Cultures & Conflits

74 | été 2009
Sécurité et protection des données

L'élargissement problématique de l'accès aux bases de données européennes en matière de sécurité

The problematic enlargement of access to European databases in the field of security

Sylvia Preuss-Laussinotte

Édition électronique
URL : http://journals.openedition.org/conflits/17441
DOI : 10.4000/conflits.17441
ISSN : 1777-5345

Éditeur :
CCLS - Centre d'études sur les conflits lilberté et sécurité, L'Harmattan

Édition imprimée
Date de publication : 1 septembre 2009
Pagination : 81-90
ISBN : 978-2-296-09110-8
ISSN : 1157-996X

Référence électronique
Sylvia Preuss-Laussinotte, « L'élargissement problématique de l'accès aux bases de données européennes en matière de sécurité », *Cultures & Conflits* [En ligne], 74 | été 2009, mis en ligne le 28 octobre 2010, consulté le 19 avril 2019. URL : http://journals.openedition.org/conflits/17441 ; DOI : 10.4000/conflits.17441

L'élargissement problématique de l'accès aux bases de données européennes en matière de sécurité

Sylvia PREUSS-LAUSSINOTTE

Sylvia Preuss-Laussinotte est directrice du Master 2 Droit des NTIC et Société de l'information, CREDOF, Université Paris-Ouest – Nanterre / La Défense.

Alors qu'à l'origine, le Parlement européen souhaitait que soit créée une base européenne de sécurité unique – le « SIE » (Système d'information européen) –, le choix, soumis à l'aléa des évolutions européennes, a été au contraire celui de la mise en place progressive d'un grand nombre de fichiers : SIS, SIS II, Eurodac, VIS, ainsi que les fichiers liés à Europol et Eurojust (voir notre première partie). C'est désormais la Commission européenne qui souhaite une unification de ces bases de données, la première phase étant celle de leur interopérabilité, actuellement en cours, associée à la définition de l'accès aux données qui y figurent. Or, on s'aperçoit que partant d'une situation d'accès aux informations très limité à certaines autorités, les textes européens ont progressivement élargi ces possibilités d'accès à un grand nombre de personnes et d'institutions, ce qui peut être source d'inquiétude (voir notre seconde partie).

Présentation des bases de données européennes en matière de sécurité

Schengen

Système d'information Schengen (SIS). Premier grand fichier de police européen, moteur des autres fichiers de sécurité, le SIS a été créé par le titre IV de la Convention de 1990 portant application de l'accord de Schengen du 14 juin 1985 relatif à la suppression graduelle des contrôles aux frontières communes dite « Convention de Schengen de 1990 » (CAAS). A l'origine issu d'un simple accord intergouvernemental visant à « compenser » la libre circulation des personnes – et ayant abouti à délimiter « l'espace Schengen » –, le SIS constitue un instrument de sécurité essentiel depuis que les dispositions de

la CAAS ont été « ventilées » sous la désignation de « l'acquis de Schengen » dans le cadre des deux traités de l'Union européenne. Dans cette logique, le Système d'information sur les visas (VIS) est d'ailleurs désigné comme étant un « *développement de l'acquis de Schengen* ».

Selon les conclusions du Conseil européen de Laeken des 14 et 15 décembre 2001, et en particulier les points 17 (coopération entre services spécialisés dans la lutte contre le terrorisme) et 43 (Eurojust et coopération policière en ce qui concerne Europol), ainsi que le plan d'action du 21 septembre 2001 en matière de lutte contre le terrorisme, il a été estimé nécessaire de renforcer le SIS et d'améliorer ses capacités, mais aussi d'élargir l'accès à ses données, très strictement limité à l'origine, justifié par l'article 93 de la Convention de Schengen de 1990 : le SIS a pour objet de préserver l'ordre et la sécurité publics, y compris la sûreté de l'Etat, sur les territoires des Etats membres en utilisant des informations communiquées par le biais du SIS conformément aux dispositions de la Convention. L'élargissement de l'accès a été effectif en 2005, malgré de vives oppositions à celui-ci [1] : accès direct par les autorités judiciaires nationales dans le cadre des enquêtes et poursuites pénales (article 101 CAAS modifié), mais surtout accès d'Europol (article 101 bis ajouté) pouvant demander des informations complémentaires aux Etats signalants, et accès des membres nationaux d'Eurojust et de leurs assistants dans les mêmes conditions.

SIS II. Remplaçant le SIS, un nouveau Système d'information Schengen de deuxième génération, le « SIS II », a été conçu dans la perspective de l'élargissement de l'Union européenne pour tenir compte de nouvelles fonctions et pour y introduire la possibilité d'enregistrer des signalements biométriques. Par ailleurs, une évolution s'est progressivement dessinée, visant à modifier les objectifs du SIS pour les amplifier, afin qu'il ne soit plus un « simple » système d'information mais qu'il devienne aussi un système d'enquête. Selon le Conseil (v. Conclusions JAI 5-6 juin 2003 par ex.), le SIS II doit répondre à de plus larges exigences liées au maintien de l'ordre public dans un espace de libre circulation, et ne plus être seulement un instrument de compensation de la libre circulation des personnes.

Dans les faits, la « mise à niveau » présentée comme technique du SIS sert également de paravent à un glissement de ses objectifs : on passe de l'accompagnement de la liberté de circulation des personnes à la constitution d'une base de données de surveillance et d'enquête, à laquelle, progressivement, vont accéder de plus en plus de personnes et d'organismes (voir *infra* notre seconde partie).

1 . Décision 2005/211/JAI du Conseil du 24 février 2005 concernant l'attribution de certaines fonctions nouvelles au Système d'information Schengen, y compris dans le cadre de la lutte contre le terrorisme.

Eurodac

Eurodac a été créé pour accompagner la mise en œuvre du règlement Dublin II. Il s'agit du premier système intégrant des données biométriques mis en œuvre dans le cadre de l'Union européenne, la biométrie étant désormais prioritaire et devant intégrer l'ensemble des autres systèmes d'information dans le cadre de la sécurité. Le choix des empreintes digitales est lié à l'identification des personnes et, surtout, à la possibilité d'établir leur « identité exacte », dans un objectif de contrôle et de surveillance des étrangers. Eurodac a pour objectif de conserver les données biométriques sous forme d'empreintes digitales des demandeurs d'asile, mais également des étrangers entrés irrégulièrement ou en situation irrégulière dans un Etat. Pour ces derniers, la raison avancée de ce fichage est de permettre aux Etats de vérifier « *si un étranger se trouvant illégalement sur son territoire a présenté une demande d'asile dans un autre Etat membre* » [2].

Pour le moment, le système Eurodac ne fonctionne que pour les demandes d'asile, les étrangers devant donner leurs empreintes digitales lorsqu'ils déposent une telle demande, afin de vérifier qu'ils n'aient pas déjà déposé d'autres demandes dans des Etats membres de l'UE.

Dans le cadre d'Eurodac, les Etats sont tenus de respecter des obligations de sécurité liées à la question de l'accès au système : ils doivent contrôler l'entrée de l'installation (empêcher l'accès de toute personne non autorisée aux installations nationales), contrôler les données (empêcher qu'elles ne soient lues, copiées, modifiées ou effacées par des personnes non autorisées, contrôler leur enregistrement, empêcher toute lecture, copie, modification ou effacement lors du transport des données). En cas de défaillance, leur responsabilité peut être engagée.

Le Système d'information sur les visas (VIS)

Constituant officiellement un « *développement de l'acquis de Schengen* », le VIS est présenté comme devant être le plus grand fichier mondial de données en matière de visas. Le règlement du 9 juillet 2008 [3], faisant suite à la décision 2004/512/CE du 8 juin 2004 créant le VIS, définit l'ensemble de ses fonctionnalités, son objet ainsi que les responsabilités et les conditions d'accès et d'échange de données entre les Etats.

---

2 . 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, JOUE no L 316, 15 décembre 2000.

3 . Règlement (CE) n° 767/2008 du Parlement européen et du conseil du 9 juillet 2008 concernant le système d'information sur les visas (VIS) et l'échange de données entre les Etats membres sur les visas de court séjour (règlement VIS), JOUE L 218/60, 13 août 2008.

La finalité générale du VIS est l'amélioration de la politique commune de visas, la coopération consulaire et la consultation des autorités consulaires centrales chargées des visas en facilitant l'échange de données entre les Etats (article 2 Règlement), avec des objectifs vastes, puisqu'il s'agit de :

> « faciliter la procédure de demande de visa ; éviter que les critères de détermination de l'Etat membre responsable de l'examen de la demande ne soient contournés ; faciliter la lutte contre la fraude ; faciliter les contrôles aux points de passage aux frontières extérieures et sur le territoire des Etats membres ; aider à l'identification de toute personne qui ne remplit pas ou ne remplit plus les conditions d'entrée, de présence ou de séjour sur le territoire des Etats membres ; faciliter l'application du règlement [« Dublin II »] ; contribuer à la prévention des menaces pesant sur la sécurité intérieure de l'un des Etats membres ».

Le système fonctionne sur le modèle du SIS, avec un système central VIS – qui est géré à Strasbourg par la France, à l'instar du SIS central, un VIS central de secours étant installé en Autriche (article 27) – et des systèmes nationaux reliés à la partie centrale (article 28) : le VIS doit permettre aux Etats de traiter les données relatives aux demandes de visas, aux visas délivrés, refusés, annulés, retirés ou prorogés. Cette base de données étant la dernière en date, ses règles illustrent l'évolution en cours, celle d'un élargissement continu d'accès aux données.

Elargissement de l'accès aux données

Des bases de données européennes

Lorsqu'on analyse la façon dont l'Union européenne envisage l'accès à ces grandes banques de données, on s'aperçoit que, progressivement, et contrairement aux objectifs initiaux de protection et de définition très stricts, l'UE a considérablement élargi ces possibilités d'accès.

L'échange de données entre Etats membres : « le principe de disponibilité ». L'accès mutuel de l'ensemble des Etats européens à leurs bases de données nationales, notamment policières, est désormais mis en place – et l'a été très rapidement : tout d'abord au nom du principe de disponibilité, qui s'est concrétisé par une décision intégrant le traité de Prüm dans le cadre de l'Union européenne [4] – selon le même processus qui avait abouti à y intégrer Schengen.

4 . Décision 2008/615/JAI du Conseil du 23 juin 2008 relative à l'approfondissement de la coopération transfrontalière, notamment en vue de lutter contre le terrorisme et la criminalité transfrontalière, JOUE L 210/1, 6 août 2008.

Le principe de disponibilité est conçu comme un nouveau principe juridique important introduit dans le programme de La Haye selon lequel « *les informations nécessaires dans le cadre de la lutte contre la criminalité doivent pouvoir traverser sans entraves les frontières extérieures de l'UE* ». Selon le Contrôleur européen à la protection des données (CEPD), il s'agit d'un principe simple :

> « Les informations accessibles à certaines autorités dans un Etat membre doivent également être communiquées aux services équivalents des autres Etats membres. Ces informations doivent être échangées aussi rapidement et aussi facilement que possible entre les services des Etats membres et de préférence dans le cadre d'un accès en ligne [5]. »

Après avoir affirmé que l'échange des informations entre les Etats membres devait obéir au principe de disponibilité, selon lequel « *tout agent des services répressifs d'un Etat membre qui a besoin de certaines informations* […] *peut les obtenir d'un autre Etat membre* », il a été décidé d'intégrer « en substance » les dispositions du traité de Prüm dans le cadre juridique de l'Union européenne. La décision 2008/616/JAI met concrètement en œuvre cet objectif, en précisant notamment les éléments techniques nécessaires à l'interopérabilité – donc à l'échange des données entre Etats membres.

Les dispositions principales du traité de Prüm destinées à améliorer l'échange d'informations entre Etats sont donc intégrées, notamment la possibilité nouvelle, et très demandée, d'accorder aux Etats des droits d'accès mutuels à leurs fichiers automatisés d'analyse ADN (FNAEG pour la France), et à leurs systèmes d'identification dactyloscopique (FAED pour la France). Le système fonctionne dans un premier temps selon une réponse : concordance/non-concordance, avec possibilité en cas de concordance de demander des informations complémentaires : les Etats sont incités à créer et conserver des fichiers nationaux d'analyse ADN (article 2) et autorisent les Etats à accéder aux données ADN indexées (article 3), à effectuer des comparaisons (article 4). En cas de concordance, la transmission d'autres données personnelles est régie par le droit national. Il peut être demandé à un Etat de procéder à un prélèvement d'ADN et de transmettre le profil génétique (article 7). Il est clair que cet accès très élargi de chaque Etat aux banques de données biométriques des autres Etats membres s'inscrit dans le cadre de l'existence déjà effective d'accès très élargis, ouverts à d'autres organismes tels qu'Europol et Interpol.

---

5 . Avis CEPD sur la proposition de décision-cadre du Conseil relative à l'échange d'informations en vertu du principe de disponibilité (COM (2005) 490 final), JOUE n° C 116, 17 mai 2006.

L'accès d'organismes aux bases de données européennes : l'exemple d'Europol. Tout d'abord formellement interdit – en application de l'article 101 initial de la CCAS, puis autorisé par un nouvel article 101 bis de cette même convention – l'accès d'Europol à l'ensemble des bases de données européennes est désormais bien accepté. Cet accès a pourtant des conséquences indirectes rarement évoquées.

Europol, Office européen de police créé en 1995 et dont le siège est à La Haye, est une organisation intergouvernementale destinée à faciliter la coopération policière européenne. Europol est chargé de faciliter l'échange d'informations, de les analyser et de coordonner les opérations entre les Etats membres de l'Union européenne pour lutter contre la criminalité internationale, le terrorisme et l'immigration clandestine. Il regroupe les services de police et des douanes des Etats membres. Europol n'est toutefois pas à proprement parler une police européenne, car cet office ne dispose pas de pouvoirs coercitifs : les Etats membres n'ont pas souhaité superposer aux autorités nationales existantes un organe policier d'essence supranationale. Europol se limite donc à faciliter l'échange d'informations entre les autorités nationales compétentes. Pour remplir ses fonctions, Europol gère un système informatisé de recueil d'informations. Le système se compose de trois éléments : le système d'informations informatisé, les fichiers de travail et le système d'index.

Or, la Convention Europol prévoit la possibilité pour cet organisme de conclure des accords de coopération stratégique ou de coopération opérationnelle avec des pays tiers et des organisations internationales : « *Conformément à l'article 42, paragraphe 2, à l'article 10, paragraphe 4, et à l'article 18 de la Convention portant création d'un office européen de police (Convention Europol), Europol est habilité à établir et maintenir des relations avec les Etats et instances tiers* ». C'est le directeur d'Europol qui signe ces accords, sans avoir à en demander l'autorisation aux institutions européennes (il est intéressant de noter que les Etats-Unis ont demandé à bénéficier, après le 11 septembre 2001, d'une clause spéciale issue d'un acte de mars 1999 relatif aux accords passés par Europol avec des Etats tiers).

Actuellement, les accords signés directement par Europol (et simplement confirmés par des Décisions du Conseil qui en prend note) sont nombreux, étant précisé que seuls les accords de coopération opérationnelle permettent la transmission de données personnelles. On y trouve notamment un accord explicite d'échange de données personnelles entre Europol et les Etats-Unis, ainsi qu'Interpol, signifiant que ces échanges existent de longue date.

Accords de coopération opérationnelle avec des Etats non-membres de l'Union européenne :

Australie Canada Croatie Islande
Norvège Suisse

Etats-Unis :

Agreement between the USA and the European Police Office

Supplemental agreement between Europol and the USA on exchange of personal data and related information

Accords de coopération opérationnelle avec des organismes européens :

Eurojust

Accords de coopération opérationnelle avec des organisations internationales :

Interpol

Ces accords posent une question récurrente : très rapidement, le Parlement européen a estimé que le contrôle sur Europol était incomplet et a plaidé pour un renforcement de ce contrôle. Alex Türk, ex-président de l'autorité de contrôle Europol, a adopté la même position, et semblait alors assez pessimiste. Ainsi, à propos de l'accord conclu entre Europol et les Etats-Unis, après qu'Hubert Haenel ait indiqué :

> « Personne ne se rend vraiment compte des dysfonctionnements de l'Organisation européenne de police. »

Alex Türk a précisé :

> « Je ne me fais pas trop d'illusions sur le fond, car je pense que les Américains disposeront alors de toutes les informations qui sont dans les fichiers » [6].

On peut rapprocher cet accord conclu entre Europol et les Etats-Unis, dont peu ont eu connaissance, avec l'émoi suscité par l'accord UE–Etats-Unis

6 . Débat de la délégation à l'Union européenne du 4 décembre 2002 sur le projet d'accord avec les Etats-Unis. http://www.senat.fr/ue/pac/E2141.html

sur le transfert des données PNR/API, qui peut faire sourire au regard de cette situation d'échange déjà ancienne. On notera que l'annulation de l'accord par la Cour de justice des Communautés européennes (CJCE) a abouti à un nouvel accord autorisant officiellement un nombre considérable d'agences américaines de sécurité à accéder aux données passagers – et non plus uniquement l'Office des douanes. Il est vrai que ce texte met fin à un certain artifice juridique, l'Office des douanes américain échangeant ses données avec ces agences de sécurités depuis longtemps déjà.

Outre ces accords d'échange de données avec des pays tiers et des institutions internationales telles qu'Interpol, Europol accède désormais officiellement aux données du SIS et du VIS. Lorsqu'on met bout à bout ces éléments, on peut dès lors s'interroger sur la transmission à l'extérieur de l'UE des informations figurant dans ces bases de données.

L'accès aux bases de données européennes par des pays tiers à l'UE. L'accès de pays tiers aux données contenues dans les bases de sécurité européennes peut inquiéter : si l'on se réfère aux accords et accès dans le cadre d'Europol, en quelque sorte, « c'est déjà chose faite ».

Nous voudrions ici nous pencher sur les raisons de l'inquiétude que suscitent ces derniers textes concernant cette fois le VIS, publiés à l'été 2008. Deux textes liés à la mise en œuvre du VIS ont été publiés, un règlement et une décision : globalement, ces textes définissent l'objet du VIS et les autorités pouvant y accéder (règlement v. note 2) et autorisent les autorités nationales chargées de la sécurité intérieure et les agents d'Europol à consulter les données du VIS (décision v. note 3).

Accès aux données du VIS par de nombreuses autorités

Globalement, on constate qu'un nombre très important de personnes ont accès aux données du VIS selon leur champ de compétence (article 15 à 22 du Règlement v. note 2) :

- autorités compétentes chargées des visas – le personnel des ambassades et des consulats – aux fins de l'examen des demandes, avec accès au dossier de demande en cas de présence d'une donnée recherchée (article 15) ;

- autorités centrales chargées des visas pour les demandes de consultation, avec saisine du VIS central, qui transmet la demande aux Etats concernés (article 16) ; elles peuvent consulter un ensemble de données pour établir des statistiques, sans identification du demandeur (article 17) ;

- autorités chargées des contrôles aux points de passage aux frontières pour vérifier l'identité du titulaire de visa, recherches effectuées avec le numéro de la vignette visa en combinaison avec les empreintes digitales (article 18) ; en cas de doute sur l'identité du titulaire du visa ou l'authenticité de celui-ci, le personnel pourra consulter l'ensemble des données (article 20) ;

- autorités chargées du contrôle sur le territoire (article 19), pour vérifier l'identité du titulaire, l'authenticité du visa ou si les conditions d'entrée/de séjour sont remplies : même règle que ci-dessus (article 20) ;

- autorités compétentes en matière d'asile : elles sont autorisées à effectuer des recherches à l'aide des empreintes digitales pour deux motifs (article 21) : dans le seul but de déterminer l'Etat responsable de l'examen de la demande d'asile (Dublin II) ; dans le seul but d'examiner une demande d'asile : la procédure est la même.

A ces autorités viennent s'ajouter les autorités nationales compétentes en matière de sécurité intérieure qui sont énumérées à l'article 5 de la décision du 23 juin 2008, et qui peuvent accéder aux données du VIS en consultation. La même décision prévoit expressément l'accès d'Europol en consultation « *dans les limites de ses missions* » [7].

Un nouveau motif d'inquiétude : l'accès aux données par des pays tiers à l'UE

L'article 31 du Règlement autorise la communication de données du VIS :

- à des organisations internationales citées en annexe : « *organisations des Nations unies (comme le Haut Commissariat pour les réfugiés), l'organisation internationale pour les migrations et le comité international de la Croix-Rouge* » ;

- mais surtout communication à des pays tiers à l'UE « *si cela s'avère nécessaire, dans des cas individuels, aux fins de prouver l'identité de ressortissants de pays tiers y compris aux fins de retour* » : on rapprochera cette possibilité de communication à un pays tiers dans le cas de renvoi d'étrangers dans leur pays d'origine avec l'arrêt de la Cour européenne des Droits de l'Homme (CEDH) NA c. Royaume-Uni [8] : la Cour européenne, qui constate la violation par le Royaume-Uni de l'article 3 (interdiction de la torture et des traitements inhumains ou dégradants) en cas de renvoi de demandeurs d'asile

7 . Décision 2008/633/JAI du Conseil du 23 juin 2008 concernant l'accès en consultation au système d'information sur les visas (VIS) par les autorités désignées des Etats membres et par l'Office européen de police (Europol) aux fins de la prévention et de la détection des infractions terroristes et des autres infractions pénales graves, ainsi qu'aux fins des enquêtes en la matière, JOUE L 218/129, 13 août 2008.

8 . CEDH 17 juillet 2008, requête n° 25904/07, NA c. Royaume-Uni.

Tamouls déboutés vers le Sri Lanka, s'inquiète de la situation de tous les demandeurs d'asile déboutés. La Cour constate de manière générale que les demandeurs d'asile peuvent être identifiés comme tels par leur pays d'origine lorsqu'ils y sont renvoyés, notamment grâce aux éléments biométriques, et que cette identification peut avoir de graves conséquences (« *irréparables* ») pour ces personnes, surtout lorsque les Etats d'origine disposent de moyens d'identification. Or, il est expressément prévu par le règlement que l'identité des personnes renvoyées soit communiquée à leur pays d'origine, avec les éléments d'identification.

Les précautions prises pour ces communications semblent inadaptées pour assurer une réelle protection : n'est en effet visée dans le texte que la protection des données personnelles, et absolument pas la question liée à la sécurité physique des personnes, même s'il est précisé que « *ces transferts de données à des pays tiers ou à des organisations internationales n'affectent par le droit des réfugiés et des personnes sollicitant une protection internationale, notamment en ce qui concerne leur non-refoulement* » [9], hypothèse différente de celle du renvoi de demandeurs d'asile dont la demande a été rejetée, qui est celle de l'arrêt NA c. Royaume-Uni.

Conclusion

Force est de constater que le mouvement général d'amplification des données contenues dans ces grandes bases européennes (notamment avec l'introduction d'éléments biométriques) et l'accès de plus en plus important d'autorités et d'institutions à ces données – selon le modèle américain – peut susciter des inquiétudes. La protection prévue semble peu adaptée ou incertaine, que ce soit sur le plan de la stricte sécurité technique ou de la fiabilité des personnes y ayant accès. La possibilité de permettre à des Etats tiers un tel accès – il est vrai déjà largement en vigueur dans le cadre d'Europol – laisse perplexe. La Cour européenne des Droits de l'Homme a sans doute envoyé un message d'alerte aux Etats européens – on espère qu'il sera entendu.

9 . Article 31, Règlement (CE) n° 767/2008 du Parlement Européen et du Conseil du 9 juillet 2008 concernant le système d'information sur les visas (VIS) et l'échange de données entre les États membres sur les visas de court séjour (règlement VIS), JOUE L 218/60, 13 août 2008.