'être très prudent au niveau de leur conception et de leur mise en œuvre. Même si cela vaut également pour d'autres signalements, le CEPD consacrera un chapitre spécifique à ces signalements car ils posent des problèmes particuliers liés aux motifs de leur introduction.

Le nouveau signalement aux fins de non-admission présente des améliorations par rapport à la situation actuelle, mais il n'est pas entièrement satisfaisant car il repose en grande partie sur des instruments qui n'ont pas encore été adoptés, ni même proposés.

Ces améliorations consistent en une description plus précise des motifs d'introduction des données. Compte tenu de la formulation actuelle de la convention de Schengen, il existe de grandes différences entre les États membres en ce qui concerne le nombre de personnes signalées au titre de l'article 96 de cette convention. L'Autorité de contrôle commune de Schengen a réalisé une étude complète ([1]) à ce sujet et a recommandé que les responsables politiques étudient la possibilité d'harmoniser les motifs d'introduction d'un signalement dans les différents États Schengen.

L'article 15 tel qu'il est proposé est plus détaillé dans sa formulation, ce qu'il convient de saluer.

En outre, l'article 15, paragraphe 2, établit une liste des cas dans lesquels des personnes ne peuvent être signalées car elles résident légalement sur le territoire d'un État membre en application de différents statuts. Même si ce mécanisme pouvait être déduit de l'actuelle convention de Schengen, l'expérience a montré que son application différait d'un État membre à l'autre. Cette clarification est donc bienvenue.

Cependant, cette disposition prête également à de sévères critiques, car elle est fondée en grande partie sur un texte qui n'est pas encore adopté, à savoir la directive «relative au retour».

Depuis l'adoption des propositions relatives au SIS II, la Commission a proposé (le 1er septembre 2005) une «directive relative aux normes et procédures communes applicables dans les États membres au retour des ressortissants de pays tiers en séjour irrégulier». Toutefois, ce texte n'étant pas définitif, il ne saurait être considéré comme un fondement valable pour introduire des données dans le système. Cela constituerait en particulier une violation de l'article 8 de la Convention européenne des droits de l'homme, car une ingérence dans la vie privée doit être notamment fondée sur une disposition législative claire et accessible.

Par conséquent, le CEPD engage la Commission à retirer cette disposition ou à la reformuler, sur la base de dispositions législatives existantes, de manière à ce que les personnes puissent savoir exactement quelles sont les mesures que les autorités peuvent prendre à leur égard.

4.4.2. *Accès aux signalements introduits conformément à l'article 15*

L'article 18 précise quelles sont les autorités qui ont accès à ces signalements, et à quelles fins. L'article 18, paragraphes 1 et 2, précise quelles sont les autorités qui ont accès aux signalements introduits sur la base de la directive relative au retour. Cette situation appelle le même commentaire que celui formulé ci-dessus.

([1]) Rapport de l'Autorité de contrôle commune de Schengen concernant une étude du recours aux signalements de l'article 96 dans le Système d'information Schengen, Bruxelles, 20 juin 2005.

L'article 18, paragraphe 3, de la proposition de règlement accorde un accès aux autorités habilitées à octroyer le statut de réfugié en vertu d'une directive qui n'a même pas encore été proposée. Vu l'absence de texte, le CEPD doit à nouveau faire le même commentaire.

4.4.3. *Durée de conservation des signalements introduits conformément à l'article 15*

En vertu de l'article 20, les signalements ne sont pas conservés pour une durée plus longue que la période de non-admission fixée dans la décision (d'éloignement ou de retour). Cette disposition est conforme aux règles applicables en matière de protection des données. En outre, les signalements sont automatiquement effacés à l'expiration d'un délai de cinq ans, sauf décision contraire de l'État membre qui a introduit les données dans le SIS II.

Un contrôle approprié au niveau national devrait garantir qu'il n'y a pas de prolongation automatique injustifiée de la durée de conservation et que les États membres effacent les données avant l'expiration du délai de cinq ans si la période de non-admission est plus courte.

4.5. **Durée de conservation**

Même si le principe régissant la conservation des signalements demeure inchangé (en règle générale, un signalement doit être effacé du SIS II dès que la conduite demandée dans le signalement a été tenue), les propositions conduiront à une prolongation générale de la durée de conservation des signalements.

La convention de Schengen prévoyait que la nécessité de conserver les données devait être examinée au plus tard trois ans après leur intégration (ou un an pour les données intégrées aux fins de surveillance discrète). Les nouvelles propositions prévoient un effacement automatique (auquel l'État membre signalant peut s'opposer) après 5 ans pour les données d'immigration, après 10 ans pour les données relatives aux arrestations, aux personnes disparues et aux personnes recherchées dans le cadre de procédures judiciaires, et après 3 ans pour les personnes devant faire l'objet d'une surveillance discrète.

Même si les États membres devront, en principe, effacer les données lorsque l'objectif du signalement aura été atteint, il s'agit d'une prolongation importante de la durée de conservation maximale (un triplement dans la majorité des cas) qui n'est nullement justifiée par la Commission. Dans le cas des données d'immigration, on doit se borner à supposer que la durée de cinq ans est liée à celle de l'interdiction de réadmission proposée dans la proposition de directive relative au retour. Dans tous les autres cas, le CEPD n'a connaissance d'aucune justification de cette prolongation.

Les éventuelles répercussions d'un signalement dans le SIS sur la vie des personnes concernées peuvent être considérables, ce qui est particulièrement préoccupant dans le cas de signalements de personnes aux fins de surveillance discrète ou de contrôle spécifique, car ces signalements peuvent être introduits sur la base de suspicions.

Le CEPD souhaiterait que la prolongation des durées de conservation des données soit valablement justifiée. En l'absence de justification convaincante, il suggère de les limiter à leur durée actuelle, et insiste tout particulièrement sur le cas des signalements aux fins de surveillance discrète ou de contrôle spécifique.

4.6. **Accès des services chargés de l'immatriculation des véhicules**

Le problème principal réside dans le choix d'une base juridique plus que contestable. La Commission ne justifie pas d'une manière convaincante le recours à une base juridique «transports» relevant du premier pilier pour une mesure qui permettrait à des autorités administratives d'accéder au SIS aux fins de prévenir et de combattre la criminalité (trafic de véhicules volés). La nécessité d'une motivation et d'une base juridique solides pour octroyer l'accès au SIS II a été exposée en détail au point 4.2.2. du présent avis.

Le CEPD renvoie aux observations formulées à ce sujet par l'Autorité de contrôle commune de Schengen dans son avis concernant la base juridique proposée pour le SIS II. Il convient en particulier de suivre sa suggestion visant à modifier la proposition de décision pour y inclure cet accès.

5. **RÔLE DE LA COMMISSION ET DES ÉTATS MEMBRES**

Il faut absolument être précis dans la description et la répartition des responsabilités dans le cadre du SIS II, non seulement pour assurer le bon fonctionnement du système, mais aussi en vue de son contrôle. La répartition des compétences en matière de supervision découlera de la description des responsabilités; il faut donc être d'une précision absolue.

5.1. **Rôle de la Commission**

Le CEPD se félicite de la présence dans les deux propositions du chapitre III, qui décrit le rôle et les responsabilités de la Commission à l'égard du SIS II (dans sa fonction de «gestion opérationnelle»). Cette clarification ne figurait pas dans la proposition sur le VIS. Toutefois, ce chapitre ne suffit pas à lui seul pour donner une description exhaustive du rôle de la Commission. En effet, comme indiqué au chapitre 9 du présent avis, la Commission est également associée à la mise en œuvre et à la gestion du système par le biais de la comitologie.

En matière de protection des données, la Commission joue un rôle qui est déjà reconnu dans les systèmes VIS et Eurodac, puisqu'elle est responsable de la gestion opérationnelle. Cette responsabilité de gestion venant s'ajouter au rôle très important qui lui échoit dans le développement et le fonctionnement du système, il convient de considérer que la Commission joue un rôle de contrôleur sui generis. Comme déjà indiqué dans l'avis du CEPD sur le VIS, ce rôle va bien au-delà du traitement des données tout en étant plus limité que celui d'un contrôleur normal, puisque la Commission n'a pas accès aux données traitées dans le SIS II.

Étant donné que le SIS II sera fondé sur des systèmes complexes, dont certains reposent sur des technologies émergentes, le CEPD insiste pour que l'on renforce la responsabilité de la Commission dans l'amélioration constante des systèmes grâce aux meilleures technologies disponibles en matière de sécurité et de protection des données.

Il convient dès lors d'ajouter, à l'article 12 des propositions, que la Commission devrait régulièrement proposer la mise en œuvre de nouvelles technologies qui soient les plus avancées dans ce domaine et permettront de renforcer le niveau de protection de sécurité et des données, tout en facilitant la tâche des autorités nationales qui ont accès à ces données.

5.2. **Rôle des États membres**

La situation n'est pas très claire en ce qui concerne les États membres, car il est malaisé de savoir quelle(s) autorité(s) fera(ont) fonction de contrôleur(s) des données.

Les propositions décrivent le rôle des Offices nationaux SIS II (pour assurer l'accès des autorités compétentes au SIS II) ainsi que celui des autorités SIRENE (chargées d'échanger toutes les informations supplémentaires). Les États membres doivent également assurer le fonctionnement et la sécurité de leur système national (NS). Il n'est pas dit clairement si cette dernière responsabilité doit incomber à une des autorités susmentionnées. En tout état de cause, il est nécessaire d'apporter des précisions à cet égard.

Pour ce qui est de la protection des données, la Commission et les États membres devraient être considérés comme des contrôleurs conjoints, ayant chacun ses propres responsabilités. Constater cette complémentarité en termes de responsabilités est le seul moyen d'éviter que l'un ou l'autre aspect des activités du SIS II n'échappe au contrôle.

6. **DROITS DES PERSONNES CONCERNÉES**

6.1. **Information**

6.1.1. *Proposition de règlement*

L'article 28 de la proposition de règlement prévoit le droit à l'information de la personne concernée, qui découle principalement de l'article 10 de la directive 95/46. Il s'agit là d'un changement bienvenu par rapport à la situation actuelle, où aucun droit à l'information n'est explicitement prévu dans la convention. On pourrait toutefois encore améliorer les choses, dans le sens indiqué ci-après.

Certaines informations devraient être ajoutées à la liste, ce qui contribuerait à assurer un traitement équitable des personnes concernées ([1]). Ces informations devraient porter sur la durée de conservation des données, l'existence du droit de demander un réexamen ou de faire appel de la décision d'introduire un signalement (dans certains cas, voir article 15, paragraphe 3, de la présente proposition de règlement), la possibilité d'obtenir une aide de l'autorité chargée de la protection des données, ainsi que l'existence de voies de recours.

La proposition de règlement ne mentionne nulle part le moment où les informations doivent être communiquées. Cela pourrait rendre impossible l'exercice de ses droits par la personne concernée. Pour que ceux-ci soient effectifs, le règlement devrait prévoir à quel moment précis les informations doivent être fournies, en fonction de l'autorité qui a introduit le signalement.

Une solution pratique consisterait d'abord à ajouter des d'informations sur le signalement dans la décision qui le motive: une décision judiciaire ou administrative, fondée sur une menace à l'ordre ou la sécurité publics (…), une décision de rapatriement ou une mesure d'éloignement accompagnée d'une interdiction de retour. Cela devrait être ajouté à l'article 28 du règlement.

6.1.2. *Proposition de décision*

L'article 50 de la décision stipule que des informations sont communiquées à la demande de la personne concernée et cite les motifs qui peuvent être invoqués pour refuser de les communiquer. Il est sans doute parfaitement compréhensible que ce droit soit soumis à certaines limites, compte tenu de la nature des données et du cadre dans lequel elles sont traitées.

Toutefois, le droit à l'information ne devrait pas être subordonné à une demande de la personne concernée (il s'agirait dans ce cas d'un droit d'accès). On peut supposer que la nécessité d'une «demande» d'information s'explique par l'éventualité qu'une personne concernée ne puisse être informée car elle n'est pas localisée.

Cette question pourrait se résoudre avantageusement en incluant une clause d'exception au droit à l'information pour les cas où la communication des informations s'avérerait impossible ou impliquerait un effort disproportionné. Il y a lieu de modifier l'article 50 en ce sens.

([1]) Dans le même ordre d'idée, voir l'avis du CEPD sur la création du système d'information sur les visas, point 3.10.1.

Cette solution serait également conforme à l'application du projet de décision-cadre sur la protection des données dans le cadre du troisième pilier.

6.2. **Accès**

Les propositions de règlement et de décision fixent toutes deux des délais pour répondre aux demandes d'accès, ce qui constitue une évolution positive. Toutefois, étant donné que la procédure régissant l'exercice du droit d'accès est fixée au niveau national, on peut se demander comment les délais imposés dans ces propositions peuvent s'accommoder des procédures existantes, en particulier lorsque les États membres ont prévu des délais de réponse plus courts. Il faudrait préciser clairement qu'il y a lieu d'appliquer les délais les plus favorables à la personne concernée.

6.2.1. *Proposition de règlement*

Il est intéressant de noter que les restrictions au droit d'accès («est refusée si elle peut nuire à l'exécution d'une tâche légale se rapportant au signalement ou à la protection des droits et libertés de tiers») qui existent actuellement dans la convention de Schengen ne figurent pas dans la proposition de règlement.

Toutefois, cela est probablement dû à l'applicabilité de la directive 95/46/CE, qui prévoit (en son article 13) la possibilité d'introduire des exceptions dans le droit national. En tout état de cause, il convient de souligner que le recours à l'article 13 dans le droit national en vue de restreindre le droit d'accès devrait toujours se faire dans le respect de l'article 8 de la CEDH, et uniquement dans un nombre limité de cas.

6.2.2. *Proposition de décision*

La proposition de décision reprend les restrictions du droit d'accès qui sont prévues dans la convention de Schengen. La proposition de décision-cadre comporte par essence les mêmes limites au droit d'accès; l'adoption de cet instrument n'apporterait dès lors aucune différence notable sur ce point.

Étant donné que, dans plusieurs États membres, l'accès aux données des services répressifs est «indirect» (c'est-à-dire qu'il s'opère par l'intermédiaire de l'autorité nationale chargée de la protection des données), il serait utile de prévoir que les autorités chargées de la protection des données sont tenues de coopérer activement dans l'exercice du droit d'accès.

6.3. **Droit de réexamen ou d'appel de la décision d'introduire un signalement**

L'article 15, paragraphe 3, du règlement institue un droit d'obtenir le réexamen ou d'introduire un recours devant une autorité judiciaire à l'égard d'une décision d'introduire un signalement, lorsque celle-ci est prise par une autorité administrative. Cet ajout par rapport à la convention de Schengen actuelle est le bienvenu.

Cela souligne la nécessité d'informer complètement et rapidement la personne concernée, comme indiqué au point 6.1 ci-dessus: sans ces informations, ce nouveau droit resterait théorique.

6.4. **Voies de recours**

L'article 30 de la proposition de règlement et l'article 52 de la proposition de décision prévoient que la personne concernée a le droit de former un recours ou de déposer une plainte devant les juridictions d'un État membre si lui sont refusés le droit d'accéder aux données la concernant, de les rectifier ou de les effacer, ou le droit d'obtenir des informations ou d'obtenir réparation.

Les termes («Toute personne ... sur le territoire de tout État membre») laissent entendre que le plaignant doit se trouver physiquement sur le territoire pour pouvoir former son recours devant une juridiction. Cette restriction territoriale ne se justifie pas et pourrait rendre inopérant le droit d'exercer des voies de recours étant donné que, très souvent, le plaignant est amené à intenter une action en justice du fait même qu'il n'obtient pas l'accès au territoire Schengen. En outre, en ce qui concerne la proposition de règlement, étant donné que la directive est la *lex generalis*, il faut tenir compte de son article 22, qui stipule que «toute personne» dispose d'un recours juridictionnel, quel que soit son lieu de résidence. La proposition de décision-cadre ne comporte pas non plus de restriction territoriale. Le CEPD suggère de renoncer à la restriction territoriale figurant à l'article 30 et à l'article 52 précités.

7. **CONTRÔLE**

7.1. **Remarque introductive: partage des responsabilités**

Les propositions répartissent la mission de contrôle entre les autorités de contrôle nationales ([1]) et le CEPD, selon leur sphère de compétence respective, conformément à l'approche adoptée dans les propositions à l'égard du droit applicable et des responsabilités relatives au fonctionnement et à l'utilisation du SIS II, ainsi qu'à la nécessité d'un contrôle effectif.

Dès lors, le CEPD se félicite de cette approche, concrétisée à l'article 31 de la proposition de règlement et à l'article 53 de la proposition de décision. Cependant, afin de mieux comprendre et de préciser les tâches respectives, le CEPD suggère de subdiviser chacun de ces articles en plusieurs dispositions consacrées chacune à un niveau de contrôle, comme cela avait été opportunément réalisé dans la proposition VIS.

([1]) Les autorités de contrôle d'Europol et d'Eurojust sont également concernées, mais dans une moindre mesure.

7.2. **Contrôle par les autorités nationales chargées de la protection des données**

D'après l'article 31 de la proposition de règlement et l'article 53 de la proposition de décision, chaque État membre doit veiller à ce qu'une autorité indépendante contrôle la licéité du traitement des données à caractère personnel du SIS II.

L'article 53 de la proposition de décision prévoit en outre que toute personne a le droit de demander à l'autorité de contrôle de vérifier la licéité d'un traitement de données la concernant. Une disposition semblable n'a pas été introduite dans la proposition de règlement car la directive s'applique comme une *lex generalis*. Par conséquent, il faut considérer que les autorités nationales chargées de la protection des données peuvent exercer, à l'égard du SIS II, toutes les compétences que leur confère l'article 28 de la directive 95/46/CE, y compris la vérification de la licéité d'une opération de traitement de données. L'article 31, paragraphe 1, du règlement décrit leur mission, mais il ne peut constituer une restriction de ces pouvoirs. La reconnaissance de ces compétences devrait être précisée clairement dans le texte de la proposition de règlement.

Quant à la proposition de décision, elle confie des tâches plus étendues aux autorités de contrôle nationales parce que sa *lex generalis* est différente. Toutefois, il ne serait pas judicieux que les autorités de contrôle aient des tâches et des compétences différentes en fonction de la catégorie de données traitées car cela serait très difficile à gérer dans la pratique. Dès lors, il convient d'éviter cette situation, soit en accordant à ces autorités les mêmes pouvoirs dans le texte de la proposition de décision, soit en renvoyant à une autre *lex generalis* (la décision-cadre relative à la protection des données dans le cadre du troisième pilier) qui confère davantage de compétences aux autorités chargées de la protection des données

7.3. **Contrôle exercé par le CEPD**

Le CEPD contrôle que les activités de traitement de données de la Commission sont menées dans le respect des textes des propositions. De même, il devrait pouvoir exercer toutes les compétences que lui attribue le règlement (CE) n° 45/2001, compte tenu toutefois des pouvoirs limités dont jouit la Commission concernant les données elles-mêmes.

Il est utile d'ajouter que, conformément à l'article 46, point f), du règlement (CE) n° 45/2001, le CEPD «coopère avec les autorités nationales de contrôle (…) dans la mesure nécessaire à l'accomplissement de leurs devoirs respectifs». La coopération avec les États membres pour le contrôle du SIS II ne découle pas uniquement des propositions, mais également du règlement (CE) n° 45/2001.

7.4. **Contrôle conjoint**

Les propositions font également ressortir la nécessité de coordonner les activités de contrôle des différentes autorités concernées. L'article 31 de la proposition de règlement et l'article 53 de la proposition de décision disposent que «les autorités de contrôle nationales et le contrôleur européen de la protection des données coopèrent activement. Le contrôleur européen de la protection des données tient une réunion à cet effet au moins une fois par an».

Le CEPD se félicite de cette proposition, qui contient en substance les éléments nécessaires pour établir la coopération, véritablement indispensable, entre les autorités chargées du contrôle au niveau national et au niveau européen. Il convient de souligner que la réunion annuelle prévue dans les propositions doit être considérée comme un minimum.

Ces dispositions (l'article 31 de la proposition de règlement et l'article 53 de la proposition de décision) gagneraient néanmoins à être quelque peu clarifiées quant au contenu de cette coordination. L'autorité de contrôle commune existante est compétente pour examiner les difficultés d'interprétation ou d'application de la convention, pour étudier les problèmes susceptibles de se poser dans l'exercice d'un contrôle indépendant ou du droit d'accès, ainsi que pour élaborer des propositions harmonisées offrant des solutions communes aux problèmes existants.

Les nouvelles propositions ne peuvent pas conduire à une diminution du champ d'application actuel du contrôle commun. Dès lors qu'il est clair que les autorités chargées de la protection des données peuvent exercer à l'égard du SIS II toutes les compétences de contrôle qui leur sont conférées au titre de la directive, la coopération entre ces autorités peut couvrir de larges aspects du contrôle du SIS II, y compris les tâches remplies par l'autorité de contrôle commune existante conformément à l'article 115 de la convention de Schengen.

Toutefois, pour que cela soit tout à fait clair, il serait utile de le réaffirmer explicitement dans le texte des propositions.

8. SÉCURITÉ

La gestion et le maintien d'un niveau de sécurité optimal pour le SIS II constituent une exigence fondamentale afin de garantir une protection suffisante des données à caractère personnel stockées dans la base de données. Pour atteindre ce niveau satisfaisant de protection, il faut mettre en place des mécanismes de sauvegarde appropriés pour faire face aux risques potentiels liés à l'infrastructure du système et aux personnes concernées. Cette question est actuellement abordée dans différents chapitres de la proposition et mérite un meilleur traitement.

Les articles 10 et 13 de la proposition comportent différentes mesures en vue d'assurer la sécurité des données et énumèrent les types d'abus qu'il est nécessaire de prévenir. Le CEPD se félicite de l'inclusion dans ces articles de dispositions relatives au (à l'auto) contrôle systématique des mesures de sécurité.

Toutefois, l'article 59 de la proposition de décision et l'article 34 de la proposition de règlement, qui traitent du suivi et de l'évaluation, ne devraient pas concerner uniquement les aspects de la production, du rapport coût-efficacité et de la qualité des services, mais également le respect des prescriptions légales, en particulier dans le domaine de la protection des données. Par conséquent, le CEPD recommande que le champ d'application de ces articles soit étendu au suivi et à l'établissement de rapports sur la licéité du traitement.

En outre, en complément des dispositions de l'article 10, paragraphe 1, point f), ou de l'article 18 de la proposition de décision, et de l'article 17 de la proposition de règlement concernant l'accès des personnes dûment autorisées aux données, les États membres (ainsi qu'Europol et Eurojust) devraient aussi veiller à ce que des profils d'utilisateurs précis soient accessibles (tenus à la disposition des autorités de contrôle nationales pour effectuer des vérifications). Outre ces profils d'utilisateurs, les États membres doivent établir et tenir à jour en permanence la liste complète des identités des utilisateurs. Cela s'applique *mutatis mutandis* également à la Commission.

Les mesures de sécurité susmentionnées sont complétées par des garanties en matière de suivi et d'organisation. L'article 14 des deux propositions définit les conditions et la finalité de l'établissement de relevés de toutes les opérations de traitement de données effectuées. Ces relevés doivent être conservés non seulement aux fins du suivi en matière de protection des données et pour assurer la sécurité des données, mais aussi pour les vérifications internes régulières du SIS II imposées par l'article 10. Les rapports de vérification interne aideront les autorités de contrôle à s'acquitter efficacement de leur mission et à recenser les points faibles qu'elles examineront en détail dans le cadre de leur propre procédure de vérification.

Comme cela a déjà été dit dans le présent avis, la multiplication des points d'accès au système doit être rigoureusement justifiée car elle augmente automatiquement les risques d'abus. L'article 4, paragraphe 1, point b), des propositions devrait dès lors exiger que la nécessité d'un deuxième point d'accès soit concrètement démontrée.

Les propositions n'expliquent pas clairement la raison d'être des copies nationales du système central et suscitent de graves inquiétudes concernant le niveau global de risque et la sécurité du système:

— la multiplication des copies augmente le risque d'abus (compte tenu notamment de la présence de nouveaux types d'informations telles que les données biométriques);

— les données concernées par ces copies ne sont pas clairement définies;

— les exigences d'exactitude, de qualité et de disponibilité énoncées à l'article 9 représentent un défi technique considérable et entraînent donc une augmentation du coût liée à l'état d'avancement de la technologie disponible;

— le contrôle de ces copies par les autorités nationales nécessitera un surcroît de ressources humaines et financières qui pourraient ne pas toujours être disponibles.

Compte tenu des risques en jeu, le CEPD n'est convaincu ni de la nécessité de réaliser des copies nationales (étant donné les technologies disponibles), ni des avantages que leur utilisation est censée apporter. Il recommande de supprimer la possibilité donnée aux États membres d'utiliser des copies nationales.

Toutefois, si des copies nationales doivent être réalisées, le CEPD rappelle que leur utilisation au niveau national doit obéir au principe de stricte limitation de l'objet du traitement des données. De même, la copie nationale ne peut en aucun cas être interrogée selon des modalités différentes de celles fixées pour la base de données centrale.

La licéité d'une opération de traitement de données à caractère personnel repose sur le strict respect de la sécurité et de l'intégrité des données. Le CEPD exercera un contrôle efficace sur ce traitement s'il peut contrôler non seulement la sécurité des données, mais aussi leur intégrité à travers l'examen des registres d'accès disponibles. Il est dès lors nécessaire d'ajouter «l'intégrité des données» à l'article 14, paragraphe 6.

9. **PROCÉDURE DE COMITOLOGIE**

Les propositions envisagent le recours à des procédures de comité dans plusieurs cas où des décisions à caractère technologique doivent être prises pour la mise en œuvre ou la gestion du SIS II. Comme indiqué dans l'avis sur le VIS et pour les mêmes raisons, ces décisions auront une incidence déterminante sur la mise en œuvre adéquate des principes de finalité et de proportionnalité.

Le CEPD recommande que les décisions ayant une incidence significative sur la protection des données, telles que celles concernant l'accès aux données ou leur introduction, l'échange d'informations supplémentaires, la qualité des données et la compatibilité entre signalements et la conformité technique des copies nationales soient prises par la voie d'un règlement ou d'une décision, de préférence dans le cadre d'une procédure de codécision ([1]).

([1]) Dans le même ordre d'idée, voir le point 3.12 de l'avis du CEPD sur le Système d'information sur les visas et le point 60 de l'avis du CEPD sur la proposition de directive sur la conservation de données traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public, rendu le 26 septembre 2005.

Pour toutes les autres situations ayant des répercussions sur la protection des données, le CEPD devrait avoir la possibilité de rendre un avis sur les choix opérés par ces comités.

Le rôle consultatif du CEPD devrait être mentionné aux articles 60 et 61 de la décision et à l'article 35 du règlement.

Dans le cas plus spécifique des dispositions techniques régissant la mise en relation de signalements (article 26 du règlement et article 46 de la décision), il faut expliquer ce qui justifie des procédures de comité différentes (consultative dans la décision et réglementaire dans le règlement).

10. **INTEROPÉRABILITÉ**

La communication de la Commission sur l'interopérabilité des systèmes émergents de l'UE n'étant toujours pas disponible, il est difficile d'évaluer correctement les avantages qui résulteraient des synergies qui sont prévues mais qui n'ont pas encore été précisées.

À cet égard, le CEPD renvoie à la déclaration du Conseil du 25 mars 2004 sur la lutte contre le terrorisme, dans laquelle le Conseil demande à la Commission de présenter des propositions visant à accroître l'interopérabilité des bases de données européennes et d'envisager la création de synergies entre les systèmes d'information actuels et futurs (SIS, VIS et EURODAC). Il renvoie aussi à la discussion en cours concernant l'organisme auquel pourrait être confiée à l'avenir la gestion des différents grands systèmes (voir également à cet égard le point 3.8. du présent avis).

Le CEPD a déjà déclaré dans son avis sur le Système d'information sur les visas qu'une condition préalable essentielle et déterminante pour garantir l'efficacité ou l'exploitation à grande échelle de systèmes informatiques tels que le SIS II consiste à en assurer l'interopérabilité. Celle-ci permet d'en réduire substantiellement le coût global et d'éviter les doubles emplois que ne manquent pas de provoquer des éléments disparates.

— L'interopérabilité peut aussi contribuer à atteindre l'objectif du maintien d'un niveau élevé de sécurité dans un espace sans contrôles aux frontières intérieures entre États membres par l'application de normes de procédure identiques à tous les éléments constitutifs de cette politique. Toutefois, il est capital de distinguer deux niveaux d'interopérabilité:

  — il est hautement souhaitable d'assurer l'interopérabilité des systèmes des États membres de l'UE; en effet, les signalements transmis par les autorités d'un État membre doivent être compatibles avec ceux qui sont transmis par les autorités de tout autre État membre;

  — par contre, on peut s'interroger sur l'opportunité d'assurer l'interopérabilité entre des systèmes servant à des fins différentes ou avec les systèmes de pays tiers.

Une des précautions pouvant être prises pour limiter l'objet du système et éviter les utilisations détournées («function creep») consiste à utiliser des normes technologiques différentes. En outre, toute forme d'interaction entre deux systèmes distincts devrait faire l'objet d'une documentation complète. L'interopérabilité ne devrait jamais permettre qu'une autorité qui n'est pas habilitée à consulter ou à exploiter certaines données puisse y accéder par l'intermédiaire d'un autre système informatique. Pour autant qu'il soit possible d'en juger à la lecture des propositions, il semble, par exemple, que le SIS II ne comportera pas, dans les premières années, d'un système d'identification automatisé d'empreintes digitales; seule la mise au point d'un futur moteur de recherche biométrique est évoquée. S'il est envisagé un scénario prévoyant l'utilisation d'un tel sytème à partir d'autres systèmes de l'UE, celui-ci devrait faire l'objet d'une description claire et être assorti des précautions requises par ce type de synergie.

Le CEPD tient à souligner une fois encore que l'interopérabilité des systèmes ne peut être instaurée en violation du principe de limitation de la finalité du traitement des données, et que toute proposition dans ce domaine devrait lui être soumise.

11. **SYNTHÈSE DES CONCLUSIONS**

11.1. **Observations d'ordre général**

1. Le CEPD relève avec satisfaction dans ces propositions plusieurs aspects positifs qui, sur certains points, représentent un progrès par rapport à la situation actuelle. Il reconnaît que les dispositions relatives à la protection des données sont d'une manière générale rédigées avec un grand soin.

2. Le CEPD souligne que, malgré sa complexité, le nouveau régime juridique devrait:

   — assurer un niveau élevé de protection des données;

   — être fiable tant pour les citoyens que pour les autorités partageant leurs données;

   — être cohérent dans son application à différents cadres (premier ou troisième pilier).

3. En outre, l'ajout dans le SIS II de nouveaux éléments accroissant son éventuelle incidence sur la vie des personnes devrait être accompagné de précautions plus restrictives, décrites dans l'avis. Par exemple:

— l'accès aux données du SIS II ne peut être octroyé à de nouvelles autorités sans que cela soit absolument justifié. Il convient également de le restreindre autant que possible, tant en ce qui concerne les données accessibles que les personnes autorisées à y accéder;

— la mise en relation des signalements ne peut jamais conduire, même indirectement, à une modification des droits d'accès;

— une mesure législative non adoptée ne peut être considérée comme un motif valable pour introduire des données dans le SIS II (signalements aux fins d'une non-admission);

— il y a lieu de réexaminer le choix de la base juridique en ce qui concerne l'accès des autorités chargées de délivrer des certificats d'immatriculation de véhicules, car cet accès est destiné principalement à lutter contre la criminalité;

— le CEPD reconnaît que l'utilisation des données biométriques pourront améliorer les prestations du système et aider les victimes d'une usurpation d'identité. Toutefois, il semble que les incidences de leur introduction dans le système n'aient pas été analysées de manière assez approfondie et que leur fiabilité ait été surestimée.

11.2. **Observations particulières**

1. Le CEPD se félicite que la Commission reconnaisse que le règlement (CE) nº 45/2001 s'applique à toutes les activités de traitement de données qu'elle mène dans le SIS II, car cela contribuera à assurer une application cohérente et homogène des règles relatives à la protection des droits fondamentaux et des libertés des personnes à l'égard du traitement des données à caractère personnel.

2. Pour garantir une stricte limitation de la finalité du traitement des données au niveau national, le CEPD recommande d'introduire dans les propositions sur le SIS II (plus précisément à l'article 21 de la proposition de règlement et à l'article 40 de la proposition de décision) une disposition ayant le même effet que l'actuel article 102, paragraphe 4, de la convention de Schengen, qui limite les possibilités offertes aux États membres d'autoriser des utilisations des données qui ne sont pas prévues dans les textes relatifs au SIS II.

3. L'octroi à toute autorité de l'accès aux données du SIS II devrait être subordonné à des conditions strictes, à savoir:

— l'accès doit être compatible avec l'objet général du SIS II et conforme à sa base juridique;

— la nécessité d'accéder aux données du SIS II doit être démontrée;

— l'utilisation qui sera faite des données doit être précisée explicitement et d'une manière restrictive;

— les conditions d'accès doivent être bien définies et limitées. En particulier, il devrait exister une liste actualisée des personnes habilitées à accéder au SIS II, y compris pour Europol et Eurojust;

— l'octroi à ces autorités de l'accès au SIS II ne peut en aucun cas justifier le fait qu'elles introduisent ou mettent à jour dans le système des données qui ne sont pas utiles au signalement précis auquel elles participent;

— la durée de conservation des données ne peut être prolongée lorsque cela n'est pas nécessaire aux fins pour lesquelles ces données ont été introduites.

4. Dans le cas particulier d'Europol et d'Eurojust, le CEPD invite instamment la Commission à définir d'une manière restrictive les tâches dont l'accomplissement justifierait l'accès au SIS II. L'accès d'Europol et d'Eurojust devrait en outre être limité aux données relatives à des personnes dont le nom figure déjà dans leurs dossiers. Il est également suggéré de n'accorder qu'un seul point d'accès en ce qui concerne Europol et Eurojust.

5. Pour ce qui est des signalements ayant pour objet la non-admission, les dispositions fondées sur des mesures législatives non encore adoptées devraient être soit retirées, soit reformulées de manière à permettre aux personnes, sur la base de la législation en vigueur, de savoir exactement quelles mesures les autorités peuvent arrêter à leur égard.

6. Les périodes de conservation des données ont été allongées sans qu'aucune justification sérieuse n'ait été apportée à cet égard. En l'absence d'une argumentation convaincante, elles devraient être ramenées à leur durée actuelle, en particulier en ce qui concerne les signalements aux fins d'une surveillance discrète ou de contrôles spécifiques.

7. Le rôle de la Commission est décrit comme celui d'un responsable de la gestion opérationnelle. Joint à la part essentielle qui lui revient dans le développement et la maintenance du système, il doit être considéré comme un rôle de contrôleur *sui generis*. C'est une fonction qui va bien au-delà du simple traitement, mais qui est aussi plus limitée que celle d'un contrôleur ordinaire, la Commission n'ayant pas accès aux données traitées dans le SIS II.

   Dans le cadre de ce rôle, il convient d'ajouter à l'article 12 des deux propositions que la Commission devrait régulièrement proposer la mise en œuvre de nouvelles technologies représentant l'état de la technique dans ce domaine et destinées à accroître les niveaux de protection des données et de sécurité.

8. Au sujet du rôle des États membres, il est nécessaire de préciser quelles autorités font fonction de contrôleurs.

9. En ce qui concerne l'information de la personne concernée:

   — dans la proposition de règlement, il y a lieu d'ajouter un certain nombre d'éléments d'information à la liste: la période de conservation des données, l'existence du droit de demander un réexamen ou de faire appel de la décision d'introduire un signalement, la possibilité d'obtenir l'aide de l'autorité chargée de la protection des données, ainsi que l'existence de voies de recours.

     En outre, pour ce qui est du moment où ces informations sont communiquées, il faudrait ajouter l'obligation de fournir des informations sur le signalement dans la décision sur laquelle celui-ci se fonde à l'origine;

   — dans la proposition de décision, il convient de modifier l'article 50 pour ne pas subordonner le droit à l'information à une demande de la personne concernée.

10. La fixation de délais de réponse à une demande d'accès dans les propositions est la bienvenue. Il y a lieu de préciser que, lorsque le droit national fixe également des délais, ce sont ceux qui sont les plus favorables à la personne concernée qui devraient s'appliquer.

    En outre, il serait utile de prévoir l'obligation pour les autorités chargées de la protection des données de coopérer activement à l'exercice du droit d'accès.

11. Concernant le droit de recours, le CEPD suggère de supprimer la limitation territoriale qui figure aux articles 30 et 52.

12. En ce qui concerne les pouvoirs des autorités nationales chargées de la protection des données:

   — dans le règlement: il faut envisager qu'elles puissent exercer, à l'égard du SIS II, toutes les compétences que leur confère l'article 28 de la directive 95/46/CE; cela devrait être précisé dans le texte de la proposition de règlement;

   — dans la proposition de décision: les autorités de contrôle devraient se voir octroyer les mêmes pouvoirs que dans le règlement et la directive.

13. Pour ce qui est des compétences du CEPD: celui-ci devrait être en mesure d'exercer toutes les compétences qu'il possède au titre du règlement (CE) n° 45/2001, compte tenu, toutefois, des pouvoirs limités de la Commission à l'égard des données proprement dites.

14. Au sujet du contrôle coordonné: les propositions reconnaissent également la nécessité de coordonner les activités de contrôle exercées par les différentes autorités concernées. Le CEPD se réjouit de ce qu'elles comportent en substance les éléments nécessaires à l'instauration de la coopération entre les autorités chargées du contrôle aux niveaux national et européen. Ces dispositions (article 31 de la proposition de règlement et article 53 de la proposition de décision) gagneraient néanmoins à être quelque peu clarifiées quant au contenu de cette coordination.

15. Les articles 10 et 13 de la proposition contiennent différentes mesures en matière de sécurité des données; on ne peut que se réjouir de l'inclusion de dispositions relatives au (ou à l'auto) contrôle systématique des mesures de sécurité.

   — Toutefois, l'article 59 de la proposition de décision et l'article 34 de la proposition de règlement, qui traitent du suivi et de l'évaluation, ne devraient pas porter uniquement sur les aspects relatifs à la production, au rapport coût-efficacité et à la qualité des services, mais aussi sur le respect des prescriptions légales, en particulier dans le domaine de la protection des données. Ces dispositions devraient être modifiées dans ce sens.

   — En outre, il convient de compléter l'article 10, paragraphe 1, point f) ou l'article 18 de la proposition de décision et l'article 17 de la proposition de règlement en ajoutant que les États membres, Europol et Eurojust devraient veiller à ce que des profils précis d'utilisateurs soient accessibles (tenus à la disposition des autorités de contrôle nationales pour effectuer des vérifications). Outre ces profils d'utilisateurs, les États membres doivent établir et tenir à jour en permanence la liste complète des identités des utilisateurs. Cela s'applique également à la Commission.

   — La licéité d'une opération de traitement de données à caractère personnel repose sur le strict respect de la sécurité et de l'intégrité des données. Le CEPD devrait être habilité à vérifier non seulement la sécurité des données, mais également leur intégrité à travers l'examen des registres d'accès disponibles. Il convient dès lors d'ajouter «l'intégrité des données» à l'article 14, paragraphe 6.

16. L'utilisation de copies nationales est une source potentielle de nombreux risques supplémentaires. Le CEPD n'est convaincu ni de la nécessité d'utiliser des copies nationales (compte tenu des technologies disponibles), ni des avantages qu'elles peuvent apporter. Il recommande d'éviter ou au moins de restreindre considérablement la possibilité pour les États membres d'utiliser des copies nationales. Néanmoins, si celles-ci doivent être créées, il faut appliquer le principe de stricte limitation de l'objet du traitement des données à leur utilisation au niveau national. De même, la copie nationale ne peut en aucun cas être interrogée selon des modalités différentes de celles fixées pour la base de données centrale.

17. Concernant la procédure de comité: les décisions ayant une incidence considérable sur la protection des données devraient être arrêtées par la voie d'un règlement ou d'une décision, de préférence au terme d'une procédure de codécision. Si la procédure de comité est effectivement utilisée, il convient de mentionner le rôle consultatif du CEPD aux articles 60 et 61 de la décision et à l'article 35 du règlement.

18. L'interopérabilité des systèmes ne peut être mise en œuvre en violation du principe de limitation de la finalité du traitement des données et toute proposition en la matière devrait être soumise au CEPD.

Fait à Bruxelles, le 19 octobre 2005.

Peter HUSTINX

Contrôleur européen de la sécurité des données