


Département Thématique C  
Droits des Citoyens et Affaires Constitutionnelles



**ECHANGE D'INFORMATIONS ET DE DONNEES  
ENTRE SERVICES REPRESSIFS  
AU SEIN DE L'UNION EUROPEENNE**

**LIBERTES CIVILES, JUSTICE ET AFFAIRES INTERIEURES**





PARLAMENTO EUROPEO EVROPSKÝ PARLAMENT EUROPA-PARLAMENTET  
EUROPÄISCHES PARLAMENT EUROOPA PARLAMENT ΕΥΡΩΠΑΪΚΟ ΚΟΙΝΟΒΟΥΛΙΟ EUROPEAN PARLIAMENT  
PARLEMENT EUROPÉEN PARLAMENTO EUROPEO EIROPAS PARLAMENTS  
EUROPOS PARLAMENTAS EURÓPAI PARLAMENT IL-PARLAMENT EWROPEW EUROPEES PARLEMENT  
PARLAMENT EUROPEJSKI PARLAMENTO EUROPEU EURÓPSKY PARLAMENT  
EVROPSKI PARLAMENT EUROOPAN PARLAMENTTI EUROPAPARLAMENTET

**Direction Générale Politiques Internes de l'Union  
Département Thématique C  
Droits des Citoyens et Affaires Constitutionnelles**

# **ECHANGE D'INFORMATIONS ET DE DONNEES ENTRE SERVICES REPRESSIFS AU SEIN DE L'UNION EUROPEENNE**

## **ETUDE**

### Résumé:

Depuis quinze ans, les échanges transnationaux d'information entre services répressifs au sein de l'Union européenne se sont considérablement développés. Ce processus a été initialement déclenché par l'abolition des frontières nationales au sein de l'espace Schengen. Il a depuis été alimenté par un nombre grandissant de menaces perçues pour la sécurité, par la croyance erronée dans la capacité de la technologie à résoudre les problèmes, et par une politique de surenchère entre certains Etats membres et le niveau communautaire. L'objectif de ce processus est d'établir un régime paneuropéen de sécurité interne.

Le présent rapport examine l'aspect juridique de ce processus et en considère le(s) principe(s) organisateur(s). Il offre un aperçu des bases de données et des systèmes d'échange d'information existants ou prévus au sein de l'UE. Il clarifie certains concepts clé en matière d'échange automatisé de l'information. Il décrit certaines des procédures d'échange d'information entre services répressifs. Il identifie certains effets collatéraux de l'échange transnational d'information. Il formule enfin certaines recommandations pour une meilleure gestion des appareils et des pratiques.

**PE 419.590**

Cette étude a été demandée par la Commission des libertés civiles, de la justice et des affaires intérieures du Parlement européen (**LIBE**).

Le présent document est publié dans les langues suivantes: EN, FR.

Auteurs: **Leon Hempel, Michael Carius et Carla Ilten (Technical University of Berlin)**

*Sous la coordination de la section Justice et Affaires intérieures du Centre for European Policy Studies (CEPS), Bruxelles*

Manuscrit achevé en **avril 2009**

Pour obtenir des copies, veuillez vous adresser à :

M. Alessandro DAVOLI  
Administrateur Département Thématique C  
Tel: 32 2 2832207  
Fax: 32 2 2832365  
E-mail: [alessandro.davoli@europarl.europa.eu](mailto:alessandro.davoli@europarl.europa.eu)

Informations sur les **publications de la DG IPOL**:

<http://www.europarl.europa.eu/activities/committees/studies.do?language=EN>

<http://www.ipolnet.ep.parl.union.eu/ipolnet/cms/pid/438>

Bruxelles, Parlement européen

Les opinions exprimées sont celles de l'auteur et ne reflètent pas nécessairement la position officielle du Parlement européen.

## TABLE DES MATIÈRES

I.	Introduction .....	1
II.	Vers une stratégie UE pour le partage des données ? .....	2
III.	Examen des bases de données et des systèmes d'échange d'informations existants ou prévus .....	5
	Systèmes d'information .....	
	S-TESTA – l'infrastructure de communication .....	11
	Interopérabilité, efficacité et protection des données.....	13
IV.	L'échec de La Haye ? Aperçu de la législation communautaire sur les échanges d'informations .....	15
	Définir l'accessibilité .....	15
	Une première approche : l' « Initiative suédoise » .....	17
	Vers l'accessibilité via Prüm ?.....	19
V.	Remarques de conclusion et recommandations .....	25
	Ralentir l'évolution du régime européen de sécurité .....	25
	Réglementer les pratiques des services répressifs en matière d'échange des données .....	26
	<i>Constructive Technology Assessment</i> .....	27
VI.	Bibliographie.....	28
	Annexe A .....	31

## I. INTRODUCTION

Le Livre blanc *Défense et Sécurité nationale*, rédigé sous l'autorité du président français Nicolas Sarkozy, a été publié en juin 2008. Il offre un exemple frappant d'une vision technocratique utopique : celle d'un système national global de sécurité où la collecte, le traitement, la centralisation et l'échange des données et des informations jouent un rôle essentiel pour anticiper les risques perceptibles dans un brouillard effrayant peuplé d'inquiétantes menaces. Dans une telle utopie, la *connaissance anticipée* représente la première ligne de défense, la garante de la sécurité :

« Le développement de la connaissance et des capacités d'anticipation est notre première ligne de défense. [...] La bataille du XXI<sup>e</sup> siècle se jouera d'abord sur le terrain de la connaissance et de l'information, des hommes comme des sociétés. [...] Les responsables politiques doivent pouvoir disposer de l'ensemble des données qui permettront d'éclairer leurs décisions et d'apprécier les situations en toute souveraineté. [Nous devons avoir la garantie que] les pouvoirs publics font le maximum pour éclairer l'avenir, analyser les risques, tenter de les éviter, et préparer les moyens d'y faire face ».

(*Défense et Sécurité nationale: Le livre blanc 2008*, p. 66)

Pour assurer ce pouvoir d'anticipation et développer les connaissances nécessaires à la sécurité, les autorités répressives européennes sont de plus en plus contraintes par les décideurs politiques d'utiliser les technologies de l'information pour collecter, lier et échanger les données à cette fin. Deux exigences principales sont considérées comme indispensables à cet égard : les données doivent être disponibles et par conséquent les systèmes doivent devenir interopérables. Dès lors, l'interopérabilité n'est plus un simple problème technologique comme le voudraient les concepteurs de l'architecture de sécurité du 21<sup>e</sup> siècle. De Hert et Gutwirth le soulignent :

« En réalité, les développements technologiques ne sont ni inévitables, ni neutres et, *mutatis mutandis*, c'est également le cas de l'interopérabilité technique. Les technologies sont inextricablement liées à une organisation, à des valeurs culturelles, des institutions, une réglementation légale, à l'imaginaire social, à des débats et des controverses, et l'inverse est également vrai, bien entendu. Cela signifie que les technologies ne peuvent être considérées comme des *faits accomplis* ou des questions, par nature, extrapolitiques. » (De Hert et Gutwirth 2006, p. 3)

Les systèmes sont des hybrides, combinant facteurs humains et technologiques, et caractérisés par des interactions aux multiples facettes. A petite échelle, elles sont à l'œuvre dans des systèmes comme la biométrie, et à grande échelle dans les systèmes de traitement électronique des données. Au lieu de l'habituelle délégation des tâches des humains aux machines, les interactions s'effectuent entre partenaires humains et technologiques au sein d'un même contexte de coordination multilatérale. De telles interactions deviennent encore plus complexes à un niveau transnational comme celui de l'UE : les différences culturelles, sociales, organisationnelles et juridiques entre les services répressifs qui s'échangent les données génèrent une complexité maximale. Le problème essentiel est double : d'une part, il réside dans le fait que la circulation des marchandises, des personnes, des services et des capitaux au sein de l'UE est dans une large mesure libre de toute restriction. Cette liberté de circulation transnationale pose une série de problèmes. Elle facilite les agissements des criminels mais complique la tâche des services répressifs. D'autre part, on constate une opacité croissante en raison du patchwork toujours plus étendu constitué par l'émergence d'organismes, de systèmes, de procédures, de technologies et de réglementations concernant la sécurité ; en fait, pris dans sa totalité, le régime de la sécurité est devenu une gigantesque boîte noire.

Ce problème est à peine ressenti au niveau politique : comme les ingénieurs, les responsables politiques estiment qu'il s'agit d'une question purement technologique, où c'est la législation

qui joue le rôle de la technologie. Ils ignorent les implications sociales d'une coopération transnationale étendue via des systèmes IT à grande échelle. Cette absence de prise de conscience est le reflet des présupposés idéologiques qui sous-tendent le régime européen de la sécurité qui est en train de se construire. Le Livre blanc de Sarkozy a fait l'objet d'un vif débat parmi les responsables de la sécurité des Etats membres de l'UE, et la question qui s'est posée est de savoir qui allait surenchérir et traduire l'utopie sarkozyste au niveau européen ? La politique européenne de sécurité est en effet à la recherche de la méthode adéquate pour faire *converger* les technologies, les systèmes, les pratiques, les organisations et les dispositions de loi, ce qui est bien entendu beaucoup plus facile au niveau national. La stratégie, toutefois, restera la même parce que la culture politique qui l'inspire est la même. Il en découlera inévitablement un recours accru à la technologie, dans une confusion entre les fins et les moyens du processus. C'est précisément ce à quoi on assiste dans les déclarations de Franco Frattini à propos de l'après-Programme de La Haye :

« Le futur défi majeur, c'est la *poursuite du développement de nouvelles technologies et leur lien à un financement au niveau de l'UE* en englobant dans le domaine de la sécurité la recherche et les fonds structurels. Les bases de données et les nouvelles technologies joueront un rôle central dans le futur développement des politiques JLS et JAI en matière de gestion des frontières, de migrations, de lutte contre le crime organisé et le terrorisme international » (cit. by Bunyan 2008, p. 7)

Lorsqu'on considère la situation dans son ensemble, nous observons une nette tendance à l'intégration des systèmes technologiques dans le but de permettre ce qu'on appelle l'interopérabilité. En invoquant des menaces nouvelles, on promeut la collecte des données, leur accessibilité, leur échange ainsi que l'extension au niveau de l'UE de systèmes entiers de sécurité sur une base technologique supposée neutre. Ni les contextes différents de ces systèmes d'information ni les questions relatives à la légitimité de ces accords contraignants ne sont abordés dans le débat. Les conceptions et les décisions – comme le traité de Prüm – ont été jusqu'à présent négociés et adoptés de manière fort peu transparente et sans contrôle démocratique. Les systèmes technologiques revêtent pourtant une dimension politique : tant les objectifs que l'architecture des futurs systèmes de sécurité doivent faire l'objet d'une large évaluation afin de déterminer très précisément si ces systèmes sont efficaces et s'ils ne sortent pas des limites d'opérations légitimes. Bien entendu, une telle approche politique et constructive demande du temps pour l'analyse et la prise de décision. Le présent article présente un aperçu des problèmes à régler en priorité.

## **II. VERS UNE STRATEGIE UE POUR LE PARTAGE DES DONNEES ?**

Aujourd'hui, l'ensemble du territoire de l'UE, à l'exception du Royaume-Uni et de l'Irlande, fait (ou fera bientôt) partie d'un ensemble qui comprend (ou qui comprendra) aussi des pays qui ne sont pas membres de l'UE (Islande, Norvège, Suisse et Liechtenstein) : *l'espace Schengen*. Cet espace rassemble une population de plus de 450 millions de personnes sur un territoire de quelque 4.500.000 km<sup>2</sup>. Au sein de ce vaste territoire, les contrôles systématiques aux frontières ont tous été abolis, ce qui change radicalement les conditions dans lesquelles les services répressifs européens doivent remplir leur tâche. Dans son document stratégique pour 2008, l'AEPC (Association of European Police Colleges) déclare : « la coopération policière internationale doit englober l'ensemble de l'Europe comme étant un seul espace pénal » (AEPC, 2008). Les services répressifs européens sont donc confrontés à une tâche véritablement titanesque. Certaines indications donnent à penser que cette tâche pourrait excéder leurs capacités

Une série de documents offrant une analyse spécifique des formes graves de criminalité et du terrorisme peuvent fournir un premier éclairage à propos de cette problématique. Les réponses au questionnaire sur la Décision-cadre relative à la simplification de l'échange d'informations et de renseignements entre les services répressifs des Etats membres de l'Union européenne (5815/1/05 REV 1), connue sous le nom d'*Initiative suédoise*, illustrent les difficultés

auxquelles est confronté l'échange de données et qui résident dans la diversité des dispositions légales autorisant les services de police à échanger des données personnelles par-delà les frontières nationales. Les réponses montrent clairement qu'il n'existe pas de réglementation commune entre autorités répressives à propos de l'accès aux données et la question qui reste encore posée aujourd'hui n'est pas seulement celle de savoir si et comment cette harmonisation pourra être atteinte, mais aussi celle de savoir si les autorités répressives veulent vraiment que cette harmonisation soit mise en place. En tout cas, lors d'un entretien avec des représentants d'une unité de lutte contre le terrorisme dans le cadre de la préparation du présent article, il nous a été dit qu'une telle harmonisation prendrait des générations.

La Stratégie de l'Union européenne visant à lutter contre le terrorisme (14469/4/05 REV 4) du 30 novembre 2005, qui regroupe les mesures à prendre sous les intitulés PREVENTION, PROTECTION, POURSUITE et REACTION, est largement basée sur un flux suffisant d'informations entre Etats membres et entre Europol et les Etats membres. Dans une Note sur la Mise en oeuvre de la stratégie de l'UE visant à lutter contre le terrorisme (15411/07) du 23 novembre 2007, qui évalue les progrès et les priorités nouvelles à adopter, le coordinateur de l'Union européenne pour la lutte contre le terrorisme évoque les difficultés du partage des informations. Il relève que cette série d'évaluations mutuelles a mis en lumière les déficiences considérables qui subsistent en matière de partage des informations au niveau national. Malgré une tendance générale au sein des Etats membres en faveur d'une approche « multiservices », ces déficiences constituent l'un des principaux obstacles à la coopération au niveau européen. Les problèmes concernent principalement l'absence de plates-formes réunissant les différents services (police, douanes, FIU, etc.) et les liens insuffisants entre les bases de données des services concernés, ajoute le Coordinateur. On peut y voir au passage une intéressante anticipation de ce qui se passera dans l'après-Programme de La Haye. A côté des discordances *juridiques*, des obstacles *techniques* sont évoqués. Jusqu'à présent, la détermination de la politique de sécurité au niveau de l'UE s'est concentrée sur ces deux dimensions, technique et juridique.

Un an plus tard, le Coordinateur a dû encore une fois signaler que l'échange des données restait inférieur aux attentes. Dans sa note du 19 novembre 2008 (15983/08), dans le cadre de la définition d'une stratégie de l'UE sur le partage des données, il indiquait que, selon un rapport d'Europol, « la mise en oeuvre de la décision 2005/671/JAI laisse encore à désirer ». En référence à la décision 2003/48/JAI du Conseil du 19 décembre 2002 (JO 2003 L 16) relative à l'application de mesures spécifiques de coopération policière et judiciaire en matière de lutte contre le terrorisme, qui a été une des principales réponses aux attaques terroristes du 11 septembre, la décision 2005/671/JAI (JO 2005 L 253) avait appelé à élargir les échanges d'information après les attentats à la bombe de Londres : « Le champ d'application des échanges d'informations doit être étendu à tous les stades de la procédure pénale, y compris aux condamnations, et à l'ensemble des personnes physiques et morales, groupes ou entités faisant l'objet d'une enquête, de poursuites ou d'une condamnation pour infraction terroriste » (préambule, para. 4). Une fois encore, le Coordinateur demande d'agir, « au besoin en modifiant la décision 2005/671/JAI/ » qui joue un rôle crucial dans la stratégie qu'il développe pour améliorer le partage des informations. Il identifie les priorités suivantes:

- établissement d'un mécanisme de gestion des systèmes informatiques à grande échelle;
- transmission systématique des informations à Europol et Eurojust conformément à la décision 2005/671/JAI (modifiée ou non) et intégration d'Europol et Eurojust dans des équipes d'enquête conjointes sur le terrorisme constituées par les Etats membres ;
- intensification de la coopération entre Europol et Eurojust et évaluation de celle-ci ;
- invitation à tous les Etats membres de procéder à des analyses des sites islamistes extrémistes pour ajouter des informations au portail *Check the Web*;
- établissement d'organismes centralisés au niveau national, chargés de coordonner les échanges et l'analyse des informations sur le terrorisme ;

- poursuite des discussions de préparation de la négociation d'un accord contraignant sur la protection des données dans les échanges d'informations avec les Etats-Unis.

Ces suggestions portent sur quatre dimensions : *l'harmonisation technologique* (soutien IT aux échanges de données et à la gestion des systèmes sur grande échelle) ; *l'harmonisation juridique* (à savoir, au moins dans ce cas, faire appliquer la législation en vigueur) ; *le rapprochement culturel* du travail policier (mesures de construction de la confiance pour que les services soient davantage disposés à partager l'information) ; enfin, la *centralisation organisationnelle* de la lutte contre le terrorisme pour faciliter les échanges d'informations au niveau transnational (nombre réduit d'acteurs, partenaires de communication clairement identifiés). Si en 2007, le Coordinateur avait principalement pointé les problèmes technologiques comme obstacles empêchant que l'échange transnational d'informations se déroule sans encombre, après le rapport d'Europol sur les difficultés rencontrées par l'application des dispositions de la décision 2005/671/JAI, il entend « adopter une approche élargie et cohérente ». Bien entendu, le principal souci du Coordinateur reste d'établir un organisme chargé de la coordination centralisée de la lutte contre le terrorisme au niveau de l'UE, mais il s'inspire désormais d'une approche multidimensionnelle. Il reste à savoir toutefois si cette approche sera suffisante pour surmonter les difficultés. Il semble bien que le choix d'une approche multifonctionnelle pour améliorer les échanges transnationaux d'information reflète le statut précaire d'Europol et d'Eurojust dans la lutte contre le terrorisme et donc la faiblesse de sa propre position. Mais cela n'explique pas tout. La réticence de certains Etats membres à transmettre leurs données à Europol et Eurojust constitue dans le même temps une réponse au moins symbolique à la stratégie générale de l'UE visant à intégrer les politiques nationales de sécurité au niveau européen, en annexant ainsi des pans essentiels de la souveraineté nationale. Selon la note du Coordinateur, le rapport d'Europol soulignait trois types d'obstacles à la transmission systématique d'informations sur les enquêtes :

- le refus des autorités judiciaires de certains Etats membres de transmettre des informations sur des enquêtes en cours;
- le fait que certains services compétents à la fois en matière répressive et en matière de sécurité se heurtent à des difficultés juridiques pour déterminer quelles informations peuvent être échangées avec Europol.
- l'exigence visée à l'article 2, paragraphe 3, de la décision, selon laquelle l'information doit intéresser ou être susceptible d'intéresser deux États membres ou plus.

L'article 2(3) de la décision 2005/671/JAI stipule que « chaque État membre prend les mesures nécessaires pour veiller à ce qu'au moins les informations [...] en ce qui concerne les enquêtes pénales et les informations [...] concernant les poursuites et les condamnations pénales pour infractions terroristes, qui intéressent ou sont susceptibles d'intéresser deux États membres ou plus et sont recueillies par l'autorité compétente, soient transmises à [...] Europol [...] et [...] Eurojust ».

Les trois obstacles mentionnés par le Coordinateur illustrent tous le phénomène de ce qu'on a pu appeler la « propriété de l'information » (Bigo et al. 2007) ; autrement dit : ils trouvent leur commune origine dans le fait que le savoir est un pouvoir et plus précisément, dans le contexte en question, la capacité à faire régner la loi et l'ordre au niveau national. Ce pouvoir, cette capacité sont des caractéristiques de la souveraineté. Les obligations exprimées dans la décision 2005/671/JAI entraînent dès lors des conflits classiques de loyauté : le fonctionnaire ou le policier obligé de transmettre des informations à Europol, par exemple, peut avoir l'impression d'aller à l'encontre de ce qui constitue l'essentiel de sa mission, à savoir la protection de la sécurité de l'Etat (national) ; le troisième obstacle à la transmission de l'information à un organisme transnational est bien la loyauté au niveau d'un ou de plusieurs Etats nations. En résumé, ce qui devait faire office de mesure de sécurité — le partage des

informations — peut être perçu comme une tentative de spoliation et dans une certaine mesure comme son exact opposé : une menace et une forme de contrôle de l'exercice d'une tâche nationale. Avant même de mettre en place des systèmes technologiquement et juridiquement convergents, l'idée même du partage des données et des informations est une question éminemment politique.

### **III. EXAMEN DES BASES DE DONNEES ET DES SYSTEMES D'ECHANGE D'INFORMATIONS EXISTANTS OU PREVUS**

La conception de la technologie comme un outil puissant mais neutre pour la résolution des problèmes va de pair avec l'absence ou le peu d'intérêt pour ses conséquences sociales et politiques. La seule manière d'éviter cette erreur est de replacer la technologie dans le contexte social et politique de son développement. Cette section décrit brièvement les principaux systèmes d'information et formule quelques remarques à propos de la situation et des problèmes actuels, avant d'aborder la question de l'interopérabilité et de l'efficacité dans certaines remarques finales de portée générale.

#### **Systèmes d'information**

Depuis le traité instituant la Communauté économique européenne (1957), le principal objectif de la politique européenne d'intégration économique a été d'établir un marché commun. En 1985, la convention intergouvernementale de Schengen a représenté un pas décisif vers l'établissement du marché commun. Les parties contractantes se disaient « animé(e)s de la volonté de parvenir à la suppression des contrôles aux frontières communes dans la circulation des ressortissants des Etats membres des Communautés européennes et d'y faciliter la circulation des marchandises et des services » (quatrième considérant de la Convention de Schengen, in Acquis Schengen, JO 2000 L 239). Elles s'affirmaient certes très conscientes des « conséquences négatives que peut entraîner l'allègement des contrôles aux frontières communes en matière d'immigration et de sécurité ». (Art. 7). Elles soulignaient la « nécessité d'assurer la protection de l'ensemble des territoires des cinq Etats contre l'immigration illégale et les activités qui pourraient porter atteinte à la sécurité » (Art. 7). Elles déclaraient que « Les Parties renforcent la coopération entre leurs autorités douanières et de police [...] A cette fin, [...], les Parties s'efforcent d'améliorer l'échange d'informations et de le renforcer en ce qui concerne les renseignements susceptibles de présenter un intérêt pour les autres Parties dans la lutte contre la criminalité » (Art. 9). La Convention d'application de l'Accord de Schengen (Convention Schengen) a été signée en 1990 et elle est entrée en vigueur en 1995, en abolissant les contrôles aux frontières intérieures des Etats signataires, et en créant une frontière extérieure unique. Des mesures compensatoires, comme un régime commun des visas mais surtout le Système d'information Schengen (SIS), furent mises en place. En 1999, l'Acquis de Schengen, y compris le SIS, a été intégré dans le cadre de l'UE par le traité d'Amsterdam. Le SIS est le père de tous les systèmes IT paneuropéens actuels et futurs, chargés d'assurer les échanges transnationaux d'information entre les services répressifs.

#### **Le Système d'information Schengen (SIS)**

La base de données du SIS est opérationnelle depuis 1995. Sa *base juridique* est la convention d'application de l'accord de Schengen du 14 juin 1985 (JO 2000 L 239), telle que modifiée par le règlement (CE) n° 871/2004 du Conseil du 29 avril 2004 concernant l'attribution de certaines fonctions nouvelles au Système d'information Schengen, y compris dans le cadre de la lutte contre le terrorisme (JO 2004 L 162) et par la décision du Conseil 2005/211/JAI (JO 2005 L 68).

*Finalité* : le SIS doit « permettre aux autorités [...] grâce à une procédure d'interrogation automatisée, de disposer de signalements de personnes et d'objets aux fins de contrôles de frontière et vérifications et autres contrôles de police et de douanes » (Art. 92(1)).

Les *catégories d'objets* suivantes sont intégrées dans le SIS : véhicules à moteur, bateaux, avions, équipements industriels, conteneurs, armes à feu, passeports, cartes d'identité, permis de conduire, permis de séjour, documents de voyage, etc., volés ou égarés (Art. 100(3)).

Les *catégories de personnes* suivantes sont intégrées dans le SIS :

- personnes recherchées pour l'arrestation aux fins d'extradition (Art. 95);
- étrangers [citoyens de pays tiers] qui sont signalés aux fins de non-admission [dans l'espace Schengen] (Art. 96);
- personnes disparues ou placées provisoirement en sécurité (Art. 97);
- témoins, etc. (Art. 98);
- personnes (ou véhicules) devant faire l'objet d'une « surveillance discrète ou de contrôle spécifique » (Art. 99).

Enfin, les *informations suivantes au sujet de ces personnes* sont intégrées dans le SIS : les nom et prénom ; les alias ; les signes physiques particuliers, objectifs et inaltérables ; la date et le lieu de naissance ; le sexe ; la nationalité ; l'indication que les personnes concernées sont armées ; l'indication que les personnes concernées sont violentes; le motif du signalement ; la conduite à tenir (Art. 94(3)).

*Architecture* : Le SIS (version actuelle : SIS I+) est une interconnexion de bases de données nationales (N-SIS), via un réseau de communication sécurisé, avec un serveur central situé à Strasbourg (C-SIS) qui envoie des données aux bases de données nationales et en reçoit de ces bases (structure radiale). L'information est fournie par chaque Etat contractant via son N-SIS et distribuée ensuite via le C-SIS auprès de tous les autres N-SIS. Le contenu de tous les N-SIS est donc identique et identique à celui du C-SIS (stockage parallèle). La recherche d'information dans chaque Etat contractant ne s'effectue que dans le N-SIS de cet Etat. Les bases de données ne contiennent que les informations indispensables (dite « données de signalement ») permettant l'identification d'une personne ou d'un objet et la prise des mesures nécessaires. Le SIS est complété par les bureaux SIRENE (*Supplementary Information Request at the National Entry*) nationaux qui fournissent sur demande des informations supplémentaires ne figurant pas dans la base de données. Les bureaux SIRENE sont reliés entre eux par un système de télécommunications protégé (SISNET).

*Utilisateurs autorisés* : « En pratique, un large éventail d'autorités nationales ont accès au SIS [...] : la police, les services de sécurité de l'Etat, le ministère public et les juges, les autorités douanières, les départements ministériels, les services de l'immigration et ceux chargés de l'immatriculation des véhicules » (Geyer 2008, p. 14). Il faut y ajouter Europol et Eurojust (depuis les amendements mentionnés).

En juin 2005, le SIS comportait plus de 15 millions de fichiers sur des personnes et des objets. Plus d'un million de ces fichiers concernaient des personnes (Brouwer 2005). Ces chiffres croissent bien entendu régulièrement. En février 2008, le SIS comportait ainsi plus de 17 millions de *records* (SEC(2008) 153 ; voir ci-dessous Publications de la Commission des CE). Fort naturellement, la question qui se pose est de savoir si tous ces *signalements* peuvent se transformer en *actions*.

*Problèmes* : Un des principaux problèmes des échanges transnationaux d'information entre services répressifs réside dans le simple fait que les pays échangeant les informations présentent d'importantes différences culturelles et juridiques. Le phénomène est clairement mis en évidence par un rapport de l'Autorité commune de contrôle (ACC) de Schengen du 18 décembre 2007 (Rapport n°07-02 ; non disponible sur le site Internet de l'ACC) examinant l'utilisation des signalements effectués dans le SIS en vertu de l'article 99. Selon cet article, un signalement peut être émis lorsqu'il existe des indices réels faisant présumer que (a) la

personne concernée envisage de commettre ou commet des faits punissables nombreux et extrêmement graves et / ou (b) lorsque l'appréciation globale de l'intéressé, en particulier sur la base des faits punissables commis jusqu'alors, permet de supposer qu'il commettra également à l'avenir des faits punissables extrêmement graves. Sur la base des chiffres au 1<sup>er</sup> octobre 2006, le SIS contenait les quantités suivantes de signalements sur la base de l'article 99 :

Pays	Surveillance	Contrôles spécifiques	Total # signalements
France	9.615	6.493	16.108
Italie	11.604	100	11.704
Espagne	15	2.142	2.157
Pays-Bas	3	1.135	1.138
Allemagne	790	0	790
Autriche	714	0	714
Suède	394	0	394
Danemark	196	0	196
Belgique	96	80	176
Finlande	58	0	58
Norvège	58	0	58
Luxembourg	33	0	33
Portugal	14	0	14
Grèce	1	0	1
Islande	0	0	0
Total	23.591	9.950	33.541

Source: rapport de l'ACC, p. 5. Le tableau sous cette forme (réarrangée) est tirée de Hayes 2008, p. 3.

Quelle est la raison des variations considérables du nombre de signalements article 99 effectués par les différents Etats Schengen ? Le rapport de l'ACC offre une réponse : « l'utilisation de l'article. 99 est régie par une grande variété de lois et est assurée par un certain nombre de pouvoirs différents dans les divers Etats Schengen » (p. 6). « La Convention de Schengen ne définit pas les termes de « faits punissables extrêmement graves ». Par conséquent, la méthode de sélection des faits criminels entraînant un signalement article 99 varie d'un Etat à l'autre » (p. 8). Et enfin : « Il est clair que les différences dans l'interprétation nationale de ce qu'est un fait punissable extrêmement grave et dans les perceptions nationales de la manière d'enquêter sur ces faits ou d'utiliser des méthodes d'investigation proactives semblent constituer le facteur le plus décisif pour l'utilisation du signalement en vertu de l'article 99 ». (p. 11). Le rapport de l'ACC établit sans le moindre doute que l'espace de liberté, de sécurité et de justice *ne peut pas* être harmonisé en termes de politique répressive en ne se fondant que sur la mise en place de canaux de communication. La diffusion transnationale de l'information est nécessairement synonyme de diffusion de traductions et d'interprétations diverses de ce qui ne sont que des dispositions générales. Les différences dans les traductions et les interprétations découlent de la diversité des pratiques effectives et du degré très variable de perception de la menace d'un pays à l'autre. On peut douter qu'une harmonisation juridique puisse modifier cette situation. Les conclusions du rapport de l'ACC doivent être considérées comme une mise en garde contre, par exemple, l'insertion du délit de « trouble violent à l'ordre public » dans le SIS.

## Le Système d'information Schengen II

*Finalité* : comme la base de données du SIS avait au départ été établie pour ne connecter que huit pays entre eux, il est rapidement apparu qu'il ne serait pas suffisant. Dès 1996, le comité exécutif Schengen envisageait le passage à un SIS de deuxième génération. La planification de ce SIS II a suscité une attention croissante, en particulier suite à la prise de conscience grandissante de nouvelles menaces, dont le crime organisé et, depuis le 11 septembre, le terrorisme. Mais le SIS II n'est pas encore opérationnel et il semble même connaître de sérieuses difficultés. Le communiqué de presse de la 2927<sup>e</sup> réunion du Conseil JAI à Bruxelles (26–27 février 2009) indique que « le Conseil regrette que, compte tenu du délai nécessaire pour résoudre les questions en suspens, la date prévue pour la migration du SIS 1+ vers le SIS II, à savoir septembre 2009, ne soit plus réaliste. ». Il convient donc de procéder « à l'élaboration d'un scénario technique de rechange qui puisse être utilisé pour développer le SIS II sur la base de l'évolution du SIS 1+ dans le cadre d'un plan de secours ». (p. 21).

L'*architecture du système* du SIS II sera fondamentalement la même que celle de l'ancien système, toujours opérationnel aujourd'hui. Dans la perspective du SIS II, le nombre des *utilisateurs autorisés* a déjà été élargi (Europol, Eurojust, le ministère public et les juges, les services chargés de l'immatriculation des véhicules, etc.; une liste de toutes les autorités nationales ayant accès au SIS figure dans le doc. du Conseil 6073/2/07 REV 2, 25.6.2007). Le contenu sera élargi (notamment aux empreintes digitales et à des photographies). Enfin, sa *plate-forme technique* sera partagée avec le VIS, EURODAC, etc. (voir ci-dessous la section consacrée à S-Testa).

La *base juridique* du SIS II est la suivante :

- le règlement (CE) n° 1987/2006 du Parlement européen et du Conseil (JO 2006 L 381) régira les aspects du SIS II sur l'immigration (signalements relatifs à des ressortissants de pays tiers) — ci-après, *le Règlement*.
- la décision 2007/533/JAI du Conseil (JO 2007 L 205) régira l'utilisation de SIS II pour la coopération policière et judiciaire en matière répressive (signalements relatifs à des personnes et à des objets) — ci-après, *la Décision*.
- le règlement (CE) n° 1986/2006 du Parlement européen et du Conseil (JO 2006 L 381) ouvre l'accès de SIS II aux services chargés de l'immatriculation des véhicules.

*Problèmes* : le 19 octobre 2005, le Contrôleur européen de la protection des données (CEPD) a publié un avis sur les trois propositions qui ont ensuite donné lieu aux règlements que l'on vient de citer (JO 2006 C 91). Comme les règlements sont pour l'essentiel identiques aux propositions, il est possible d'analyser la base juridique du SIS II à la lumière de l'avis du CEPD sur ces propositions. Le CEPD observe que « 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 » (C 91/43), à savoir de permettre aux « autorités [...] de disposer de signalements de personnes et d'objets, à l'occasion de contrôles de frontière et de vérifications et autres contrôles de police et de douanes exercés ».

La disposition correspondante, tant du règlement que de la décision, se lit comme suit : « L'objet du SIS II [...] est d'assurer un niveau élevé de sécurité dans l'espace de liberté, de sécurité et de justice de l'Union européenne, y compris la préservation de la sécurité publique et de l'ordre public et la sauvegarde de la sécurité sur les territoires des États membres » (Art. 1(2)). Par comparaison avec les propositions, la formulation s'est même élargie. Cette rhétorique pompeuse et creuse peut être interprétée comme un signe alarmant qu'une idéologie sécuritaire se développe. Une telle lecture est certainement correcte mais d'autre part, cet article 1(2) doit simplement être pris comme signifiant ce qu'il veut dire, à savoir que le *SIS-II entend être un outil universel*. Cette affirmation exprime la raison d'être de la législation en question. Si le SIS-II doit être une *machine d'information géante produisant de la sécurité sous tous les aspects possibles*, il ne peut exister de limitation de principe quant

aux catégories de données susceptibles d'y être enregistrées, ou des catégories d'autorités pouvant y accéder, ou quant aux fonctions de recherche qu'on peut y effectuer. La fin justifie les moyens et les mesures à adopter comme les acteurs à impliquer. Cette vision prosaïque est celle qui est évoquée dans l'avis du CEPD. Ce dernier – il ne le fait d'ailleurs pas que dans l'avis en question – plaide à raison pour une limitation des finalités du système.

Bien loin de limiter son objet, le SIS II est conçu comme un outil général d'investigation. En faisant référence notamment aux autorités chargées de l'asile, à Europol et à Eurojust, le CEPD commente : « *L'accès leur est accordé pour leur permettre d'obtenir des informations servant leurs propres objectifs* » (C 91/45). L'article 37(1) du Règlement et l'article 52(1) de la Décision illustrent eux aussi parfaitement le caractère investigateur de SIS II ; « Un Etat membre peut mettre en relation des signalements qu'il introduit dans le SIS II. Cette mise en relation a pour effet d'établir un lien entre deux ou plusieurs signalements », c'est-à-dire, d'abord et avant tout, entre deux personnes ou davantage. Le CEPD commente : « puisque l'établissement de liens relève de la législation nationale, il pourra advenir que des liens illégaux dans un Etat membre soient établis dans un autre, ce qui alimenterait le système en données «illégalles» » (C 91/46). Comme on l'a déjà établi dans le cas des signalements établis en vertu de l'article 99, le problème ne se pose pas seulement pour *la liaison* des signalements. Il convient de répéter que les échanges transnationaux d'information sur large échelle conduisent inévitablement à une *fusion de fait* incontrôlable entre des législations et des pratiques répressives nationales fondamentalement différentes. C'est l'une des principales causes de l'opacité de la situation dans les questions de sécurité (intérieure) au niveau de l'UE. Un autre élément important dans ce contexte concerne le fait que l'architecture du système du SIS II est la même que celle du SIS I : une interconnexion de bases de données nationales qui stockent en parallèle (ou qui en tout cas pourraient le faire) l'ensemble de la série des données. Le CEPD « recommande de supprimer la possibilité donnée aux États membres d'utiliser des copies nationales », parce que « la multiplication des copies augmente le risque d'abus » (C 91/52).

## **EURODAC**

*Finalité* : EURODAC est une base de données qui enregistre et compare les empreintes digitales via un système automatisé d'identification des empreintes. Son but est d'établir l'identité des demandeurs d'asile et des personnes appréhendées à l'occasion du franchissement irrégulier d'une frontière extérieure de la Communauté. Chaque Etat membre est tenu de transmettre rapidement à l'unité centrale les données suivantes relatives à tout étranger non expulsé : Etat membre d'origine, lieu et date de la demande d'asile; données dactyloscopiques ; sexe ; numéro de référence attribué par l'Etat membre d'origine ; date à laquelle les empreintes ont été relevées ; date à laquelle les données ont été transmises à l'unité centrale. Les demandeurs d'asile sont attribués à l'Etat membre de l'UE en fonction de leur première apparition dans le registre. EURODAC traite les empreintes digitales des catégories de personnes suivantes :

- (a) les demandeurs d'asile ;
- (b) les étrangers appréhendés à l'occasion du franchissement irrégulier d'une frontière extérieure ;
- (c) les étrangers se trouvant illégalement sur le territoire d'un Etat membre.

EURODAC est opérationnel depuis 2003. C'est le premier système automatisé d'identification par empreintes digitales (AFIS) au sein de l'UE. Sa *base juridique* est fournie par le règlement (CE) n° 2725/2000 du Conseil du 11 décembre 2000 concernant la création du système «Eurodac» pour la comparaison des empreintes digitales aux fins de l'application efficace de la convention de Dublin (JO 2000 L 316).

*Architecture*: EURODAC consiste en une unité centrale qui comprend une base de données où sont stockées les empreintes digitales. Les demandes sont effectuées selon une procédure

binaire « *hit/no-hit* » si bien que les données restent stockées au niveau central et qu'aucun accès direct n'est possible. En cas de réponse positive, les Etats membres concernés peuvent agir conformément au règlement de Dublin (règlement (CE) du Conseil n° 343/2003) qui détermine l'Etat membre responsable de l'examen d'une demande d'asile. (JO 2003 L 50).

*Problèmes* : Les principales conclusions du rapport annuel au Conseil et au Parlement européen sur les activités de l'unité centrale d'EURODAC en 2007 (COM(2009) 13 final (26 janvier 2009)) sont intéressantes. Des problèmes techniques mais aussi d'acceptation ou de confiance semblent se poser :

- 300.018 transmissions réussies (une transmission qui a été correctement traitée par l'unité centrale) au total (contre 270.611 en 2006)
- 197.284 transmissions portant sur des demandeurs d'asile (contre 165.958 en 2006)
- 38.173 personnes appréhendées alors qu'elles franchissaient irrégulièrement une frontière extérieure (contre 41.312 en 2006)
- 64.561 personnes séjournant illégalement sur le territoire d'un Etat membre (contre 63.341 en 2006)
- *obsolescence de la plate-forme technique* (l'actualisation du système EURODAC doit être finalisée en 2009)
- qualité des transactions : le taux moyen de *transmissions rejetées* pour l'ensemble des Etats membres s'élève à 6,13 % ; 14 Etats membres ont un taux de rejet supérieur à la moyenne (les causes de ce taux de rejet sont principalement la qualité médiocre des images d'empreintes présentées, les erreurs humaines ou la mauvaise configuration de l'équipement des Etats membres expéditeurs)
- certains Etats membres accusent toujours d'*importants retards* pour l'envoi des empreintes, allant jusqu'à près de 12 jours (Espagne, Bulgarie, Grèce et Danemark)
- le problème de la réticence des Etats membres à effectuer systématiquement les transmissions pour la « catégorie 2 » (franchissement de la frontière) reste non résolu. *8 Etats membres n'ont pas effectué de transmission pour la catégorie 2* (Chypre, République tchèque, Danemark, Estonie, Islande, Lettonie, Luxembourg et Portugal)

### **Le système d'information sur les visas (VIS), en phase de développement**

*Finalité* : Chaque année, 160 millions de citoyens de l'UE, 60 millions de ressortissants de pays tiers (TCN) qui n'ont pas besoin de visa et 80 millions de personnes qui doivent avoir un visa franchissent la frontière extérieure de l'UE dans une direction ou l'autre. Une telle situation ne va bien sûr pas sans poser des problèmes. On a estimé qu'il y avait « jusqu'à huit millions d'immigrants illégaux au sein de l'UE en 2006 »<sup>(1)</sup>, dont beaucoup sont en dépasement de visa. Il a dès lors été prévu d'instituer une nouvelle gestion de la frontière, en particulier un nouveau système entrée-sortie pour tous les TCN (COM(2008) 69 final: Préparer les prochaines évolutions de la gestion des frontières dans l'Union européenne). Le Parlement européen ne croit pas que ce système résoudra le problème, contrairement à Franco Frattini (allocation/08/142 du 12 mars 2008). Le futur système dit VIS « sera pleinement opérationnel au plus tôt en 2012 » (COM(2008) 69 final). Il sera l'un des outils du nouveau régime de gestion des frontières. Selon un rapport rédigé par Jeanine Hennis-Plasschaert, le fait que ni le VIS ni le SIS II ne soient encore opérationnels constituera un obstacle au bon fonctionnement du système entrée-sortie planifié<sup>(2)</sup>.

*Architecture et fonctions prévues* : Il semble que l'architecture du futur système VIS sera articulée autour d'une base de données centrale (C-VIS) permettant un accès direct par les systèmes nationaux d'information sur les visas (N-VIS). Le VIS fournira aux systèmes nationaux d'information sur les visas les données permettant de vérifier, à l'entrée,

<sup>1</sup> "The European Parliament discusses new measures for border management" (9 mars 2009). Source: <http://soderkoping.org.ua>

<sup>2</sup> Ibid.

l'authenticité du visa et l'identité de son titulaire. Tous les TCN soumis à l'obligation de visa pourraient fournir leurs données biométriques (photographie, empreintes digitales) au VIS lorsqu'ils demandent un visa auprès d'un consulat d'un Etat membre et les points de passage des frontières pourraient être équipés pour échanger des données vers le N-VIS. Pour les vérifications à l'intérieur de l'espace Schengen, les services répressifs auront accès au VIS, ce qui leur permettra d'identifier les personnes dépourvues de documents si elles avaient précédemment obtenu un visa.

*Problèmes* : (1) Le CEPD, dans son avis sur le VIS (JO 2006 C 97), est préoccupé par «la tendance générale qui est d'accorder aux services répressifs l'accès à plusieurs systèmes d'information et d'identification à grande échelle ». Il y voit une violation grave du principe de limitation des finalités. (2) Il est difficile de savoir dans quelle mesure la transmission des données des détenteurs de visa entre les consulats des Etats membres et ces Etats se fera en toute sécurité. Les textes sont muets sur ce point (notamment la décision du Conseil 2004/512/CE (JO 2004 L 213) et la Proposition modifiant le règlement (CE) n° 562/2006 (COM(2008) 101 final)).

### **Le Système européen d'information sur les casiers judiciaires (ECRIS), en phase de développement**

*Finalité et architecture prévues*: ECRIS est un système prévu pour l'échange des casiers judiciaires suivant un format normalisé. Aucune fonctionnalité nouvelle n'est envisagée jusqu'à présent. Les données transférées via ECRIS seront stockées dans les bases de données respectives de chaque Etat membre (Projet de décision du Conseil 14571/08 du 20 janvier 2009, Art. 3(2)). Aucune base de données centralisée ne sera constituée : ECRIS adopte une architecture *peer to peer*. « Les autorités centrales des Etats membres. [...] ne disposent pas d'un accès direct en ligne aux bases de données relatives aux casiers judiciaires des autres Etats membres » (Art. 3(3)). Les informations transmises entre les Etats membres seront « extraites des casiers judiciaires » (Art. 1). Le motif de la création d'ECRIS est le suivant : « Les échanges d'informations relatives aux condamnations pénales se font actuellement sur la base de la Convention européenne d'entraide judiciaire en matière pénale de 1959 [...] Ce système présente des lacunes importantes, [...] Il apparaît que les juridictions nationales prononcent fréquemment des peines sur la seule base du relevé des condamnations produit par leur registre national, en totale méconnaissance des condamnations éventuellement prononcées dans d'autres Etats membres » (Proposition de décision du Conseil relative à la création du système européen d'information sur les casiers judiciaires (ECRIS), COM(2008) 332 final).

*Problèmes* : Si l'on considère l'architecture d'ECRIS, il apparaît de toute évidence que la seule approche possible est celle d'un système décentralisé. A travers l'Europe et au sein des Etats membres, les casiers judiciaires présentent une très grande diversité. Dès lors, avant d'établir un système commun, il semble raisonnable de convenir d'une nomenclature de délits. Faute de quoi, les systèmes formalisés conduiront à des taux d'erreur élevés et à des erreurs d'interprétation. Pour l'essentiel, ECRIS se limite à faciliter la transmission de données, alors que la responsabilité de la protection des données et de leur accès reste assurée par les Etats nationaux — ce qui ne constitue pas vraiment une menace *nouvelle* pour la protection des données, selon l'avis du CEPD sur la proposition de décision du Conseil relative à la création du système européen d'information sur les casiers judiciaires (ECRIS), (JO 2009 C 42). La sécurité de l'information dépend de l'infrastructure de transmission, qui devrait être assurée par S-TESTA.

### **S-TESTA – l'infrastructure de communication**

S-TESTA (Services télématiques transeuropéens sécurisés entre administrations) est le réseau de la Communauté européenne à base IP, une infrastructure de télécommunication parallèle à Internet par exemple, et qui vise à mettre en connexion les réseaux nationaux des administrations, des institutions et des bases de données. Le développement de S-TESTA fait

partie du programme de fourniture interopérable de services paneuropéens d'administration en ligne aux administrations publiques, aux entreprises et aux citoyens IDABC, qui sera suivi par l'ISA (Interoperability Solutions for European Public Administrations) à partir de 2010. L'objectif qui justifie la mise sur pied d'une infrastructure spécifique (distincte) pour l'échange de données au sein de l'UE est de faciliter un échange sûr et plus rapide des données. Comme le dit l'IDABC : « le besoin d'une sécurité rigoureuse peut parfois sembler en contradiction avec le besoin d'un échange d'information efficace. Mais S-TESTA offre une solution appropriée. »

En réalité, l'architecture de S-TESTA peut être vue comme un compromis entre *le coût*, *l'interopérabilité* à plusieurs niveaux et les *risques en matière de sécurité*. En tant que réseau de réseaux, S-TESTA connecte seulement des Domaines locaux décentralisés via sa structure centralisée. Cette architecture, selon le CEPD, offre de meilleures possibilités en matière de gestion des risques et de protection des données qu'une architecture *peer to peer*, où tous les réseaux établissent des liens les uns avec les autres. (Avis sur ECRIS, JO 2009 C 42). Les données, par exemple les casiers judiciaires d'ECRIS, restent plus ou moins en sécurité au sein des réseaux nationaux (au lieu de figurer dans une base de données centrale) et ne peuvent être échangés qu'à des fins spécifiques via l'infrastructure de S-TESTA.

D'une part, cette séparation des bases de données offre une protection physique des données, d'autre part, des problèmes d'interopérabilité doivent encore être réglés pour que les échanges de données aient un intérêt. Les problèmes concernent tous les niveaux de l'interopérabilité : formats des données, contenus, codes utilisés, etc. On trouve ici une source possible d'erreurs durant les échanges de données ou lors de leur utilisation et de leur interprétation, ce qui revêt une importance encore accrue pour les données sensibles. Ces questions doivent être réglées par les programmes eLink et CIRCA sur les intergiciels et l'interopérabilité de l'application.

L'infrastructure S-TESTA est conçue pour être une infrastructure de télécommunications *one-for-all*, ce qui signifie que les finalités des échanges de données effectués via S-TESTA ne feront que se multiplier. Des données concernant les risques naturels et technologiques, les ingrédients alimentaires, la santé, les statistiques, la circulation, mais aussi les demandeurs d'asile (EURODAC), les visas (VIS), les voyageurs (SIS II) et les personnes condamnées en justice (ECRIS) seront échangées via la même infrastructure hardware. Du point de vue de la gestion, ce mode d'utilisation de l'infrastructure est le plus intéressant en termes de ratio coût-efficacité.

Cela signifie que la *sécurité* des informations échangées via l'infrastructure S-TESTA constitue le talon d'Achille de tous les échanges de données concernés. Les risques pour la protection des données au niveau physique sont réduits aux seuls moments *effectifs* de l'échange physique ou du transport du paquet d'informations. Mais une fois encore, le risque que pose le système centralisé se trouve généralisé à tous les types de données et à toutes les actions d'échange : si le système présente *une seule* faille en matière de sécurité, elle peut affecter toutes les transactions. Il s'agit alors de savoir, au niveau de la gestion de la sécurité de l'information, si la surveillance du système, la détection des problèmes et leur traitement sont à la hauteur des besoins de sécurité pour les données les plus sensibles qui sont concernées. L'IDABC affirme que « l'amélioration permanente de la sécurité sur S-TESTA aura pour conséquence que l'infrastructure de communication sera accréditée d'ici à 2009 pour transmettre des informations classifiées jusqu'au niveau RESTREINT UE selon les règles de sécurité du Conseil (décision du Conseil 2001/264/CE [JO 2001 L 101]) ». Un examen permanent des risques, des évolutions technologiques, des contextes des échanges de données sur une base politique et juridique (par ex. des critères d'accréditation) doit être associé à une gestion du réseau et à un entretien des infrastructures de qualité supérieure – ce qui pourrait être un autre point critique, étant donné que l'infrastructure est réalisée, exploitée et maintenue en état par un consortium de sociétés privées (Orange Business Services et HP), ce qui ajoute encore une division des responsabilités pour l'ensemble du système.

## Interopérabilité, efficacité et protection des données

La communication de la Commission au Conseil et au Parlement européen sur le renforcement de l'efficacité et de l'interopérabilité des bases de données européennes dans le domaine de la justice et des affaires intérieures et sur la création de synergies entre ces bases (COM(2005) 597 final) a été publiée le 24 novembre 2005. La communication plaide pour un système plus puissant de bases de données européennes, en particulier SIS II, VIS et EURODAC, et pour de nouvelles fonctionnalités dans l'utilisation de ces bases de données. La communication est motivée par la nécessité ressentie d'une amélioration de la sécurité intérieure en raison des attentats terroristes, comme l'indique l'évocation du « *contexte* ». Toutefois, les lacunes identifiées et les scénarios proposés ne sont pas exclusivement orientés vers les menaces terroristes — en réalité, les arguments développés font penser à une transformation complète, à une reconfiguration des flux de données, des contenus et des institutions au sein du régime européen de sécurité. Le contexte de menace terroriste élevée que l'on peut difficilement qualifier de problème d'immigration illégale, est utilisé pour refondre l'ensemble des systèmes d'information pour des finalités très variées.

Dans cette perspective, les lacunes dénoncées dans les structures existantes concernent moins l'interopérabilité que l'ajout de données et de fonctionnalités nouvelles, *conjugué* à des questions d'interopérabilité. Les limitations des recherches alphanumériques, l'absence de possibilité d'identification d'immigrants illégaux, l'absence d'accès aux bases de données pour les services de sécurité intérieure, le suivi incomplet des sorties et l'absence d'outils biométriques et en particulier d'un enregistrement des citoyens de l'UE ne sont *pas* des problèmes concernant l'interopérabilité mais l'extension des fonctionnalités des systèmes — une croissance qualitative en termes de tâches et de possibilités. Cette croissance pourrait expliquer l'appel de la Commission en faveur de l'*efficacité*. En réalité, l'emploi de ce terme n'est pas défini dans la communication, alors que les termes d'*interopérabilité* et de *synergie* le sont, quoique de manière très problématique.

L'*interopérabilité* est définie apparemment de manière technique, comme étant « sans rapport avec la question de savoir si l'échange de données est légalement ou politiquement possible ou nécessaire ». Cette affirmation est très problématique comme le montrent à la fois le CEPD (Observations sur la communication, 10 mars 2006) et De Hert et Gutwirth (2006). Tout d'abord, l'interopérabilité est un concept à plusieurs niveaux qui peut s'appliquer aux données, aux connexions, aux structures juridiques et à d'autres catégories — la communication n'est pas claire à ce sujet. Ensuite, même l'interopérabilité *technique* englobe toujours des aspects sociaux, organisationnels, sémantiques, etc. Il est naïf de concevoir des scénarios d'infrastructures sans prévoir leurs effets — on retrouve ici l'*impératif technologique* bien connu des études sur la technologie. Tertio, la communication emploie l'interopérabilité de manière partielle, positive, en suggérant une relation linéaire entre le niveau d'interopérabilité et l'efficacité ou l'efficacité des systèmes. Cette conception doit être complétée par l'expertise du CEPD sur l'emploi de l'absence délibérée d'interopérabilité en vue d'une amélioration technique et de la garantie de la protection des données (cf. les remarques du CEPD sur la possible « limitation de l'accès [aux] clés primaires » à la page 3 de ses Observations). Cette perspective concerne à la fois la fonctionnalité et la protection des données dans la conception des caractéristiques des infrastructures, plutôt que de générer un contraste entre les *possibilités* technologiques, d'une part, et les *réglementations et restrictions* juridiques et politiques, d'autre part. L'interopérabilité ne peut donc *pas* être dissociée des questions politiques et juridiques.

Ceci nous conduit à la *synergie* et à l'*efficacité*, qui sont présentées comme des objectifs qui doivent être atteints grâce à l'interopérabilité. Ces termes sont bien connus depuis la littérature spécialisée en management des années 1990 exaltant la production maigre, les hiérarchies horizontales ou le *streamlining*, comme le fait la communication. S'agissant des

entreprises, ces termes impliquent d'utiliser moins de ressources en les regroupant, ce qui implique aussi une dépendance par rapport à des actifs centralisés. La synergie, d'autre part, ne doit pas être confondue avec l'efficacité, mais elle implique une efficacité accrue et même des compétences nouvelles. Ces termes visent une *réduction des frais généraux d'infrastructure* grâce à la connexion et à l'administration des nombreuses sources nationales. D'où l'idée de centraliser la « gestion journalière » sous les auspices de l'agence FRONTEX. Du point de vue de la protection des données, comme le disent De Hert et Gutwirth (2006), *la séparation physique des données et des systèmes est le moyen le plus sûr de prévenir les utilisations abusives*. Par conséquent, on *ne peut pas équilibrer* efficacité et protection des données. (Pour une discussion générale de la métaphore de l'équilibre entre liberté et sécurité, voir Guild, Carrera et Balzacq (2008). Cette métaphore dont il est fait rituellement usage dans l'actuel discours officiel sur la sécurité, chaque fois que l'on introduit de nouvelles restrictions aux libertés individuelles au nom de la sécurité, *ne fonctionne pas*.)

Les recherches biométriques proposées peuvent être critiquées comme des méthodes fondées sur des probabilités, comme le souligne le CEPD. La compatibilité avec les droits de l'homme et la protection des données pose également des problèmes. La communication fait une distinction entre les voyageurs « innocents », « de bonne foi », au casier vierge et, par ex. les immigrants dépourvus de pièces d'identité : les voyageurs de bonne foi peuvent être séparés des autres pour rendre les contrôles plus « efficaces » - cette proposition contredit totalement le principe de proportionnalité invoqué dans la communication. En outre, cette proposition semble non seulement dépasser mais même totalement contredire la finalité initiale de prévention des attentats terroristes. La communication ne précise pas le moindre élément de connaissance quant à la nature criminelle des « attentats terroristes » par opposition, par exemple, à l'« immigration illégale » qui servirait de point de départ pour concevoir les structures de l'information. Au lieu de quoi, la communication traite d'un large éventail de finalités, de scénarios, de fonctions et de données — toutes comprises dans un seul nouveau système interopérable pouvant offrir toutes les combinaisons possibles entre ces éléments.

Pour résumer, les systèmes d'information doivent être analysés selon une approche différenciée, pour permettre de porter des jugements sur l'interopérabilité, l'efficacité, la protection des données et les risques pour la sécurité. L'architecture des systèmes respectifs – qui englobe l'organisation sociale autant que l'infrastructure technique – crée une grande diversité quant à leurs effets possibles.

- Tout d'abord, le type de données à stocker doit être pris en compte. Dans quelle mesure s'agit-il de données « sensibles » ? Comment sont-elles codées ? Sont-elles « interopérables » à un niveau interprétatif (cela a-t-il un sens ? des erreurs seront-elles commises ?) et à un niveau technique (dans quel format les données entrent-elles ?)
- Comment, où et pendant combien de temps les données sont-elles stockées ? Sont-elles (1) stockées de manière centralisée ? Ou (2) distribuées de manière décentralisée entre tous les Etats membres dans leurs bases de données respectives ? Dans le second cas, les bases de données contiennent-elles des données différentes ? Ou les données sont-elles confrontées entre les Membres ?
- Comment peut-on accéder aux données ? directement ou sur demande ? intégralement ou partiellement ? sur un mode logique ou dans la version intégrale du texte (hit/no-hit) ? A qui revient la décision ?
- Qui peut accéder aux données ? Quelles sont les raisons formelles à donner ? quelles sont les conditions juridiques à remplir ? Comment sont-elles mises en œuvre ? les activités d'accès sont-elles enregistrées et examinées ? Comment les résultats sont-ils utilisés ?
- Quelle infrastructure hardware est-elle utilisée pour l'accès ? Quels sont les autres éléments connectés via cette infrastructure ? Comment la connexion est-elle

sécurisée ? Qui entretient et gère l'infrastructure ? Qui d'autre connaît bien l'infrastructure ?

- Dans quelle mesure les règles sont-elles strictes pour les utilisateurs, tant pour l'expédition que pour la réception ? Les Etats membres peuvent-ils appliquer des règles plus strictes sur la protection des données et par exemple refuser l'accès ?

Tous ces aspects considérés dans leur ensemble constituent des architectures spécifiques pour les systèmes d'information qui présentent certaines caractéristiques – forces et faiblesses – quand il s'agit d'interopérabilité, d'efficience et de risques pour la sécurité. Par conséquent, ces caractéristiques correspondent à des niveaux différents de protection des données.

#### **IV. L'ECHEC DE LA HAYE ? APERÇU DE LA LEGISLATION COMMUNAUTAIRE SUR LES ECHANGES D'INFORMATIONS**

L'abolition des frontières nationales au sein de l'UE, initialement provoquée par l'Accord de Schengen, a transformé une énorme partie du continent européen en un seul espace pénal. Le concept d'espace de liberté, de sécurité et de justice qualifie le territoire de l'UE dans sa totalité comme indivisible dans les questions de sécurité intérieure, c'est-à-dire, de facto, comme le territoire d'un seul et même Etat. C'est dans ce contexte qu'un gigantesque régime transnational de sécurité est aujourd'hui en voie de constitution. Le système d'échange transnational d'informations se trouve au cœur de ce nouveau régime européen de sécurité. Ce système doit être un système de systèmes où la totalité des informations liées à la sécurité, collectées et traitées au niveau national, circulent librement entre tous les organismes nationaux et transnationaux de sécurité à travers l'UE.

La décision du Conseil 2005/671/JAI (JO 2005 L 253), déjà citée, doit être considérée comme un des nombreux outils juridiques pour la mobilisation de l'information qui sont utilisés pour réaliser l'idéal d'une circulation absolument libre de l'information. La décision oblige chaque Etat membre à transmettre les informations concernant les enquêtes pénales, les poursuites et les condamnations pénales pour infractions terroristes, à Europol et Eurojust (article 2(3)). En outre, l'article 2(6) de la décision oblige chaque Etat membre à « veiller à ce que toute information pertinente contenue dans un document, dossier, élément d'information, objet ou autre moyen de preuve, qui a été saisi ou confisqué au cours d'enquêtes ou de procédures pénales en rapport avec des infractions terroristes, puisse être accessible dès que possible [...] aux autorités d'autres Etats membres intéressés ». Ainsi, toutes les informations doivent être regroupées de manière centralisée et en même temps, autant que possible, distribuées auprès des Etats membres. Le principe exprimé dans cette double obligation (transmettre spontanément et rendre accessible autant d'informations que possible) est connu sous le nom de *principe de disponibilité* et il a fait l'objet de nombreuses discussions. C'est la réponse la plus radicale que l'UE pouvait fournir à la prise de conscience grandissante de menaces omniprésentes.

#### **Définir la disponibilité**

Au cours de ces dix dernières années, le processus législatif dans les questions relatives à l'échange transnational d'informations a été très dynamique. Il montre une tendance manifeste à connaître encore une intensification accrue qui se reflète dans l'extension permanente de la liste des menaces possibles qui nécessitent un échange d'informations et l'extension consécutive des catégories de données considérées comme pertinentes en termes de sécurité.

L'apparition du terrorisme en Europe a accéléré le processus. Le 25 mars 2004, deux semaines après les attentats à la bombe de Madrid, le Conseil européen a adopté une Déclaration sur la lutte contre le terrorisme : « L'Union et ses Etats membres s'engagent à faire tout ce qui est en leur pouvoir pour combattre le terrorisme sous toutes ses formes, dans le respect des principes fondamentaux de l'Union, des dispositions de la Charte des Nations

Unies et des obligations énoncées dans la résolution 1373 (2001) du Conseil de sécurité des Nations Unies » (7906/04).

La Déclaration plaidait notamment pour une législation entraînant une « simplification de l'échange d'informations et de renseignements entre les services répressifs des Etats membres ». En réponse à cette demande, toute une série de notes et de communications ont suivi et réitéré la nécessité d'un échange d'informations pour combattre le terrorisme. Une première contribution de la Commission européenne a été publiée le 16 juin 2004, (COM(2004) 429 final). Elle identifiait cinq éléments « qui sont indispensables pour atteindre une *libre circulation de l'information* entre les autorités répressives des Etats membres, et ce d'une manière plus structurée que ce qui a été le cas jusqu'à présent » [c'est nous qui soulignons]. Ces éléments sont :

1. le principe d'un accès équivalent aux données entre autorités responsables du maintien de l'ordre public et du respect de la loi ;
2. la délimitation des conditions d'accès ;
3. la collecte des données ;
4. l'échange et le traitement des données
5. la recherche.

Le 22 septembre 2004, la présidence néerlandaise du Conseil de l'UE a répondu par une note (12680/04). Elle se référait particulièrement au premier élément de la communication de la Commission, le principe d'un accès équivalent aux données, et elle l'a rebaptisé « principe de disponibilité » : « A compter du 1<sup>er</sup> janvier 2008, les échanges d'information dans les domaines politiques relatifs à l'espace de liberté, de sécurité et justice doivent être basés sur le principe de disponibilité ». Cette position est clairement illustrée en ces termes :

« Ce que le principe de disponibilité signifie en pratique, c'est que, à travers toute l'Union, un membre des services répressifs d'un Etat membre qui a besoin d'information pour effectuer sa mission peut l'obtenir auprès d'un autre Etat membre sans le moindre problème, et le service répressif de cet autre Etat membre qui possède l'information en question est obligé de la lui rendre accessible pour la finalité indiquée. Il est essentiel que les citoyens soient protégés contre les utilisations abusives et les informations incorrectes. »

L'expression « principe de disponibilité » a été introduite dans le discours officiel de l'UE avec le Programme de la Haye (5 novembre 2004) qui a adopté le concept et la définition que l'on vient de citer. Le Programme déclare que « le simple fait que ces informations franchissent les frontières ne devrait plus être pris en considération ». Adopté en hâte, le principe de disponibilité est immédiatement devenu un leitmotiv dans les décisions politiques ultérieures en matière de sécurité intérieure. Son élaboration fait l'objet depuis lors de contestation parmi les Etats membres proposant une législation sur l'échange transnational de d'information. En outre, le Programme de la Haye précise explicitement que « les méthodes utilisées pour échanger les informations devraient exploiter pleinement les nouvelles technologies et être adaptées à chaque type d'information, s'il y a lieu, par le biais d'un accès réciproque aux banques de données nationales, de leur interopérabilité ou de l'accès direct (en ligne), y compris pour Europol, aux bases de données centrales dont dispose déjà l'Union européenne, telles que le SIS. » Le principe de disponibilité est dès lors devenu également la force motrice des nouvelles recherches en matière de sécurité concernant les systèmes interopérables figurant dans le septième programme-cadre pour la recherche et le développement technologique, qui vise à favoriser le développement et l'utilisation des technologies de l'information et de la communication pour la période 2007–2013.

Une Note de la présidence luxembourgeoise du 25 mars 2005 (7641/05) décrivait une application en deux temps du principe de disponibilité : d'abord, le principe devait être établi dans ses grandes lignes générales, et ensuite il devait désigner l'utilisation de toutes les

possibilités technologiques nouvelles disponibles. La note identifiait quatre modalités de transposition de l'accès transnational à l'information en vertu du principe en question :

1. accès indirect à l'information sur demande ;
2. accès indirect à l'information d'un autre Etat membre via un index central, sur une base binaire *hit/no-hit* ;
3. accès direct aux bases de données d'un autre Etat membre ;
4. création de bases de données européennes centralisées.

Ce qui est frappant, s'agissant de ces modalités, c'est qu'elles peuvent se lire comme la description d'un processus graduel allant jusqu'à l'intégration totale des données. Dans ce cas, la souveraineté nationale en matière de sécurité intérieure serait totalement abolie. De fait, la transposition des communications et des notes en propositions législatives voire en textes de droit communautaire déjà adoptés montre que ce processus devrait probablement parvenir à son objectif, sauf si des proclamations de souveraineté nationale y font obstacle.

### **Une première approche : l'Initiative suédoise**

La note de la présidence luxembourgeoise faisait déjà référence à l'Initiative du Royaume de Suède en vue de l'adoption d'une décision-cadre relative à la simplification de l'échange d'informations et de renseignements entre les services répressifs des États membres de l'Union européenne, notamment en ce qui concerne les infractions graves, y compris les actes terroristes (OJ 2004 C 281).

Publiée au Journal officiel le 18 novembre 2004, immédiatement après l'adoption du Programme de la Haye, l'Initiative suédoise a semblé perturber le débat sur le principe de disponibilité, du moins dans une certaine mesure. Elle a été explicitement perçue par les experts en sécurité au niveau de l'UE comme un projet d'amélioration des échanges transnationaux d'information ne visant que le court terme. Comme le déclarait le directeur général Jonathan Faull (Direction générale JAI), « notre proposition d'établissement d'un droit d'accès équivalent est vue par certaines délégations au sein du groupe de travail du Conseil (connu sous le nom de groupe multidisciplinaire), comme un projet à plus long terme qui assurera dans le futur un plus large partage des informations entre les services répressifs des Etats membres » (Chambre des Lords 2005, témoignage oral, p. 39).

Toutefois, conformément à la déclaration du Conseil européen, l'Initiative suédoise exprimait clairement des préoccupations à propos de l'absence de structures et de procédures communes pour l'échange d'informations pertinentes entre les Etats membres. Le paragraphe 8 de son préambule indique que « l'absence d'un cadre juridique commun favorisant l'échange efficace et rapide d'informations et de renseignements entre les services répressifs des Etats membres représente une lacune qu'il conviendra de combler [...] ». Face au terrorisme, le principal objet de l'Initiative est d'établir la base d'un cadre juridiquement contraignant pour accroître le caractère effectif du partage des données au sein de l'UE. Suivant la modalité d'accès indirect à l'information sur demande, quatre aspects se trouvent au cœur de l'Initiative suédoise :

1. demandes et réponses directes pour un échange d'informations entre les services répressifs ;
2. limites de temps pour la fourniture des informations ;
3. obligation de répondre à une demande ;
4. conditions identiques pour l'échange intra-national et transnational d'information.

En 2006, l'Initiative a finalement donné lieu à une décision-cadre (2006/960/JAI ; JO 2006 L 386). Néanmoins, la pleine réalisation du principe de divisibilité requerrait une nouvelle action législative, comme on le verra. Entre la proposition initiale de l'Initiative suédoise et la

décision-cadre du Conseil, on constate un certain nombre de changements et d'ajouts qui méritent qu'on s'y arrête. Dans la décision-cadre, la préoccupation clé de la proposition a été rendue invisible : la phrase se référant au terrorisme dans le titre a été supprimée. Le terrorisme est vu à présent comme un délit grave parmi d'autres, et pour ainsi dire *normalisé*, alors que son importance pour justifier, aux côtés de la criminalité organisée, les échanges transnationaux de données n'est pas remise en cause : « Il importe de promouvoir aussi largement que possible l'échange d'informations, notamment pour ce qui est des infractions liées directement ou indirectement à la criminalité organisée et au terrorisme [...] » (préambule, para. 10). Néanmoins, la nouvelle formulation du titre traduit clairement l'intention de souligner la *continuité* de la politique européenne des échanges transnationaux de données depuis la Convention de Schengen.

La seconde modification concerne la définition des autorités compétentes pour demander ou recevoir des informations via le système de demande. Alors que la proposition de départ était à tout le moins peu claire sur ce point, la décision-cadre exclut explicitement les services secrets de la procédure d'échange d'informations et de données (article 2(a)). D'autre part, le pouvoir de déterminer quelles sont les instances considérées comme services répressifs compétents demeure aux mains des Etats membres conformément à leur droit national individuel. Ce point est essentiel. La décision-cadre indique explicitement qu'elle n'entend pas modifier les systèmes juridiques nationaux existants (préambule, para. 7). Comme la décision-cadre accepte les différents systèmes juridiques nationaux tels qu'ils sont, cela remet en question l'exclusion déclarée des services secrets : si dans un Etat membre, la séparation entre les forces de police et les services secrets est floue ou inexistante, la possibilité que ces services soient malgré tout impliqués dans les échanges transnationaux d'informations est tout à fait réelle. Un problème similaire se pose quant à l'application de mesures coercitives pour obtenir des informations et des renseignements (article 1(6)).

Un autre changement entre la proposition et la directive-cadre concerne les canaux de communication utilisés pour les échanges d'information. Alors que la proposition suggérait des canaux différents, comme les bureaux SIRENE (article 7(1)), la directive-cadre ne lie pas la procédure qu'elle régit à un canal spécifique (article 6(1)). Au moins théoriquement, cela signifie que n'importe quel service répressif peut communiquer avec n'importe quel autre service partout dans l'UE. Ce seul fait assure déjà l'application du principe de disponibilité, dans le cadre, il est vrai, de l'accès indirect et sur demande à l'invitation. Cette information est prélevée après avoir octroyée, elle ne peut être purement et simplement prélevée. Le fonctionnaire du service répressif d'un Etat membre qui a besoin d'une information pour exécuter sa tâche, doit justifier sa demande avant que les données soient transmises par le service répressif de l'Etat membre sollicité. La procédure de demande et de réponse est standardisée. A cet égard, l'adjonction la plus importante par rapport à la proposition initiale concerne les deux formulaires annexés à la décision-cadre et qui doivent être utilisés dans la procédure d'échange. Ils limitent la communication à une série de points prédéfinis comme la nature des délits, la finalité de la demande d'information ou de renseignement, les personnes qui font l'objet de l'enquête pénale et quelques autres points. Seuls trois champs libres sont proposés pour préciser les motifs de l'urgence, le type d'information requis et le type d'activité criminelle faisant l'objet de l'enquête. Cet instrument à première vue purement bureaucratique revêt en fait une grande importance parce qu'il régit la procédure d'échange en empêchant un accès direct aux bases de données d'un autre Etat membre. Il présente un double avantage : d'abord, la documentation des actes d'échange d'information permet de retracer les demandes et réponses faites par les services d'enquête. Ensuite, le niveau accru de transparence de l'échange fait que cette même documentation peut fournir un moyen d'évaluer la protection des données.

DÉCISION-CADRE 2006/960/JAI DU CONSEIL du 18 décembre 2006 relative à la simplification de l'échange d'informations et de renseignements entre les services répressifs des Etats membres de l'Union européenne (JO 2006 L 386). La DC règle les échanges transnationaux d'information entre services répressifs compétents sur la base d'un système de demande. On définit comme « service répressif compétent » « un service national de police, de douane ou autre qui est autorisé par le droit national à dépister et à prévenir les infractions ou les activités criminelles [...] Les agences ou les unités spécialisées dans les questions de sécurité nationale ne relèvent pas de la notion de service répressif compétent » (article 2(a)). « Informations et/ou renseignement » est défini comme « tout type d'informations ou de données détenues par des services répressifs » ou « par des autorités publiques ou par des entités privées et qui sont accessibles aux services répressifs sans prendre de mesures coercitives » (article 2(d)). Mais, « lorsque leur droit national le permet et conformément aux dispositions de celui-ci, les Etats membres communiquent les informations ou les renseignements obtenus précédemment par des mesures coercitives. (article 1(6)). La disposition essentielle de la DC indique que « les Etats membres veillent à ce que les conditions régissant la transmission d'informations ou de renseignements aux services répressifs compétents des autres Etats membres ne soient pas plus strictes que celles s'appliquant au niveau national à la transmission ou à la demande d'informations ou de renseignements (article 3(3)). Des délais maximums sont établis pour la transmission de l'information (article 4). Mais l'Etat membre sollicité peut refuser de fournir l'information demandée. Une information peut être retenue notamment lorsque sa transmission « porterait atteinte aux intérêts vitaux de l'Etat membre requis en matière de sécurité nationale » (article 10(a)). En matière de protection des données, l'échange d'informations et de renseignements est soumis aux lois nationales sur la protection des données de l'Etat qui reçoit les données, cependant que les données personnelles doivent être protégées conformément à la Convention 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, et, pour les Etats membres qui l'ont ratifié, à son protocole additionnel du 8 novembre 2001 concernant les autorités de contrôle et les flux transfrontières de données (article 8). Enfin, deux formulaires ont été annexés à la DC (Annexes A et B) pour être utilisés respectivement par l'Etat sollicité et par l'Etat demandeur.

La décision-cadre offre un cadre réglementaire pour les échanges transnationaux d'informations sur la base d'un système assez simple et technologiquement moins sophistiqué. On peut supposer que sa facilité d'utilisation explique le fait qu'il a été rapidement accepté par les acteurs et organismes concernés. Les Etats membres ont mis en place la procédure. Dans les cas urgents, les demandes doivent recevoir une réponse dans les huit heures ; pour les autres demandes, le délai ne peut dépasser 14 jours. Néanmoins, par rapport à un échange transnational d'informations selon le principe de disponibilité, cette décision-cadre ne représente qu'une étape intermédiaire.

### **Vers l'accessibilité via Prüm?**

A cet égard, le traité de Prüm a permis d'aplanir certaines difficultés. Il a été signé le 27 mai 2005 par la Belgique, l'Allemagne, l'Espagne, la France, le Luxembourg, les Pays-Bas et l'Autriche (10900/05). Invoquant la souveraineté nationale et affirmant que les parties signataires étaient « désireuses de jouer un rôle pionnier dans le but d'atteindre [...] un niveau aussi élevé que possible dans leur coopération », le traité a été perçu dans le contexte des efforts menés au niveau de l'UE comme une avancée à tout le moins ambivalente, voire comme un contournement du cadre UE. Le traité a remis en cause l'équilibre entre les actions intergouvernementales et supragouvernementales, « en créant une hiérarchie au sein de l'UE » selon certains spécialistes (Balzacq et al. 2006). Destiné à intensifier la coopération policière transfrontalière, en particulier dans la lutte contre le terrorisme, la criminalité transfrontalière et l'immigration illégale, le système de Prüm implique un *mix* de diverses modalités d'accès mutuel par la création d'un réseau de bases de données spécifiques : premièrement, un accès indirect aux informations sur l'ADN et les empreintes digitales

détenues par une autre partie contractante via un indice centralisé sur une base *hit/no-hit* ; ensuite, un accès direct en ligne permettant la lecture de la base de données relative aux immatriculations de véhicules d'un autre Etat contractant. Certes, l'échange d'informations est limité aux points nationaux de contact où travaille un personnel spécifiquement affecté à cette tâche. Néanmoins, avec ce modèle, le traité de Prüm a établi une forme avancée d'échange transnational d'informations. Les échanges d'information et les autres formes de coopération concernant des événements de grande envergure, catastrophes et accidents graves et dans le cas de danger imminent sont également réglementés par le traité de Prüm. En outre, les services répressifs et de l'immigration peuvent être autorisés à effectuer des opérations conjointes sur le territoire d'une partie contractante. Le traité est entré en vigueur le 1<sup>er</sup> novembre 2006. Le CEPD a qualifié l'approche suivie par le traité de Prüm d'approche « catégorie de données par catégorie de données », « une approche plus prudente portant sur un seul type de données », qui évalue ensuite « dans quelle mesure le principe de disponibilité peut réellement contribuer au respect de la loi, ainsi que les risques spécifiques pour la protection des données à caractère personnel » (paragraphe 50 de l'Avis sur la proposition de décision-cadre du Conseil relative à l'échange d'informations en vertu du principe de disponibilité; JO 2006 C 116). Il est moins préjudiciable, d'autre part, que le traité de Prüm « entraîne nécessairement la création de nouvelles bases de données, ce qui présente des risques pour la protection des données à caractère personnel » (para. 49).

#### TRAITE DE PRÜM

Les articles concernant notre sujet sont les articles 2 à 15. Les Parties contractantes (PC) conservent les fichiers des analyses ADN. Elles autorisent les points de contact nationaux des autres PC à accéder aux données de référence dans leurs fichiers (accès *hit/no-hit*). Si la procédure montre une concordance entre les profils ADN, la transmission de toute autre information est régie par le droit national (article 2-6). Sur demande, la PC sollicitée accorde l'entraide judiciaire en prélevant et en analysant le matériel génétique d'une personne présente sur le territoire de la PC sollicitée et conformément à la législation de la PC sollicitée (article 7). Les PC autorisent le point de contact national des autres PC à accéder aux données indexées de leurs systèmes automatisés d'identification dactyloscopique créés, avec le droit de procéder à une consultation automatisée à l'aide d'une comparaison des données dactyloscopiques (article 8-9(1)). L'établissement définitif d'un lien entre une donnée dactyloscopique et une donnée indexée de la Partie contractante gestionnaire du fichier est réalisé par le point de contact national de la Partie ayant réalisé la consultation (article 9(2)). La transmission d'autres données à caractère personnel se rapportant aux données indexées ainsi que d'autres informations s'opère en vertu du droit national (article 10). Les PC autorisent les points de contacts nationaux des autres PC à accéder à des données des registres nationaux des véhicules, relatives notamment aux propriétaires et opérateurs et aux véhicules dans le respect du droit national de la PC effectuant la consultation (article 12(1)). En vue de prévenir des infractions pénales et de maintenir l'ordre et la sécurité publics lors de manifestations de grande envergure à dimension transfrontalière, en particulier dans le domaine sportif ou en rapport avec des réunions du Conseil européen, les PC se transmettent mutuellement, sur demande ou de leur propre initiative, et suivant le droit national de la PC transmettant les données, des données relatives à des personnes, lorsque des condamnations définitives ou d'autres faits justifient la présomption que ces personnes vont commettre des infractions pénales dans le cadre de ces événements ou qu'elles présentent un danger pour l'ordre et la sécurité publics, pour autant que la transmission de ces données soit permise suivant le droit national de la PC transmettant les données (article 14(1)). En tout état de cause, les données transmises sont effacées au plus tard après un an (article 14(2)). (Cf. l'aperçu de la situation des ratifications et dates d'entrée en vigueur du traité de Prüm dans l'annexe A au présent article.)

Comme l'Initiative suédoise, le traité de Prüm a nettement accru la pression exercée sur les intentions législatives de la Commission depuis l'adoption du Programme de La Haye. Suite à l'avancée que Prüm représente sur la voie de la réalisation du principe de disponibilité, la question s'est posée de savoir comment passer à l'étape suivante au niveau de l'UE. Il était fait référence tant à l'Initiative suédoise qu'au traité de Prüm, présentées comme les

approches « les plus importantes » dans la Proposition de décision-cadre du Conseil relative à l'échange d'informations en vertu du principe de disponibilité, présentée par la Commission le 12 octobre 2005 (COM(2005) 490 final). Même si le CEPD souligne les similarités entre l'actuelle proposition visant à appliquer le principe de disponibilité et le traité de Prüm, il exprime aussi des critiques. L'exposé des motifs de la proposition souligne « sept obstacles principaux » à « la disponibilité générale, dans toute l'UE, des informations ». Entre autres, le CEPD critique les accords bilatéraux ou multilatéraux entre Etats membres, considérés comme « géographiquement limités » (Prüm) ou parce qu'ils « ne font pas obligation aux Etats membres de fournir des informations, de sorte que l'échange de données est soumis à un pouvoir discrétionnaire » (Initiative suédoise). En outre, « les formes actuelles de coopération dans l'action répressive exigent généralement l'intervention des unités nationales ou des points de contact centraux ». Elle estime donc que le potentiel du principe de disponibilité n'est donc pas épuisé. L'Initiative suédoise et Prüm sont salués pour mieux éclairer l'approche élargie de la proposition elle-même, qui :

pose, quant à elle, le principe d'un accès en ligne aux informations disponibles et aux données d'index renvoyant à des informations non accessibles en ligne, dès que les États membres auront notifié les informations disponibles sur leur territoire. Ce faisant, elle évite de devoir chercher partout les données nécessaires, puisqu'il sera possible de savoir si les informations recherchées sont disponibles avant même d'émettre une demande d'informations, et permet d'introduire des demandes ciblées et efficaces. Elle harmonise en outre les motifs de refus, lesquels lient également les autorités qui – en vertu du droit national – doivent autoriser l'accès aux informations ou leur transfert. L'incertitude inhérente à toute demande d'informations est donc fortement atténuée (p. 4).

PROPOSITION DE DECISION-CADRE DU CONSEIL relative à l'échange d'informations en vertu du principe de disponibilité (COM(2005) 490 final)

La proposition de décision-cadre (PDC) oblige les Etats membres à faire en sorte que les informations soient fournies, dans les conditions prévues par la présente décision-cadre, aux autorités compétentes équivalentes des autres États membres et à Europol (article 6). L'équivalence entre les autorités compétentes des États membres est évaluée, sur la base d'une liste de critères (article 5(1)). L'« information » est définie comme étant « les informations existantes » (article 3(a)) des types suivants : profils ADN, empreintes digitales, balistique, Informations sur les immatriculations de véhicules, Numéros de téléphone et autres données relatives aux communications (à l'exclusion de données sur le contenu), données personnelles (Annexe II). Les informations qui ont été collectées légalement en recourant à des mesures coercitives sont traitées comme des informations disponibles (article 2(2)). L'équivalence entre les autorités compétentes des États membres est évaluée sur la base d'une liste de critères (article 5(1)). L'obligation de transmettre des informations comprend l'obligation de veiller à ce que les Etats fassent en sorte que les autorités compétentes équivalentes des autres États membres et Europol aient accès en ligne aux informations contenues dans les bases de données électroniques auxquelles leurs autorités compétentes correspondantes ont un tel accès (article 9(1)), sachant que « accès en ligne » signifie l'accès automatisé, sans intervention d'une autre autorité ou d'une autre partie, à une base de données électronique aux fins de consultation de son contenu et d'accès à celui-ci à partir d'un autre lieu que celui où est installée cette base de données (article 3(f)). C'est la première des deux dispositions clé, qui font en sorte que les données d'index renvoyant à des informations non accessibles en ligne soient consultables en ligne [...] et mettent en place à cet effet l'infrastructure technique appropriée (article 10(1)). Lorsqu'en consultant des données d'index, une autorité compétente équivalente trouve une correspondance, elle peut émettre une demande d'information (article 11). La transmission des informations peut être refusée pour protéger les droits fondamentaux et les libertés fondamentales des personnes dont les données sont traitées en vertu de la PDC (Article 14(1)(d)).

Tout d'abord, l'accès en ligne, « sans intervention d'une autre autorité ou d'une autre partie » signifie en fait la perte de contrôle d'un Etat membre sur le traitement des données collectées par cet Etat. Ensuite, l'obligation figurant dans la proposition d'établir une infrastructure technique appropriée pour les fichiers de données d'index est très onéreuse et demande

beaucoup de temps. Dans ce contexte, la proposition en est restée au niveau d'une monstruosité optimiste. En revanche, l'Initiative suédoise a été un réel succès, même si elle reste en retrait par rapport à la vision développée au niveau de l'UE. L'Initiative doit être vue comme une solution pragmatique et de bon sens au problème brûlant de la mise en place aussi rapidement que possible d'un cadre légal pour les échanges transnationaux de données.

Comme la proposition en est restée au statut de projet, au moins à ce stade, il semble que ce soit Prüm qui ait effectivement ouvert la voie pour la poursuite de la mise en œuvre du principe de disponibilité. Pour leurs sept initiateurs, le traité apparaît comme un succès. Finalement, sous la pression accrue due au nombre croissant d'Etats adhérant au traité (cf. Annexe A du présent article), en juin 2008, les dispositions du traité de Prüm furent intégrées, en substance, dans le cadre juridique de l'Union européenne par la décision du Conseil 2008/615/JAI relative à l'approfondissement de la coopération transfrontalière, notamment en vue de lutter contre le terrorisme et la criminalité transfrontalière (JO 2008 L 210). La présidence allemande avait lancé le débat sur l'intégration de Prüm dans le cadre juridique de l'Union européenne lors d'une réunion informelle des ministres, à Dresde, les 15–16 janvier 2007 et a immédiatement recueilli un large soutien. Alors que le Secrétariat du Conseil n'avait pas eu besoin de plus de quatre jours après la réunion pour publier un premier projet de décision du Conseil, à peine un mois plus tard, le 15 février 2007, lors du Conseil de la Justice et des Affaires intérieures, 15 Etats membres s'accordaient sur l'adoption d'une décision du Conseil sans consulter davantage les autres Etats membres et le Parlement européen, sans autres études d'incidence ou autres, comme le Programme de La Haye le demandait pourtant. « Nous avons été mis devant le *fait accompli* [...] La manière dont l'accord a été obtenu démontre seulement à quel point les Eurocrates peuvent manœuvrer de manière sournoise – le tout aux dépens de la souveraineté nationale » (Kierkegaard 2009).

La décision du Conseil rejoint le système de Prüm en l'identifiant comme compatible avec le principe de disponibilité. Cela montre sans le moindre doute que Prüm n'a pas contourné le cadre UE. Si le traité de Prüm a violé le droit de l'UE (en ne respectant pas l'obligation de coopération visée à l'article 10 TCE ; cf. Balzacq 2006), cela n'a pas eu de conséquence : « On pourrait certes affirmer que le traité de Prüm enfreint le droit de l'Union européenne. [...]. Toutefois, il s'agit d'un argument essentiellement théorique, étant donné que, dans le cadre du troisième pilier, la Commission a des compétences limitées pour veiller au respect du droit de l'Union européenne par les États membres [...] » (Avis du CEPD du 4 avril 2007 (JO 2007 C 169), para. 14). Comme l'histoire le montre, les initiateurs pouvaient escompter avec une relative certitude que leur initiative serait finalement entérinée par la politique commune de l'UE comme l'art. 1(4) du traité de Prüm le prévoyait. L'instrumentalisation stratégique mutuelle des propositions nationales, des initiatives intergouvernementales et l'eupéanisation constituent la dynamique de la législation en cours sur les échanges transnationaux d'informations. Les autres Etats membres ont été encouragés à se joindre à eux, ou n'ont pas été écoutés. La présidence allemande était tout à fait consciente du fait que l'UE, avec son appareil administratif, voulait conserver son leadership et le contrôle du processus. Tôt ou tard, en dépit de toutes les ambiguïtés, l'UE saluerait le potentiel très intégrateur de Prüm pour répondre aux exigences du Programme de La Haye. Hugo Brady a donc raison de corriger les critiques de certains observateurs comme Balzacq et al. (2006) selon qui le traité irait à contre-courant de l'intégration de l'UE (p. 2):

Certains observateurs ont craint que le groupe de Prüm puisse saper les efforts visant à faciliter le partage des informations dans l'ensemble de l'UE, parce qu'il n'impliquait qu'une poignée de pays et qu'il ignorait les initiatives de la Commission européenne en la matière. Mais il s'est avéré que le traité de Prüm a été la meilleure manière d'encourager un plus large partage des informations. Le groupe des sept pays de Prüm a fait office de laboratoire en négociant en petit groupe des accords techniques complexes pour permettre une interrogation mutuelle rapide et efficace des bases de données de chacun (Brady 2007, pp. 21–22).

L'intégration de Prüm dans le cadre de l'UE a été un résultat hautement apprécié. Il concorde parfaitement avec l'idée de l'eupéanisation, de la transformation du marché commun en un Etat européen commun, déjà mise en exergue dans l'espace de liberté, de sécurité et de justice. De fait, à certains égards, l'eupéanisation de Prüm peut être considérée comme la réalisation de la proposition de la Proposition de la Commission de décision-cadre du Conseil relative à l'échange d'informations en vertu du principe de disponibilité (COM (2005) 490 final). Il n'était plus nécessaire d'insister sur la proposition parce que la décision 2008/615/JAI (« décision Prüm ») a poussé le processus législatif aussi loin que possible pour l'instant. L'Initiative suédoise a également été intégrée dans les dispositions de la décision : dans le cas d'une concordance dans les données d'indice liées par ex. à un fichier de données de contenu ADN, le mécanisme bien établi basé sur la décision 2006/960/JAI (Initiative suédoise) peut être utilisé pour demander des données de contenu (préambule, para. 10). La décision Prüm fusionne donc les différents courants en matière de législation sur les échanges transnationaux d'information qui ont émergé depuis que le programme de La Haye avait invité à proposer des approches novatrices.

DECISION DU CONSEIL 2008/615/JAI du 23 juin 2008 relative à l'approfondissement de la coopération transfrontalière, notamment en vue de lutter contre le terrorisme et la criminalité transfrontalière (JO 2008 L 210)

La décision du Conseil (DC) incorpore en substance les parties essentielles du traité de Prüm dans le cadre juridique de l'UE (préambule, para. 1 et 9). « A l'égard des États membres concernés, les dispositions pertinentes de la présente décision s'appliquent en lieu et place des dispositions correspondantes qui figurent dans le traité de Prüm. Les autres dispositions du traité de Prüm restent d'application entre les parties contractantes du traité de Prüm. » (art. 35(1)). La DC ne reprend pas les dispositions suivantes du traité de Prüm : les dispositions sur les gardes armés à bord des aéronefs (art. 17–19) ; les mesures de lutte contre les migrations illégales (art. 20 –23) ; les mesures en cas de danger présent (*hot pursuit*) (art. 25) ; la coopération sur demande (art. 27). Les autres dispositions sont identiques, presque mot pour mot. La DC contient notamment des dispositions sur (a) la transmission automatisée de profils ADN, empreintes digitales et données d'immatriculation des véhicules (Chapitre 2) ; (b) les conditions de la transmission d'informations en vue de prévenir des infractions terroristes (art. 16) ; (c) la fourniture de données liées à des événements majeurs ayant une dimension transfrontalière (art. 18) ; (d) les opérations conjointes (art. 17). La DC souligne la possibilité de recourir à la procédure de demande conformément à la DC 2006/960/JAI suite à une concordance dans un fichier de données indexées. En matière de protection des données, la DC souligne avec insistance que « ces arrangements en matière de protection des données devraient tenir particulièrement compte de la nature spécifique de l'accès en ligne transfrontalier aux bases de données. *Etant donné que, avec l'accès en ligne, il n'est pas possible pour l'Etat membre gestionnaire du dossier de réaliser des contrôles préalables, il conviendrait de mettre en place un système garantissant qu'une vérification ultérieure est bien effectuée* (préambule, para. 17) [c'est nous qui soulignons]. La DC souligne aussi que « la transmission de données à caractère personnel à un autre Etat membre exige un niveau suffisant de protection des données de la part de l'Etat membre destinataire » (préambule, para. 18). En matière de transposition, « les Etats membres prennent les mesures nécessaires pour se conformer aux dispositions de la présente décision dans l'année qui suit sa prise d'effet, à l'exception du chapitre 2, pour lesquelles les mesures nécessaires seront prises dans les trois ans qui suivent la prise d'effet de la présente décision et de la décision du Conseil relative à la mise en œuvre de la présente (art. 36). Les délais de transposition sont donc respectivement août 2009 et août 2011.

La décision Prüm n'est certainement pas une application du principe de disponibilité au plein sens du terme. Lorsque le Programme de La Haye voyait dans ce principe une réaction au « fait que ces informations franchissent les frontières ne devrait plus être pris en considération [c'est nous qui soulignons], cela semble difficilement être le cas. Il existe différents modèles couvrant différents degrés du principe qui doivent être pris en considération pour comprendre la logique de sa réalisation. Selon Bigo et al. (2007), le principe de disponibilité se divise en

deux sous-principes : *visibilité* et *lisibilité*. Si l'on tient compte aussi de l'Initiative suédoise, il convient d'en ajouter un troisième qui pourrait être appelée le sous-principe *pragmatique*. Il est basé sur l'accès indirect à l'information sur demande. Le sous-principe de la visibilité de l'information est en fait déjà un pas en avant. Il est basé sur le modèle *hit/no-hit* pour lancer une recherche de données auprès d'une unité centrale ou d'une base de données nationale pour identifier si elle contient un élément spécifique. En cas de concordance (« hit »), les services répressifs peuvent demander davantage d'informations à l'Etat membre où les données en questions sont stockées. Seul le sous-principe de lisibilité de l'information implique un accès intégral à la lecture en ligne. Le fait que Prüm est un système mixte montre que le sous-principe de lisibilité totale est seulement envisagé et que l'affirmation selon laquelle le fait que l'information franchisse la frontière ne serait plus pertinent est un pur phantasme technocratique ou l'expression de l'idéologie naturelle d'une instance transnationale.

Dans son avis précité du 4 avril 2007 (JO 2007 C 169), le CEPD commente la décision Prüm attendue : « l'initiative ne constitue qu'un petit pas. [...] L'initiative peut être qualifiée de mesure allant dans le sens de la disponibilité, mais au sens strict elle n'applique pas le principe de disponibilité » (para. 24). Cela signifie-t-il toutefois que le processus de pleine réalisation du principe soit parvenu à son terme ? La situation de la législation communautaire sur la protection des données correspond parfaitement à la vision d'une réalisation progressive du principe de disponibilité au-delà de Prüm. La réalisation du principe de disponibilité doit s'accompagner d'une législation correspondante sur la protection des données. Dans sa proposition du 8 juin 2006 de Recommandation au Conseil sur l'interopérabilité des bases de données européennes dans le domaine JAI et sur la création de synergies entre ces bases, Alexander Alvaro exprimait déjà sa grande préoccupation sur les risques liés à l'utilisation de bases de données à grande échelle. Il mentionnait explicitement l'établissement de profils, l'extraction de données et l'utilisation abusive de ces bases à des fins autres que celles pour lesquelles elles ont initialement été conçues. Il s'agit d'un problème de principe. L'absence d'une décision-cadre sur la protection des données dans le troisième pilier a créé une situation où la protection des données personnelles a pris un tour précaire. Cette situation s'est aggravée sous l'impact du principe de disponibilité. Elle est devenue inacceptable vis-à-vis d'une politique dont le principe directeur, depuis la Stratégie européenne de sécurité (décembre 2003, établie sous l'autorité du HR Javier Solana) est l'intensification des mesures de lutte contre la criminalité basée sur la surveillance de la vie quotidienne des citoyens européens. L'affirmation de Solana selon laquelle la sécurité externe et la sécurité interne étaient indissolublement liées avait une double implication. D'abord, elle signifiait que la sécurité interne ne devait pas seulement être assurée dans le pays mais aussi à l'étranger, dans la mesure où l'action extérieure façonnait l'environnement dans lequel l'UE se trouvait insérée. Ensuite, et c'est ce point qui importe le plus dans ce contexte, cela voulait dire que la sécurité externe devait aussi être assurée dans le pays même. Dans la même veine, le *9/11 Report* de la « *National Commission on Terrorist Attacks upon the United States* » (juillet 2004) affirmait : « dans le monde de l'après – 11 septembre, les menaces sont définies davantage par les lignes de fracture au sein des sociétés que par les délimitations territoriales entre eux » (*9/11 Report*, p. 361). Ce changement capital dans la définition des conditions dans lesquelles il faut assurer la sécurité modifie nécessairement les relations entre l'Etat, ses services répressifs et les citoyens : « le risque réel est la liberté et le véritable ennemi de la société – en principe et en général – c'est le citoyen libre » (Nelles 2004, p. 84). *Suivant cette définition, la protection des données apparaît comme un risque pour la sécurité.* La formulation du principe de disponibilité est l'une des conséquences les plus graves des évaluations de la situation telles que celles fournies par la *Stratégie européenne de sécurité* ou le rapport de la *9/11 Commission Report*. Et ce principe de disponibilité est l'ennemi naturel du principe clé de la protection des données – le principe de la limitation des finalités.

La dernière chance de régler le problème de la grande diversité des règles de protection des données dans l'UE, qui touche en particulier l'échange transnational d'information, a été

gâchée. Il faut noter que cela s'est passé une fois encore sous la présidence allemande – la même année qui vit l'intégration de Prüm dans le droit de l'UE. Après plusieurs années de discussions et de débats au niveau européen et au niveau national, la présidence allemande a modifié la proposition initiale de décision-cadre présentée par la Commission en ignorant tout simplement les nombreuses préoccupations à ce sujet. La décision-cadre 2008/977/JAI (JO 2008 L 350) du Conseil sur la protection des données personnelles, adoptée en décembre dernier, apparaît en rupture avec la conception qui veut les données personnelles soient en principe protégées contre un accès complet de l'Etat.

Le principe de disponibilité continuera à faire office de leitmotiv mais il sera complété par ce qu'on appelle le *principe de convergence* tel qu'il a été formulé par le Groupe Futur dans son rapport de juin 2008 :

Le *principe de convergence* s'appliquera à tous les domaines où des relations plus étroites entre Etats membres sont possibles : agents, institutions, pratiques, équipements et cadres juridiques. Ces relations plus étroites seront basées sur l'acquis de l'Union et feront pleinement usage des instruments de l'Union européenne. On cherchera systématiquement une valeur ajoutée dans la définition et la mise en œuvre des projets correspondants. Rechercher de la valeur ajoutée et développer le principe de convergence conduisent au même objectif. Plus les Etats membres coopèrent étroitement entre eux, plus les valeurs partagées et les réserves nationales apparaîtront clairement (p. 11).

Ce principe de convergence rappelle fortement *l'approche élargie et cohérente* du Coordinateur pour la lutte contre le terrorisme. La politique européenne de sécurité a bien entendu conscience qu'une pure interopérabilité technique ne suffit pas pour faire progresser l'efficacité de la lutte contre les menaces pour la sécurité.

## V. REMARQUES DE CONCLUSION ET RECOMMANDATIONS

Le Programme de La Haye était déficient. Sa recommandation de faire pleinement usage des nouvelles technologies en vertu du principe de disponibilité était non seulement irréaliste mais technocratique, comme trois aspects au moins ont permis de s'en apercevoir :

1. l'incapacité complète d'adapter de manière appropriée la législation sur la protection des données, en mettant ainsi en danger le respect de la vie privée et les libertés civiles ;
2. l'aveuglement face à ce qu'on pourrait appeler la diversité des cultures de la sécurité parmi les services répressifs, provoquant ainsi une discrétion accrue et même un refus des autorités de partager des données entre elles ;
3. la réduction du problème politique et social très sensible posé par les échanges transnationaux d'informations à un problème purement technologique, comme cela apparaît de la manière la plus marquée dans les investissements inadéquats dans SIS II ou dans la préparation de l'après – Programme de La Haye qui se focalise sur la création d'une intégration totale de l'information de la vie quotidienne.

**S'agissant de ces trois domaines, on peut formuler les remarques et les recommandations suivantes.**

### **Ralentir l'évolution du Régime européen de la sécurité**

Si l'avenir du régime européen de la sécurité doit être celui d'un *ordre* gérable au mieux des intérêts des citoyens européens, d'autres types de flexibilité, d'anticipation et de participation démocratique doivent entrer en jeu. Cela implique nécessairement que l'évolution future du Régime européen de la sécurité doit être ralentie d'urgence et sa situation actuelle faire l'objet d'une évaluation complète avant d'adopter de nouvelles mesures.

1. Il est à conseiller de ne pas élargir davantage les catégories de personnes à inscrire dans les systèmes de traitement et d'échange des informations (par ex. les « auteurs de trouble »).
2. Il est à conseiller de ne pas élargir davantage les catégories de données personnelles à inscrire dans les systèmes de traitement et d'échange des informations.
3. Il est à conseiller de ne pas élargir davantage les catégories d' « autorités compétentes » ayant accès aux systèmes de traitement et d'échange des informations.
4. Dans ce contexte, il n'est pas seulement recommandable mais impératif d'évaluer le niveau d'accès des services secrets aux systèmes d'échange transnational d'informations. Cela paraît nécessaire en raison de l'importance croissante du rôle des services secrets dans l'action de lutte contre le terrorisme (cf. chap. 4 du *Report of the Eminent Jurists Panel on Terrorism, Counter-Terrorism and Human Rights*, récemment publié).
4. Il est à conseiller de ne pas simplifier davantage les procédures d'échange des informations entre les services répressifs (par ex., accès en lecture directe).
5. Au contraire, il est à conseiller de reconnaître la procédure d'échange transnational d'information décrite plus haut en vertu de la décision-cadre 2006/960/JAI (Initiative suédoise) comme un *modèle standard*.
6. Sur la base de ce Modèle suédois qui fonctionne déjà, une harmonisation juridique non sollicitée, *volontaire*, et progressive semble la plus concevable, de même qu'un rapprochement culturel du travail policier au sein de l'UE, parce que ce modèle est le moins agressif sur l'échelle de l'intégration transnationale des données, comme l'a souligné la Note de la présidence luxembourgeoise (voir ci-dessus, p. 15).
7. Il semble n'y avoir que *très peu de recherches universitaires indépendantes sur l'efficacité réelle* de la politique instaurant progressivement un échange transnational d'informations entre les services répressifs au sein de l'UE. Cette situation peut être la conséquence du fait que, comme Fijnaut et Paoli (2004, p. 1040) l'ont observé dans un contexte similaire, « les pouvoirs politiques nationaux et internationaux n'ont pas intérêt à voir les résultats de telles recherches révéler qu'il existe une différence énorme entre la politique telle qu'elle est formulée sur papier et les résultats atteints en pratique ». Mais parce que l'échange transnational d'information a des conséquences politiques et sociales considérables, cette situation doit changer : il faut développer cette recherche universitaire indépendante empirique. Cela représenterait une étape décisive vers une démocratisation urgente et nécessaire de l'actuelle politique de l'UE dans les questions de sécurité (intérieure).

### **Réglementer les pratiques des services répressifs en matière d'échange des données**

Jusqu'à présent, la législation sur la protection des données a fait l'objet de nombreuses critiques concernant son manque d'efficacité, sa tendance à être réactive plutôt que proactive, son incapacité à suivre le rythme du rapide développement des nouvelles technologies et procédures de la surveillance et de l'information. A juste titre, parce que ce sont les exigences de la protection des données qui doivent déterminer la technologie et non l'inverse.

8. Une approche importante pour résoudre le problème du caractère purement réactif de la législation traditionnelle en matière de protection des données est une méthodologie appelée « KORA » (« Konkretisierung rechtlicher Anforderungen », c'est-à-dire « concrétisation des exigences juridiques »), développée par Alexander Roßnagel (Université de Kassel, Allemagne). KORA vise à combler le fossé entre les dispositions juridiques générales et les décisions spécifiques dans le processus de la conception technique. L'application de KORA

signifie que les exigences juridiques pour les technologies concernées se basent sur les normes constitutionnelles et les autres normes de droit. Ces exigences juridiques sont transformées en critères pour la conception de systèmes techniques spécifiques. Les juristes et les experts techniques travaillent ensemble pour répondre à la question de savoir quelles sont les fonctions essentielles que doit posséder la technologie pour répondre à ces critères légaux définis. KORA représente une tentative d'intégrer la protection des données dans le processus de conception technique. Il convient de faire usage d'une *méthode hybride (juridico-technique)* pour le développement des futurs systèmes de traitement et d'échange de l'information.

### ***Constructive Technology Assessment***

Un autre point, qui n'a pas été cité explicitement dans le présent article, doit être abordé : le problème du manque d'acceptation de la technologie qui va de pair avec l'introduction de technologies toujours plus sophistiquées, par ex. des systèmes complexes d'échange automatisé d'informations.

9. Une approche importante pour résoudre ce problème consiste en ce qu'on appelle l'évaluation constructive des technologies ou Constructive Technology Assessment (CTA). La CTA entend œuvrer à de *meilleures technologies*, c'est-à-dire des *technologies ayant moins d'effets sociaux négatifs*, depuis les premiers stades des cycles de vie technologique. Dans la perspective de la CTA, l'évaluation des technologies est considérée comme faisant partie d'une co-évolution réflexive des sciences, des technologies et de la société - elle est dès lors *constructive* : « la CTA peut être vue comme une nouvelle pratique de conception – comprenant des outils – où les impacts sont anticipés et les utilisateurs et les autres communautés concernées sont impliqués depuis le début, sur un mode interactif, et qui contient un élément d'apprentissage sociétal » (Schot et Rip 1996, p. 255). Le recours au CTA doit être encouragé pour soutenir à la fois les décideurs politiques en matière d'échange transnational d'informations et les utilisateurs finaux des systèmes techniques au sein des services répressifs afin d'éviter autant que possible les discordances, les conflits éventuels et les investissements erronés.

10. Les auteurs du présent article espèrent que le futur Groupe de travail du Conseil sur les échanges transnationaux d'information sera conscient du fait que la capacité d'une technologie de résoudre les problèmes peut être parfois supérieure à la capacité de la société de résoudre les problèmes posés par l'usage de cette technologie.

## VI. BIBLIOGRAPHIE

### Publications au Journal Officiel

- OJ 2000 L 239: Agreement between the Governments of the States of the Benelux Economic Union, the Federal Republic of Germany and the French Republic on the gradual abolition of checks at their common borders [Schengen Agreement, 1985]
- OJ 2000 L 239: Convention implementing the Schengen Agreement of 14 June 1985 [1990]
- OJ 2000 L 316: Council Regulation (EC) No 2725/2000 concerning the establishment of ‘Eurodac’ for the comparison of fingerprints for the effective application of the Dublin Convention
- OJ 2001 L 101: Council Decision 2001/264/EC adopting the Council’s security regulations
- OJ 2003 L 16: Council Decision 2003/48/JHA on the implementation of specific measures for police and judicial cooperation to combat terrorism
- OJ 2003 L 50: Council regulation (EC) No 343/2003 establishing the criteria and mechanisms for determining the Member State responsible for examining an asylum application lodged in one of the Member States by a third-country national
- OJ 2004 L 162: Council Regulation (EC) No 871/2004 concerning the introduction of some new functions for the Schengen Information System, including in the fight against terrorism
- OJ 2004 L 213: Council Decision 2004/512/EC establishing the Visa Information System (VIS)
- OJ 2004 C 281: Initiative of the Kingdom of Sweden with a view to adopting a Framework Decision on simplifying the exchange of information and intelligence between law enforcement authorities of the Member States of the European Union, in particular as regards serious offences including terrorist acts
- OJ 2005 L 68: Council Decision 2005/211/JHA concerning the introduction of some new functions for the Schengen Information System, including in the fight against terrorism
- OJ 2005 L 253: Council Decision 2005/671/JHA on the exchange of information and cooperation concerning terrorist offences
- OJ 2006 C 91: Opinion of the EDPS on the Proposals COM(2005) 230 final, 236 final and 237 final [concerning establishment, operation and use of SIS II]
- OJ 2006 C 97: Opinion of the EDPS on the Proposal for a Council Decision concerning access for consultation of the Visa Information System (VIS) by the authorities of Member States responsible for internal security and by Europol for the purposes of the prevention, detection and investigation of terrorist offences and of other serious criminal offences (COM(2005) 600 final)
- OJ 2006 C 116: Opinion of the EDPS on the Proposal for a Council Framework Decision on the exchange of information under the principle of availability (COM(2005) 490 final)
- OJ 2006 L 381: Regulation (EC) No 1986/2006 of the European Parliament and of the Council regarding access to SIS II by the services in the Member States responsible for issuing vehicle registration certificates
- OJ 2006 L 381: Regulation (EC) 1987/2006 of the European Parliament and of the Council on the establishment, operation and use of SIS II
- OJ 2006 L 386: Council Framework Decision 2006/960/JHA on simplifying the exchange of information and intelligence between law enforcement authorities of the Member States of the EU
- OJ 2007 C 169: Opinion of the EDPS on the Initiative of the Kingdom of Belgium, the Republic of Bulgaria, the Federal Republic of Germany etc., with a view to adopting a Council Decision on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime
- OJ 2007 L 205: Council Decision 2007/533/JHA on the establishment, operation and use of SIS II
- OJ 2008 L 210: Council Decision 2008/615/JHA on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime
- OJ 2008 L 350: Council Framework Decision 2008/977/JHA on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters
- OJ 2009 C 42: Opinion of the EDPS on the proposal for a Council Decision on the establishment of the European Criminal Records Information System (ECRIS)

## **Publications du Conseil de l'Union européenne**

- Declaration on combating terrorism (7906/04; 29 March 2004)
- Exchange of Information [Note from the Presidency] (12680/04; 22 September 2004)
- The Hague Programme (16054/04; 13 December 2004)
- Replies to questionnaire on Framework Decision on simplifying the exchange of information and intelligence between law enforcement authorities of the Member States of the EU, in particular as regards serious offences including terrorist acts (5815/1/05 REV 1; 2 February 2005)
- Approach for the implementation of the principle of availability [Note from the Presidency] (7641/05; 25 March 2005)
- Prüm Convention [i.e., Treaty of Prüm] (10900/05; 7 July 2005)
- The European Union Counter-Terrorism Strategy [Note from the Presidency and the EU Counter-Terrorism Coordinator] (14469/4/05 REV 4; 30 November 2005)
- List of competent authorities which are authorised to search directly the data contained in the Schengen Information System pursuant to Art. 101(4) of the Schengen Convention (6073/2/07 REV 2; 25 June 2007)
- Implementation of the Strategy and Action Plan to Combat Terrorism [Note from the EU Counter-Terrorism Coordinator] (15411/07; 23 November 2007)
- EU Counter-Terrorism Strategy — Discussion paper [Note from the EU Counter-Terrorism Coordinator] (15983/08; 19 November 2008)
- Council Decision on the establishment of the European Criminal Records Information System (ECRIS) in application of Article 11 of Framework Decision 2008/.../JHA [draft] (14571/08; 20 January 2009)
- Press Release: 2927<sup>th</sup> meeting of the Council Justice and Home Affairs, Brussels, 26–27 February 2009 (6877/09 (Presse 51))

## **Publications de la Commission des Communautés européennes**

- Towards enhancing access to information by law enforcement agencies [Communication to the Council and the European Parliament] (COM(2004) 429 final; 16 June 2004)
- Proposal for a Council Decision on the establishment, operation and use of SIS II (COM(2005) 230 final; 31 May 2005)
- Proposal for a Regulation of the European Parliament and of the Council on the establishment, operation and use of SIS II (COM(2005) 236 final; 31 May 2005)
- Proposal for a Regulation of the European Parliament and of the Council regarding access to SIS II by the services in the Member States responsible for issuing vehicle registration certificates (COM(2005) 237 final; 31 May 2005)
- Proposal for a Council Framework Decision on the exchange of information under the principle of availability (COM(2005) 490 final; 12 October 2005)
- Communication on improved effectiveness, enhanced interoperability and synergies among European databases in the area of Justice and Home Affairs [to the Council and the European Parliament] (COM(2005) 597 final; 24 November 2005)
- Preparing the next steps in border management in the European Union [Communication to the European Parliament, the Council, The European Economic and Social Committee and the Committee of the Regions] (COM(2008) 69 final; 13 February 2008)
- Preparing the next steps in border management in the EU [Commission Staff Working Document accompanying COM(2008) 69 final] (SEC(2008) 153; 13 February 2008)
- Proposal for a Regulation of the European Parliament and of the Council [...] amending Regulation (EC) No 562/2006 as regards the use of the Visa Information System (VIS) under the Schengen Borders Code (COM(2008) 101 final; 22 February 2008)
- Proposal for a Council Decision on the establishment of the European Criminal Records Information System (ECRIS) in application of Article 11 of Framework Decision 2008/XX/JHA (COM(2008) 332 final; 27 May 2008)
- Annual report to the Council and the European Parliament on the activities of the EURODAC Central Unit in 2007 (COM(2009) 13 final; 26 January 2009)

## Autres documents et rapports officiels

- [Javier Solana]: *European Security Strategy (A secure Europe in a better world)*. Brussels, 12 December 2003
- *The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks upon the United States*. Official Government Edition, 22 July 2004
- House of Lords: *After Madrid: the EU's response to terrorism*. 5<sup>th</sup> Report of Session 2004–05 of the European Union Committee, HL Paper 53, London, 8 March 2005
- European Data Protection Supervisor: *Comments on the Communication of the Commission on interoperability of European databases*. Brussels, 10 March 2006 [disponible sur EDPS website]
- Alvaro, Alexander: “Proposal for a recommendation to the Council on interoperability and synergies among European databases in the area of justice and home affairs”. Session document B6–0336/2006 of the European Parliament, 8 June 2006
- Schengen Joint Supervisory Authority: *Article 99 Inspection: report on an inspection of the use of Article 99 alerts in the Schengen Information System*. Report nr. 07–02, Brussels, 18 December 2007
- The Association of European Police Colleges (AEPC): *AEPC, the future: strategy document*. 2008 [disponible sur [www.aepc.net](http://www.aepc.net)]
- Frattini, Franco: *Providing Europe with the tools to bring its border management into the 21<sup>st</sup> century*. Speech (08/142) at the Ministerial Conference on the Challenges of the EU External Border Management, Brdo (Slovenia), 12 March 2008
- The Future Group: *Freedom, Security, Privacy — European Home Affairs in an open world*. Report of the Informal High Level Advisory Group on the Future of European Home Affairs Policy, June 2008
- *Défense et sécurité nationale: Le livre blanc*. Paris, June 2008
- [Eminent Jurists Panel]: *Assessing Damage, Urging Action: Report of the Eminent Jurists Panel on Terrorism, Counter-terrorism and Human Rights*. Geneva, 2009

## Bibliographie secondaire

- Balzacq, Thierry: *The Treaty of Prüm and the principle of loyalty (Art. 10 EC)*. Briefing Paper for LIBE, 13 January 2006 [disponible sur [www.libertysecurity.org](http://www.libertysecurity.org)]
- Balzacq, Thierry et al.: *Security and the two-level game: the Treaty of Prüm, the EU and the management of threats*. CEPS Working Document No. 234, January 2006 [disponible sur [www.ceps.eu](http://www.ceps.eu)]
- Bigo, Didier et al.: *The principle of information availability*. 1 March 2007 [disponible sur [www.libertysecurity.org](http://www.libertysecurity.org)]
- Brady, Hugo: *The EU and the fight against organised crime*. Centre for European Reform Working Paper, London, April 2007
- Brouwer, Evelien: *Data surveillance and border control in the EU: balancing efficiency and legal protection of third country nationals*. 14 June 2005 [disponible sur [www.libertysecurity.org](http://www.libertysecurity.org)]
- Bunyan, Tony: *The shape of things to come — EU Future Group*. September 2008 [disponible sur [www.statewatch.org](http://www.statewatch.org)]
- De Hert, Paul and Serge Gutwirth: *Interoperability of police databases within the EU: an accountable political choice?* TILT Law & Technology Working Paper No. 001/2006, 1 April 2006, Version 2.0 & Tilburg University Legal Studies Working Paper No. 003/2006
- Fijnaut, Cyrille and Letizia Paoli [eds.]: *Organised crime in Europe: Concepts, patterns and control policies in the European Union and beyond*. Dordrecht, 2004
- Geyer, Florian: *Taking stock: databases and systems of information exchange in the area of freedom, security and justice*. Challenge Research Paper No. 9, May 2008 [disponible sur [www.ceps.eu](http://www.ceps.eu)]
- Guild, Elspeth, Sergio Carrera and Thierry Balzacq: *The changing dynamics of security in an enlarged European Union*. Challenge Research Paper No. 12, October 2008 [disponible sur [www.ceps.eu](http://www.ceps.eu)]
- Hayes, Ben: *Schengen Information System Article 99 report: 33,541 people registered in SIS for surveillance and checks*. February 2008 [disponible sur [www.statewatch.org](http://www.statewatch.org)]
- Kierkegaard, Sylvia: “Explanatory Notes: From Prüm to the EU.” Presentation at the International Conference *Computers, Privacy and Data Protection*, Brussels, 16–17 January 2009
- Nelles, Ursula: “Steps towards harmonisation — steps towards friction.” In Kauko Aromaa and Sami Nevala (eds.): *Crime and crime control in an integrating Europe: Plenary presentations held at*

*the Third Annual Conference of the European Society of Criminology, Helsinki 2003*. European Institute for Crime Prevention and Control Publication Series No. 44, Helsinki 2004  
 — Schot, Johan and Arie Rip: “The past and future of Constructive Technology Assessment”. *Technological Forecasting and Social Change*, Vol. 54, 1996

## ANNEXE A

Situation au 18 décembre 2008

### Traité de Prüm (27 mai 2005)

Etat de la situation en termes de ratification/entrée en vigueur

Etats signataires			
	Dépôt du document de ratification		Entrée en vigueur
<b>AT</b>	<b>21/06/06</b>		<b>01/11/06</b>
<b>BE</b>	<b>05/02/07</b>		<b>06/05/07</b>
<b>DE</b>	<b>25/08/06</b>		<b>23/11/06</b>
<b>ES</b>	<b>03/08/06</b>		<b>01/11/06</b>
<b>FR</b>	<b>02/10/07</b>		<b>31/12/07</b>
<b>LU</b>	<b>08/02/07</b>		<b>09/05/07</b>
<b>NL</b>	<b>20/02/08</b>		<b>20/05/08</b>
Etats ayant adhéré par la suite			
	Déclaration d'adhésion	Dépôt du document de ratification	Entrée en vigueur
BG	02/02/07		
EL	05/01/07		
<b>EE</b>	-	<b>23/09/08</b>	<b>22/12/08</b>
<b>FI</b>	<b>21/06/06</b>	<b>19/03/07</b>	<b>17/06/07</b>
<b>HU</b>	<b>12/04/07</b>	<b>16/10/07</b>	<b>14/01/08</b>
IT	04/07/06		
PT	23/06/06		
<b>RO</b>	<b>23/01/07</b>	<b>03/12/08</b>	03/03/09
SE	18/01/07		
<b>SK</b>	28/03/07		
<b>SI</b>	<b>28/07/06</b>	<b>10/05/07</b>	<b>08/08/07</b>

Source: Auswärtiges Amt (Ministère allemand des Affaires étrangères)  
 [L'Allemagne est la dépositaire du traité]