www.jusletter.ch

Dr. Michele Albertini

La protection des données et Schengen

Une vision de l'expérience suisse

Depuis le 9 avril 2013, le système d'information Schengen de deuxième génération (SIS II) est en fonction. Les dispositions de la Convention de Schengen réglant la précédente version technique du SIS sont remplacées par un nouveau cadre juridique. Cette évolution est l'occasion de faire le point, dans la perspective suisse de la protection des données, sur la mise en œuvre de l'acquis ainsi que sur le rôle et les expériences des autorités de surveillance chargées d'exercer un contrôle indépendant du SIS et de vérifier que le traitement et l'utilisation des données y intégrées ne sont pas attentatoires aux droits de la personne concernée.

Domaine(s) juridique(s) : Droit européen ; Accords bilatéraux CH-UE ; Contributions

Proposition de citation : Michele Albertini, La protection des données et Schengen, in : Jusletter 6 mai 2013

ISSN 1424-7410, www.jusletter.ch, Weblaw AG, info@weblaw.ch, T +41 31 380 57 77 Editions Weblaw

Table des matières

1. La Suisse dans l'espace Schengen

1.1. L'accord d'association à Schengen et la Suisse

[Rz 1] Le 14 juin 1985, la République fédérale d'Allemagne, la France, la Belgique, le Luxembourg et les Pays-Bas ont signé un accord relatif à la suppression graduelle des contrôles aux frontières communes (Accord de Schengen[1]), qui était la première étape de la création du soi-disant *espace Schengen*, du nom du village luxembourgeois, tripoint frontalier entre le Luxembourg, l'Allemagne et la France. Signée le 19 juin 1990 et applicable depuis le 26 mars 1995, la *Convention de Schengen* (CAAS[2]) complète l'accord et définit les conditions d'application et les garanties de mise en oeuvre de la libre circulation. L'Accord et la Convention de Schengen, ainsi que les accords connexes progressivement adoptés, forment *« l'acquis de Schengen » (ou « accords de Schengen »)*, qui est intégré dans le cadre institutionnel et juridique de l'Union européenne (UE)[3]. Depuis 1990 nombre d'Etats européens y ont successivement et progressivement adhéré. Par la coopération Schengen, un espace qui repose sur les principes de liberté, de démocratie, d'Etat de droit et de respect des droits de l'homme, tels que garantis en particulier par la Convention européenne des droits de l'homme (CEDH[4]), a été constitué. Les accords de Schengen contiennent ainsi des règles qui visent à protéger la vie privée et la personnalité des personnes concernées, en couvrant donc, entre autres domaines, celui de la protection des données.

[Rz 2] Dans le cadre des accords bilatéraux II (seconde série) de 2004, la Suisse a négocié avec l'Union européenne sa participation à Schengen et à Dublin : le 26 octobre 2004, elle a signé l'Accord d'association de la Confédération suisse à la mise en oeuvre, à l'application et au développement de l'acquis de Schengen (AAS[5]), accord qui a été accepté par le peuple le 5 juin 2005, en approuvant un référendum par 54.6% des voix[6]. Ratifié le 20 mars 2006, l'accord est formellement entré en vigueur pour la Suisse le 1er mars 2008[7].

1.2. L'évaluation de la Suisse en 2008 et les recommandations de l'Union européenne

[Rz 3] Avec l'entrée en vigueur de l'Accord AAS, l'évaluation de la Suisse a été entamée, comme prescrit par les conditions de participation au système (art. 14 et 15 AAS). Au cours de cette procédure, qui s'est déroulée sur plusieurs mois, des équipes d'experts, composées de représentants des Etats membres de Schengen, de la Commission européenne et du Conseil de l'Union européenne, ont vérifié que la Suisse applique correctement les dispositions de Schengen aux différents domaines touchés, comme la sécurisation des frontières extérieures (aéroports), la coopération policière, ainsi que l'octroi des visas et le Système d'Information Schengen (SIS).

[Rz 4] Le domaine de la protection des données a, lui aussi, été examiné. L'évaluation avait pour objectif, en particulier, de vérifier si la législation nationale spécifique avait été adaptée aux dispositions de Schengen et comment les données SIS seraient, à l'avenir, protégées et les citoyens informés de leurs droits en matière de protection des données. En mars 2008, l'équipe d'experts a évalué les autorités de surveillance et de contrôle de la Confédération, ainsi que de quatre cantons (Vaud, Fribourg, Tessin et Zurich).

---

1 Accord entre les Gouvernements des Etats de l'Union économique Benelux, de la République fédérale d'Allemagne et de la République française relatif à la suppression graduelle des contrôles aux frontières communes, signé à Schengen le 14 juin 1985 (JO L 239 du 22 septembre 2000, p. 13).

2 Convention d'application de l'Accord de Schengen du 14 juin 1985 entre les Gouvernements des Etats de l'Union économique Benelux, de la République fédérale d'Allemagne et de la République française relatif à la suppression graduelle des contrôles aux frontières communes (JO L 239 du 22 septembre 2000, p. 19).

3 Décision 1999/435/CE du Conseil du 20 mai 1999 relative à la définition de l'acquis de Schengen en vue de déterminer, conformément aux dispositions pertinentes du traité instituant la Communauté européenne et du traité sur l'Union européenne, la base juridique de chacune des dispositions ou décisions qui constituent l'acquis (JO L 176 du 10 juillet 1999, p. 1).

4 Convention européenne des droits de l'homme de sauvegarde des droits de l'homme et des libertés fondamentales du 4 novembre 1950 (RS 0.101).

5 Accord entre la Confédération suisse, l'Union européenne et la Communauté européenne sur l'association de la Confédération suisse à la mise en oeuvre, à l'application et au développement de l'acquis de Schengen, approuvé par l'Assemblée fédérale le 17 décembre 2004 (RS 0.362.31).

6 FF 2005 4891.

7 RO 2008 447, 481.

[Rz 5] Les rapports d'évaluation établis par les experts à l'issue de leurs visites en Suisse ont été discutés au Conseil de l'UE et, ensuite, approuvés au niveau ministériel. En juin 2008, l'UE a estimé que, globalement, les exigences en matière de protection des données découlant de la coopération Schengen étaient remplies par la Suisse ; elle a toutefois adressé quelques recommandations. Celles-ci concernaient notamment l'indépendance des autorités de protection des données, la coopération entre elles, leurs ressources, leurs activités de contrôle ainsi que la formation et la sensibilisation des utilisateurs du SIS et l'information aux citoyens.

[Rz 6] L'évaluation positive dans tous les domaines a été la prémisse de la décision du Conseil de l'UE concernant l'entrée en vigueur opérationnelle de l'acquis de Schengen en Suisse. Par cette décision, le Conseil de l'UE a fixé la date de l'accès de la Suisse au SIS, ainsi que celle de la suppression des contrôles systématiques des personnes aux frontières intérieures. La participation opérationnelle de Schengen en Suisse a donc débuté le 12 décembre 2008, à minuit. La levée des contrôles systématiques des vols internes à l'espace Schengen dans les aéroports a, quant à elle, débuté le 29 mars 2009. À partir de ces dates, la Suisse est pleinement associée à Schengen en tant qu'Etat tiers, avec la Norvège, l'Islande et le Liechtenstein.

1.3. Les effets de l'entrée de la Suisse dans l'espace Schengen

[Rz 7] L'Accord de Schengen abolit les contrôles systématiques des passeports aux frontières communes des Etats participants. Il facilite ainsi les voyages entre la Suisse et les Etats Schengen, le passage des frontières et les séjours de courte durée jusqu'à trois mois (visa Schengen, art. 5 CAAS). Parallèlement, une série de mesures de sécurité a été destinée à compenser l'abolition des frontières intérieures, en rendant plus efficace la lutte contre la criminalité. Ces instruments se concentrent sur une meilleure collaboration internationale dans les domaines de la justice et de la police, sur le renforcement des contrôles opérés aux frontières extérieures de Schengen et sur l'adoption de mesures nationales de remplacement (contrôles mobiles des personnes dans la zone frontière ou à l'intérieur du pays[8]). Ces mesures sont complétées par l'accès, fondamental, au SIS, qui constitue l'élément central de la coopération.

[Rz 8] Parallèlement, l'UE a élaboré des règles de protection des données visant à protéger la vie privée et la personnalité des personnes concernées, qui sont d'autant plus touchées du fait que les mesures et les instruments de coopération et d'harmonisation sont très évolués et performants, comme c'est en particulier le cas pour le SIS. Pour atteindre ces objectifs, la Suisse a dû mettre en oeuvre les accords du point de vue *juridique*, en adoptant ou édictant des lois touchant aussi à la protection des données, ainsi que du point de vue *technique*, en procédant notamment à l'installation technique du SIS.

[Rz 9] Au centre de nos prochaines réflexions dans la perspective de la protection des données figureront la mise en oeuvre de l'acquis et les effets de l'introduction du SIS, ainsi que le rôle et les expériences des autorités suisses de protection des données. Ces dernières sont appelées à vérifier, notamment, que le traitement et l'utilisation des données intégrées dans cette base de données ne sont pas attentatoires aux droits des personnes concernées.

2. La mise en oeuvre de Schengen dans le droit suisse de protection des données

2.1. Mise en oeuvre, application et développement de l'acquis

[Rz 10] Dans la mesure où elles s'appliquent aux Etats membres, les dispositions de l'acquis de Schengen énumérées dans l'Accord AAS[9], ainsi que les dispositions des actes de l'Union européenne et de la Communauté européenne énumérées qui ont remplacé et/ou développé les dispositions correspondantes de la CAAS[10], doivent être mises en oeuvre, c'est-à-dire transposées en droit national, par la voie législative, et appliquées par la Suisse (art. 1, 2 et 15 AAS).

[Rz 11] La coopération entre l'UE et la Suisse ne concerne pas seulement la reprise, la mise en oeuvre et l'application pratique de l'acquis de Schengen lors de son entrée en vigueur pour la Suisse en 2008, mais aussi son *développement ultérieur*. En effet, les accords d'association sont conçus de manière à permettre l'adaptation de la coopération à des menaces et aux besoins actuels, qui sont en constante mutation, et donc à permettre l'élaboration de nouveaux standards de coopération policière en Europe. Si les actes juridiques ou les mesures notifiées impliquent des droits ou des devoirs (normalement, suite à des échanges de notes), ils constituent, du point de vue de la Suisse, des traités internationaux dont l'approbation est de la compétence du Conseil fédéral, du Parlement fédéral (notamment lorsque l'acte

[8] En outre, il demeurera possible d'introduire temporairement des contrôles systématiques aux frontières intérieures en cas de grandes manifestations ou de menace particulière.

[9] Accord AAS, annexe A : Accord de Schengen de 1985 et CAAS (avec exceptions), instruments d'adhésion (avec exceptions), ainsi que les actes Schengen secondaires pertinents (décisions et déclarations du Comité exécutif et du Groupe central).

[10] Accord AAS, annexe B : directives, règlements et décisions divers, dont la Directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (JO L 281 du 23 novembre 1995, p. 31).

en question contient des dispositions importantes qui fixent des règles de droit) et, dans certains cas, aussi du peuple, conformément aux dispositions constitutionnelles en la matière. Le cas échéant, les cantons doivent également mettre en oeuvre des développements de l'acquis.

[Rz 12] La reprise du droit communautaire est le résultat final d'une série de processus assez complexes. Les accords de Schengen ne prévoient pas à ce sujet un droit formel de codécision, mais un ample droit de participation, dont la Suisse tire parti : un *comité mixte* – composé des représentants du Gouvernement suisse, des membres du Conseil de l'UE et de la Commission des Communautés européennes, qui se réunit au niveau des ministres, des hauts fonctionnaires ou des experts, selon les besoins (art. 3 AAS) – a été institué, afin d'associer la Suisse aux activités de l'UE dans les domaines couverts par l'acquis de Schengen et de permettre sa participation. Au sein du comité mixte réuni au niveau ministériel, les représentants de la Suisse ont la possibilité d'exposer les problèmes que leur pose une mesure ou un acte particulier ou d'apporter une réponse aux problèmes rencontrés par les autres délégations, et de s'exprimer sur toute question portant sur l'élaboration de dispositions les concernant ou sur leur mise en oeuvre (art. 4 par. 2 AAS). La Commission ou un Etat membre peut, après discussion, examiner ces suggestions en vue de formuler une proposition ou de prendre une initiative, conformément aux règles de l'UE, aux fins de l'adoption d'un acte ou d'une mesure de la Communauté européenne ou de l'Union européenne (art. 4 par. 4 AAS). Lorsque les compétences ou des intérêts essentiels des cantons sont engagés, la Suisse est aussi représentée par des délégués des autorités cantonales. Dans ce cadre, la Confédération et les cantons ont donc la possibilité de participer à la définition de la teneur des actes juridiques destinés à être repris dans le droit suisse, la prise de décision formelle y relative étant réservée aux institutions compétentes de l'UE (art. 7 par. 1 AAS).

[Rz 13] Pour régler les droits et les obligations mutuels de la *Confédération* et des *cantons* dans la mise en oeuvre, l'application et le développement de nouveaux actes ou mesures de l'UE (conformément à l'art. 7 AAS) notifiés à la Suisse, la Confédération et les cantons ont conclu le 20 mars 2009 une convention spécifique[11] fondée sur l'article 1 al. 2 de l'arrêté fédéral portant approbation et mise en oeuvre des accords bilatéraux d'association à l'Espace Schengen et à l'Espace Dublin du 17 décembre 2004[12]. La convention règle en particulier la transmission d'informations entre la Confédération et les cantons dans le champ d'application de l'Accord AAS, la représentation et la participation des cantons dans les comités mixtes et les groupes de travail de l'UE et l'élaboration de positions communes des délégations suisses dans les comités mixtes. Cette convention stipule explicitement que dans les domaines couverts par l'acquis de Schengen, la Confédération et les cantons coopèrent étroitement et de manière concertée dans les limites de leurs compétences et que les cantons participent en particulier au développement, à l'application et à la mise en oeuvre de l'acquis de Schengen, qu'ils s'informent mutuellement, de manière complète et suffisamment tôt, de leurs projets d'actes normatifs dans les domaines couverts par l'AAS, qu'ils échangent également des informations sur la jurisprudence dans ces domaines et qu'ils coordonnent la mise en oeuvre des actes et des mesures dans les domaines couverts par l'AAS. Pour ce faire, la Confédération et les cantons désignent chacun un organe de liaison. Dans les domaines qui affectent leurs compétences ou leurs intérêts essentiels, les cantons prennent part à l'élaboration des positions de la Suisse dans les comités mixtes et les groupes de travail de l'UE et ils délèguent des représentants dans les groupes de travail de la Confédération qui effectuent les travaux préparatoires ou les analyses en vue des négociations au sein des comités mixtes et des groupes de travail de l'Union. À ce propos, la Conférence des gouvernements cantonaux a institué, dans le cadre de l'organisation d'accompagnement à Schengen/Dublin (OASD), entre autre, un groupe de travail horizontal et un groupe de travail Protection des données, dont font aussi partie des représentants des autorités de surveillance et de contrôle en matière de protection des données des cantons. Enfin, conformément à l'article 9 par. 1 AAS, la Confédération et les cantons présentent aux comités mixtes un rapport sur la manière dont les autorités administratives et les tribunaux ont interprété et appliqué les dispositions de l'acquis.

[Rz 14] L'adhésion de la Suisse à Schengen connaît donc des effets sur le plan juridique national, dans la mesure où la conformité du cadre juridique national doit être vérifiée par rapport aux exigences établies par l'acquis et adaptée en conséquence, comme il a été fait notamment pour certains aspects de protection des données. La mise en oeuvre et les développements de l'accord imposent au niveau national deux types d'intervention : la *modification* du droit existant et la *création* du nouveau droit, tant au niveau fédéral que cantonal. Finalement, la collectivité concernée (Confédération et/ou cantons) à laquelle s'adresse l'obligation de mise en oeuvre, est choisie en fonction de la répartition des compétences dans le domaine considéré.

2.2. Droit spécial fédéral

[Rz 15] Les principales adaptations du droit suisse concernent le droit spécial fédéral. Tout d'abord, l'adoption de l'arrêté fédéral portant approbation et mise en oeuvre des accords bilatéraux d'association à l'Espace Schengen et à l'Espace Dublin du 17 décembre 2004, par lequel a été approuvé entre

[11] Convention entre la Confédération et les cantons relative à la mise en oeuvre, à l'application et au développement de l'acquis de Schengen et de Dublin (RS 362.1), approuvée pour le Canton du Tessin par son Grand Conseil (législatif) le 23 septembre 2008 (RL 1.2.3.4).

[12] RS 362.

autres l'Accord AAS, a conduit à des *modifications de lois spéciales*[13]. Des nouvelles sections concernant la protection des données dans le cadre des accords d'association à Schengen ont été introduites dans différentes lois.

[Rz 16] Du point de vue organisationnel il a fallu notamment transposer dans le droit suisse les dispositions de la Convention CAAS pour l'introduction du SIS. Ainsi, l'art. 108 CAAS oblige chaque Etat membre à désigner une instance qui a la compétence centrale pour la partie nationale du SIS (c'est-à-dire, le système de données national, qui est relié au SIS central) et est donc responsable de son bon fonctionnement ; elle prend également les mesures propres à assurer le respect des dispositions de la Convention. Cette instance est appelée *« Bureau SIRENE »* (acronyme pour **S***upplementary* **Information Re**quest at the **N**ational **E**ntry; **S***upplément d'***Information R**equis à l'**E**ntrée **N**ational**E**). Les dispositions nécessaires ont été insérées dans le Code pénal suisse (CP[14]). L'art. 355e CP constitue le fondement juridique qui confère à l'Office fédéral de la police (fedpol) la compétence de gérer un service centralisé (bureau SIRENE Switzerland) responsable du N-SIS, appelé à être l'autorité de contact, de coordination et de consultation pour l'échange d'informations en relation avec les signalements figurant dans le SIS. Ce service est aussi compétent pour le contrôle de l'admissibilité formelle des signalements nationaux et étrangers dans le SIS.

[Rz 17] Au début, les bases légales formelles pour la partie nationale du SIS étaient intégrées dans le Code pénal[15], mais par la suite, elles ont fait l'objet d'une nouvelle loi spécifique. Le 13 juin 2008 a en effet été promulguée la loi fédérale sur les systèmes d'information de police de la Confédération (LSIP[16]), qui constitue dorénavant le fondement juridique suisse pour le traitement des données concernant les signalements internationaux au sens des articles 95 à 100 CAAS (art. 16 al. 1 LSIP). L'ordonnance sur la partie nationale du SIS et sur le bureau SIRENE (Ordonnance N-SIS[17]) règle et clarifie les principes en la matière, notamment la responsabilité du N-SIS, l'architecture du système informatique et du système de gestion des affaires et des dossiers du bureau SIRENE, les droits d'accès et les compétences des autorités concernant le N-SIS, l'organisation et les tâches du bureau SIRENE, l'échange des informations supplémentaires par le bureau SIRENE, les procédures, les conditions, les mesures et l'apposition d'indicateurs de validité sur les signalements de personnes et d'objets dans le N-SIS, le traitement et la durée de conservation des données, les droits des personnes concernées, la sécurité des données, le rôle des conseillers à la protection des données et la surveillance du traitement de données (art. 1 al. 1 lit. a-h de l'ordonnance N-SIS). On verra ci-après cette base de données et sa grande importance dans le contexte de l'acquis de Schengen dans son ensemble.

[Rz 18] De nombreux exemples montrent la vitalité du domaine de la coopération opérationnelle entre la Suisse et les autres Etats Schengen, attestée d'ailleurs par le nombre de développements (qui, à l'heure actuelle, dépassent déjà les cent trente), parfois contestés (comme cela a été notamment le cas pour l'introduction des passeports biométriques, essentiellement pour des raisons de protection des données[18]).

[Rz 19] À ce sujet, un développement très important de l'acquis de Schengen concerne la reprise de la décision-cadre 2008/977/JAI du Conseil du 27 novembre 2008 relative à la protection des données à caractère personnel traitées dans le cadre de la coopération policière et judiciaire en matière pénale[19]. L'arrêté fédéral du 19 mars 2010 portant approbation et mise en oeuvre de l'échange de notes entre la Suisse et l'Union européenne concernant la reprise de ladite décision-cadre[20] et la loi fédérale du même jour y

[13] RO 2008 447, RO 2008 447,

[14] RS 311.0.

[15] Sauf celles qui règlent la responsabilité des dommages découlant de l'exploitation du SIS, qui étaient introduites – et y figurent encore – dans la loi fédérale sur la responsabilité de la Confédération, des membres de ses autorités et de ses fonctionnaires du 14 mars 1958 (RS 170.32).

[16] RS 361.

[17] RS 362.0. Une nouvelle version du 8 mars 2013 (entrée en vigueur : 9 avril 2013) a remplacé la précédente du 7 mai 2008 sans apporter des changements significatifs.

[18] En effet, la reprise du Règlement (CE) n. 2252/2004 du Conseil du 13 décembre 2004 établissant des normes pour les éléments de sécurité et les éléments biométriques intégrés dans les passeports et les documents de voyage délivrés par les Etats membres (JO L 385 du 29 décembre 2004, p. 1) avait suscité des discussions animées. L'arrêté fédéral du 13 juin 2008 portant approbation et mise en oeuvre de l'échange de notes entre la Suisse et l'UE concernant ledit règlement avait été objet de référendum. La population avait finalement accepté l'objet le 17 mai 2009, mais seulement par 50.1% des voix! L'introduction de données biométriques enregistrées électroniquement dans le passeport suisse et dans les documents de voyage des personnes étrangères a été critiquée en particulier à cause du fait qu'elle prévoyait l'enregistrement de données biométriques des citoyens dans une banque de données centrale (ce qui poserait en plus des problèmes de sécurité des données) et l'introduction d'une carte d'identité biométrique, alors que les accords de Schengen ne les prévoyait pas. Le fait qu'il n'était pas possible de savoir exactement quand et où les données de la puce RFID seraient lues, ni ce qu'il en adviendrait après lecture, a aussi été critiqué. Les nouvelles dispositions sont entrées en vigueur le 1er octobre 2011 (RO 2009 5521). Pour la petite histoire, en tenant partiellement compte des critiques, le Conseil fédéral avait renoncé à introduire une carte d'identité biométrique, mais il a entretemps décidé que le passeport suisse et la carte d'identité devront être renouvelés d'ici fin 2016. Pour ce qui est de la carte d'identité, les citoyens pourront opter pour une carte sans puce électronique ou choisir entre trois modèles, tous munis d'une puce, à savoir une carte comportant des données enregistrées électroniquement (communiqué de presse du 16 décembre 2011).

[19] JO L 350 du 30 décembre 2008, p. 60. Dans les propos de la Commission européenne, cette décision-cadre est destinée à être remplacée par une directive dans le contexte de la révision, actuellement en cours, du cadre européen relatif à la protection des données, adapté aux défis du XXI siècle.

[20] RO 2010 3417.

relative (entrée en vigueur le 1er décembre 2010[21]), mettent en oeuvre l'acte normatif européen, dans la mesure où la législation suisse ne remplit pas entièrement les exigences concernant la conservation de données personnelles dans l'intérêt de la personne concernée, les conditions applicables en cas de transfert de données reçues d'un Etat Schengen à des tiers[22], le devoir d'informer la personne concernée de toute collecte de données la concernant et l'indépendance de l'autorité de contrôle. Cela étant le cas, la mise en oeuvre a impliqué la modification de plusieurs lois fédérales en relation à certains aspects de la protection des données :

- la nouvelle loi sur l'échange d'informations entre les autorités de poursuite pénale de la Confédération et celles des autres Etats Schengen du 12 juin 2009 (LEIS[23]) précise maintenant que le traitement des informations au sens de la loi est régi par les dispositions fédérales et cantonales en matière de protection des données (art. 2 al. 3 LEIS) ;
- de nouvelles dispositions concernant la coopération judiciaire dans le cadre des accords d'association à Schengen en matière de communication de données personnelles à un Etat tiers, à un organisme international et à une personne physique ou morale ont été introduites dans le Code pénal (art. 355f et 355g CP) ;
- des dispositions de nature sectorielle concernant le devoir d'information prévues dans la loi sur les étrangers (LEtr)[24], dans celle sur l'asile (LASi)[25], ainsi que dans celles sur les armes (LArm)[26] et sur les stupéfiants (LStup)[27] ont été abrogées et substituées de manière générale dans le cadre de loi fédérale sur la protection des données (LPD[28]), lorsque l'autorité compétente est un organe fédéral[29]. Il a en autre été précisé que le droit d'accès de la personne concernée est régi par les dispositions fédérales ou cantonales de protection des données, compte tenu de l'autonomie des cantons à légiférer dans cette matière ;
- des modifications touchent, enfin, à la LPD, *lex generalis* en la matière, dont l'on verra les plus importantes ci-dessous.

2.3. Droit général fédéral et cantonal

[Rz 20] Pour ce qui est du droit général fédéral de protection des données, la révision de la LPD entrée en vigueur le 1er décembre 2010, qui met en oeuvre les exigences de la décision-cadre 2008/977/JAI, entérine en particulier un *renforcement des pouvoirs et de l'indépendance* du préposé fédéral à la protection des données et à la transparence (PFPDT) en tant qu'autorité de surveillance et contrôle. Cette réforme tient également compte des recommandations de l'UE lors de l'évaluation de la Suisse selon lesquelles l'indépendance du Préposé fédéral devait être renforcée. Les nouvelles dispositions concernent en particulier sa nomination (par le Conseil fédéral, mais soumise à l'approbation de l'Assemblée fédérale, pour une période de quatre ans reconduite tacitement, à moins que le Conseil fédéral décide de ne pas la renouveler pour des motifs objectifs suffisants) et son statut (fonctions exercées de manière indépendante et sans recevoir d'instructions de la part d'une autorité ; rattachement administratif à la Chancellerie fédérale).

[Rz 21] Du point de vue matériel, il est intéressant de relever que le législateur fédéral a profité de la procédure de reprise pour introduire dans la LPD (art. 14 de la version actuellement en vigueur) un devoir d'information prévu dans la décision-cadre (à l'art. 16 par. 1), qui constitue un principe général de protection des données qui n'est pas spécifique à la coopération instaurée par Schengen. Le législateur a notamment retenu qu'une transposition de cette norme à l'ensemble des traitements effectués par les organes fédéraux indépendamment du domaine concerné permet d'éviter des lacunes par rapport au principe d'information, en raison du fait qu'il n'est pas toujours possible de déterminer lors d'une collecte de données si celles-ci seront ensuite transmises à l'étranger dans le cadre de la coopération policière ou judiciaire instaurée par Schengen. Il a aussi considéré nécessaire de généraliser l'obligation des organes fédéraux de conservation des données pour protéger un intérêt digne de protection de la personne concernée. Le législateur fédéral a donc conclu qu'il ne fallait pas circonscrire cette obligation aux seules données personnelles échangées dans le cadre de la coopération instaurée par Schengen.

[Rz 22] En ce qui concerne le droit général cantonal de protection des données, depuis l'association de la Suisse aux accords de Schengen, chaque canton dispose obligatoirement d'un acte normatif formel et d'une autorité cantonale

---

21 RO 2010 3387.

22 La décision-cadre a un champ d'application limité, dans le sens qu'elle doit s'appliquer uniquement aux communications transfrontières de données, effectuées dans le cadre de la coopération instaurée par Schengen. Les Etats Schengen restent toutefois libres de l'appliquer également à leurs traitements nationaux.

23 Dite aussi loi sur l'échange d'informations Schengen (RS 362.2), qui transpose la 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 L 386 du 29 décembre 2006, p. 89). À l'exception de la transmission spontanée d'informations au sens de l'article 7 LEIS, la loi ne crée pas de nouveaux droits en matière de traitement ; l'échange d'informations continue d'avoir lieu selon les dispositions du droit national : tel est le cas si une loi spéciale et un accord prévoient la communication de données à l'étranger à des fins de prévention ou de poursuite d'infractions.

24 Loi du 16 décembre 2005 (RS 142.20).

25 Loi du 26 juin 1998 (RS 142.31).

26 Loi du 20 juin 1997 (RS 514.54).

27 Loi du 3 octobre 1951(RS 812.121).

28 RS 235.1.

29 cf. ci-après.

de contrôle et surveillance au sens de la CAAS[30]. Certes, de grandes différences entre les cantons du point de vue de l'extension territoriale, de la population et de la force financière, ne permettent pas d'avoir une pleine harmonisation des législations. La situation s'est tout de même améliorée du point de vue normatif : les lois générales déjà existantes ont été adaptées suite à l'entrée en vigueur des accords, pour garantir l'effectivité des droits des citoyens (moyens de recours) et pour régler la transmission des données à l'étranger. Ceci a été par exemple le cas pour le canton du Tessin, qui a renforcé, par modification de sa loi sur la protection des données[31], le statut, l'indépendance, la fonction et les compétences du préposé cantonal à la protection des données et a introduit ou amélioré des dispositions concernant les droits de contrôle du citoyen et la communication des données à l'étranger. En revanche, la reprise de la décision-cadre 2008/977/JAI n'a pas eu d'effets significatifs au niveau normatif cantonal. Le droit tessinois en matière de protection des données ne contient pas non plus de références explicites au SIS et aux tâches de contrôle, qui trouvent en revanche un fondement juridique dans le droit fédéral (notamment dans l'ordonnance N-SIS).

3. La Suisse et le Système d'Information Schengen (SIS)

[Rz 23] L'un des développements les plus importants de l'acquis de Schengen, dont la reprise a nécessité l'aval du Parlement, concerne le Système d'information Schengen[32] : comme nous le verrons, le reliement au SIS et son utilisation présupposent une prise en considération accrue des dispositions en matière de protection des données.

3.1. La base de données SIS

[Rz 24] Le SIS est une base de données informatique commune, qui relie entre eux les Etats participants aux accords de Schengen et qui porte sur le maintien de la sécurité publique, sur l'appui à la coopération policière et judiciaire et sur la gestion des contrôles aux frontières extérieures. Entre les formes de coopération transfrontalière, comme les contacts directs et les échanges d'informations entre forces de police selon des procédures standardisées (dorénavant possibles avec les Etats pour lesquels la Suisse n'a pas passé d'accord bilatéral de coopération policière), le SIS constitue un outil essentiel, voire l'élément central pour l'application des dispositions de l'acquis de Schengen et donc pour la coopération en matière de maintien de la sécurité publique, pour l'appui à la coopération policière et judiciaire et pour la gestion des contrôles aux frontières extérieures.

[Rz 25] Ces constats fondamentaux sont valables tant pour le SIS de première génération, créé conformément aux dispositions du titre IV de la Convention CAAS, que pour son développement ultérieur, le SIS 1+[33], et, dès le 9 avril 2013, le Système d'information Schengen de deuxième génération, SIS II[34], qui est désormais régi par des bases légales nouvelles (notamment le règlement 1987/2006 du 20 décembre 2006[35] et la décision 2007/533/JAI du 12 juin 2007[36]). Dans cette contribution, qui regarde forcément en arrière, nous retiendrons uniquement l'ancien droit, applicable donc au SIS I, déterminant pour les statistiques et les expériences en le matière traitées ci-dessous.

[Rz 26] S'articulant autour d'une base de données centrale, gérée à Strasbourg, à laquelle sont rattachés des systèmes nationaux (N-SIS, SIS nationaux), le SIS permet aux autorités compétentes (en particulier aux autorités judiciaires, de police et douanières), grâce à une procédure d'interrogation automatisée, de disposer en temps réel des informations introduites dans le système par l'un des Etats membres, ceci notamment à l'occasion de contrôles de frontière et de vérifications et autres contrôles de police et de douanes exercés à l'intérieur du pays (art. 92 CAAS). Ces informations se réfèrent en particulier aux catégories répertoriées dans les articles 95 à 100 CAAS, qui peuvent concerner des *personnes* ou des *objets*, et précisément :

- art. 95 CAAS : arrestation de personnes ou, si une arrestation n'est pas possible, recherche de leur lieu de séjour aux fins d'enquête pénale, d'exécution d'une peine ou d'une mesure ou encore d'extradition *(arrestation aux fins d'extradition)* ;
- art. 96 CAAS : prononcé et contrôle d'interdictions

[30] La ratification du Protocole additionnel du 8 novembre 2001 (STE n. 179) du Conseil de l'Europe à la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (Convention STE n. 108), concernant les autorités de contrôle et les flux transfrontières de données (approuvé par l'Assemblée fédérale le 24 mars 2006 et entré en vigueur pour la Suisse le 1er avril 2008 ; RS 235.11), a aussi imposé une modification du cadre normatif cantonal.

[31] Legge sulla protezione dei dati personali del 9 marzo 1987 (LPDP ; RL 1.6.1.1) ; modification du 23 juin 2008, en vigueur depuis le 1er octobre 2008 (BU 2008 549).

[32] Article 2 par. 2 AAS, annexe B.

[33] Avec extension aux nouveaux Etats membres selon la solution transitoire appelée *SISone4all* (qui est le clone du N-SIS portugais ; cf. doc. 13540/06 SIS-TECH 101 COMIX 799 du 12 octobre 2006).

[34] Décision 2013/158/UE du Conseil du 7 mars 2013 fixant la date d'application du règlement (CE) n. 1987/2006 du Parlement européen et du Conseil sur l'établissement, le fonctionnement et l'utilisation du système d'information Schengen de deuxième génération (SIS II) (JO L 87 du 27 mars 2013, p. 10). La mise en service du SIS II intervient avec sept ans de retard en raison de difficultés techniques.

[35] Règlement 1987/2006 du Parlement européen et du Conseil du 20 décembre 2006 sur l'établissement, le fonctionnement et l'utilisation du système d'information Schengen de deuxième génération (SIS II) (JO L 381 du 28 décembre 2006, p. 4).

[36] Décision 2007/533/JAI du Conseil du 12 juin 2007 sur l'établissement, le fonctionnement et l'utilisation du système d'information Schengen de deuxième génération SIS II (JO L 205 du 7 août 2007, p. 63).

et de restrictions d'entrée à l'encontre de personnes non ressortissantes d'un Etat lié par l'un des accords d'association à Schengen *(interdictions d'entrée)* ;

- art. 97 CAAS : recherche du lieu de séjour de personnes (adultes et mineurs) disparues *(personnes disparues)* ;
- art. 98 CAAS : internement et mise en détention de personnes afin d'assurer leur propre protection ou de faire appliquer des mesures tutélaires, des mesures privatives de liberté ou des mesures visant à prévenir les risques pour la sécurité publique ainsi que la recherche du domicile ou du lieu de séjour de témoins, de prévenus, d'inculpés ou de condamnés, dans le cadre ou au terme d'une procédure pénale *(personnes participant à une procédure pénale)* ;
- art. 99 CAAS : surveillance discrète ou contrôle ciblé de personnes et de véhicules en vue de poursuivre une infraction pénale ou de prévenir les risques pour la sécurité publique *(surveillances discrètes)* ;
- art. 100 CAAS : recherche de véhicules et d'objets aux fins de saisie ou de sauvegarde de preuves dans une procédure pénale (p. ex. armes à feu, faux billets et documents d'identité) perdus ou volés *(objets)*.

[Rz 27] Comme l'explique l'art. 93 CAAS, le but du SIS est la préservation de l'ordre et de la sécurité publics – y compris la sûreté de l'Etat – et l'application des dispositions sur la circulation des personnes de la Convention CAAS sur les territoires des Parties contractantes à l'aide des informations transmises par ce système. Dans cette base de données informatique, fondée sur le système de recherche *hit/no hit* (« trouvé/non trouvé »), les différents services de sécurité autorisés peuvent, selon les droits qui leur sont attribués, consulter des informations (effectuer des *requêtes*) ou enregistrer des informations (effectuer des *signalements*) concernant personnes et objets.

[Rz 28] Les données personnelles pouvant y figurer sont clairement définies à l'art. 94 CAAS : la base de données contient notamment l'identité de la personne, ses caractéristiques physiques particulières, le motif de son signalement et les mesures à prendre à son encontre (p. ex. arrestation ou déclaration) et la précision selon laquelle la personne concernée est armée ou violente. Les dispositions applicables indiquent les conditions auxquelles une personne (p. ex. un étranger signalé aux fins de non-admission) peut être signalée dans la base de données (p. ex. parce que cet étranger a commis une infraction passible d'une peine privative de liberté d'au moins un an, comme le trafic de drogue ou l'assassinat ; art. 96 par. 2 lit. a CAAS).

[Rz 29] L'importance pour la Suisse de cette base de données très puissante – à laquelle elle a accès depuis le 14 août 2008 – est donc certaine, ce qui l'amène à garantir le bon fonctionnement du SIS national, condition indispensable pour que la Suisse puisse être pleinement intégrée à Schengen.

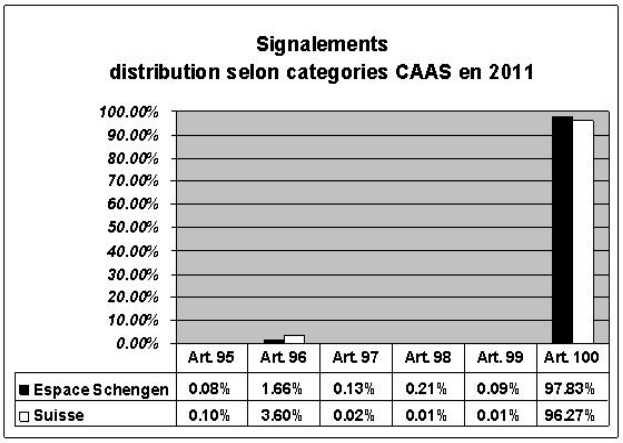
3.2. Le succès du SIS – quelques statistiques

[Rz 30] Aux yeux de la Suisse, mais pas seulement, le SIS, qui contient à l'heure actuelle plus de 42 millions d'enregistrements, a montré déjà dès les premiers mois d'utilisation qu'il est très performant et qu'il donne de bons résultats. Au niveau de l'espace Schengen, les requêtes qui aboutissent (dites *« hits »)*, dépassaient les 100'000 à fin 2011. Un regard plus précis sur quelques statistiques intéressantes corrobore ces considérations.

a. Signalements

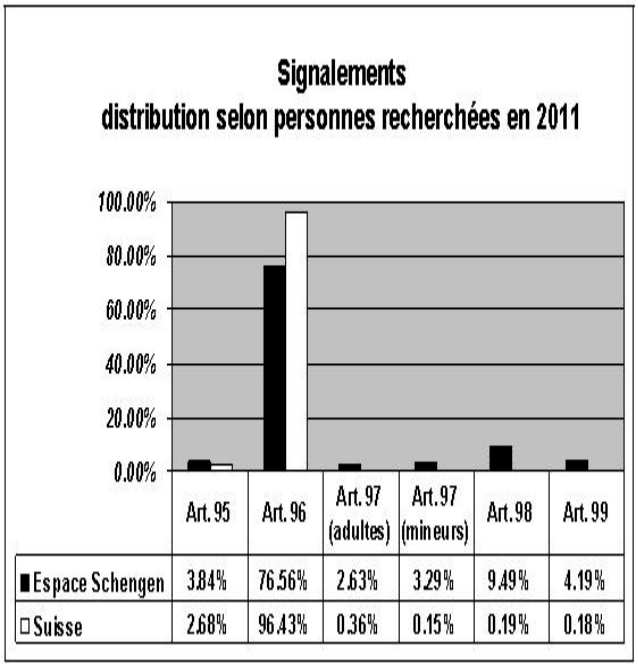
[Rz 31] Le *signalement (alert),* comme défini dans le droit suisse (art. 2 lit. a ordonnance N-SIS), est un bloc de données aux fins de non-admission ou de la recherche de personnes ou d'objets, qui doit être enregistré dans le SIS ou qui y figure déjà. Les objets tombant dans le champ d'application de l'article 100 CAAS (documents et véhicules) concernent à peu près 98% des 42'038'610 signalements de l'espace Schengen (fin 2011). Les signalements concernant des personnes recherchées se montaient à 904'355 (fin 2011), soit 2% du total, dont la très grande majorité (692'226 : 77%) de personnes ayant fait l'objet d'une mesure d'interdiction d'entrée au sens de l'article 96 CAAS.

[Rz 32] En comparaison, le pourcentage global des signalements en Suisse est comparable à celui de l'espace Schengen. Les signalements concernant les objets tombant sous le champ d'application de l'article 100 CAAS représentent 96% du total des signalements. Les 4% restants concernent les autres catégories (art. 95 à 99 CAAS). A leur tour, 96% de ces 4% de signalements restants touchent la catégorie des personnes recherchées en vertu de l'article 96 CAAS (comparés aux 77% de l'espace Schengen). Ce constat – concernant les recherches étrangères en Suisse et les recherches suisses à l'étranger de personnes signalées aux fins de non-admission (interdiction d'entrée) – n'est pas trop surprenant si l'on considère la situation particulière de la Suisse.



	Art. 95	Art. 96	Art. 97	Art. 98	Art. 99	Art. 100
■ Espace Schengen	0.08%	1.66%	0.13%	0.21%	0.09%	97.83%
□ Suisse	0.10%	3.60%	0.02%	0.01%	0.01%	96.27%

Tab. 1 – Source des données : 11970/12 SIRIS 56 COMIX 415 et SIRENE Switzerland Statistics 2011

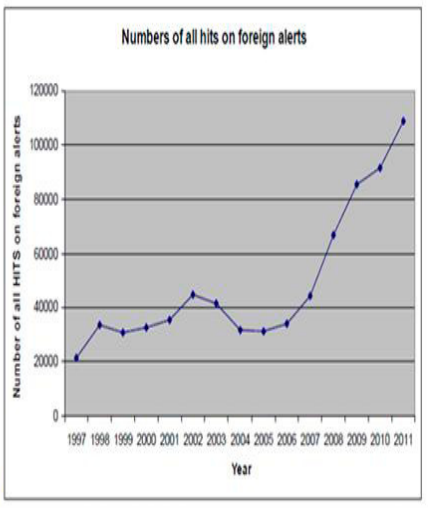


Tab. 2 – Source des données : doc. 11970/12 SIRIS 56 COMIX 415 et SIRENE Switzerland Statistics 2011

b. Hits

[Rz 33] Pour démontrer le succès du SIS, il est intéressant d'évaluer les statistiques des résultats positifs, c'est-à-dire les requêtes qui aboutissent. Au niveau de l'espace Schengen, les *hits* ont connu une évolution remarquable dans les dernières années : ils étaient 44'342 à fin 2007, alors que fin 2011 les *hits* atteignaient le nombre de 108'951, soit plus du double, ce qui coïncide avec une augmentation de 19% par rapport à fin 2010.

SIRENE Bureaux		
1997	21280	Evolution
1998	33551	158%
1999	30762	145%
2000	32566	153%
2001	35414	166%
2002	44877	211%
2003	41485	195%
2004	31749	149%
2005	31383	147%
2006	33930	159%
2007	44342	208%
2008	66961	315%
2009	85569	402%
2010	91351	429%
2011	108951	512%



Tab. 3 – Source : doc. 11970/12 SIRIS 56 COMIX 415

[Rz 34] Les statistiques suisses (effectuées à partir de 2009) montrent aussi des résultats dignes d'être relevés. Le nombre de requêtes qui aboutissent lors de recherches étrangères en Suisse se situe à 7'518 (fin 2011), voire à 9'791 au total (y compris les *hits* de recherches suisse à l'étranger ; + 11% par rapport à fin 2010). Certes, face à un total d'environ 260'000 recherches manuelles et automatiques en moyenne par jour, les résultats positifs pourraient sembler négligeables (0.01% du total des recherches) ; mais si l'on tient compte du fait que le SIS a permis, en 2011, l'aboutissement de 27 recherches en moyenne par jour, soit une augmentation de 13% par rapport à 2010 (24), la vision change, ce qui met en exergue l'efficacité substantielle du système. Par rapport à l'année précédente, on relève 19% de *hits* en plus pour les recherches étrangères en Suisse ; l'on constate en revanche une diminution de 4% de réponses positives à l'étranger liées à des signalements émis par la Suisse.

RÉPONSES POSITIVES DANS LE SYSTÈME D'INFORMATION SCHENGEN

Catégorie «recherches»	2011 CH	2011 Etranger	2010 CH	2010 Etranger	2009 CH	2009 Etranger
• Arrestation aux fins d'extradition[1]	185	107	216	95	199	112
• Interdictions d'entrée[2]	3 690	1 850	2 907	1 960	2 999	1 860
• Personnes disparues[3]	213	20	235	18	191	16
• Personnes recherchées par la justice[4] (par ex. témoins)	1 082	3	952	5	986	1
• Surveillances discrètes[5]	1 044	20	766	1	626	0
• Objets[6] (véhicules et documents d'identité)	1 304	273	1 246	286	1 476	166
Total	**7 518**	**2 273**	**6 322**	**2 365**	**6 477**	**2 155**

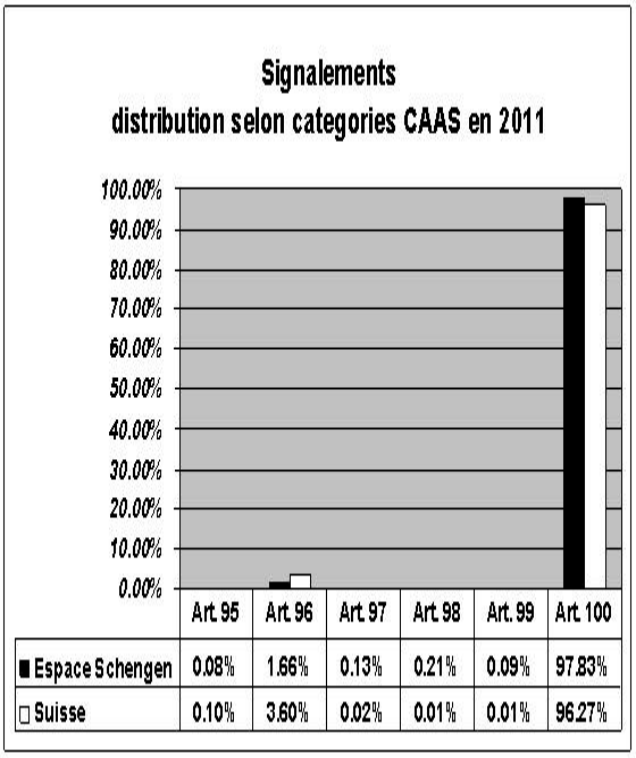
> [1]art. 95 CAAS, [2]art. 96 CAAS, [3]art. 97 CAAS, [4]art. 98 CAAS, [5]art. 99 CAAS, [6]art. 100 CAAS.

> CAAS: Convention d'application de l'accord de Schengen.

Tab. 4 – Source : Rapport annuel fedpol 2011

[Rz 35] Une comparaison entre les statistiques de l'espace Schengen et de la Suisse (recherches étrangères en Suisse

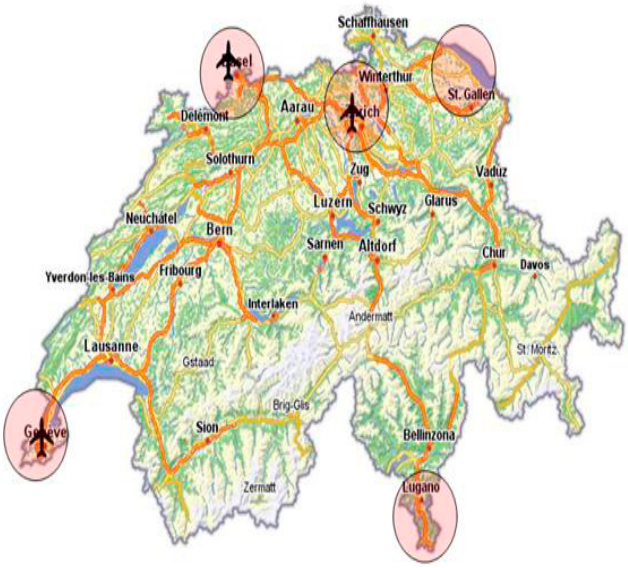
et recherches suisses à l'étranger additionnées) révèle que la plus grande différence concerne les étrangers qui sont signalés aux fins de non-admission (interdiction d'entrée) au sens de l'art. 96 CAAS. En Suisse, plus de la moitié des réponses positives globales (57%) a trait à cette catégorie, alors que ce pourcentage est clairement inférieur au niveau de l'espace Schengen (32% des *hits*). De plus, il est utile de constater que le pourcentage des réponses positives globales s'élève, toujours fin 2011 et toujours pour l'article 96 CAAS, à 81%, si l'on ne tient compte que des *hits* des recherches suisses à l'étranger.



	Art. 95	Art. 96	Art. 97	Art. 98	Art. 99	Art. 100
Espace Schengen	0.08%	1.66%	0.13%	0.21%	0.09%	97.83%
Suisse	0.10%	3.60%	0.02%	0.01%	0.01%	96.27%

Tab. 5 – Source des données : doc. 11970/12 SIRIS 56 COMIX 415 et Rapport annuel fedpol 2011

[Rz 36] Il est intéressant de constater qu'en Suisse, la répartition territoriale des réponses positives étrangères se concentre surtout dans les cantons frontaliers liés aux grands axes routiers et ferroviaires (Bâle-Ville, Genève, Tessin et Saint Gall), respectivement aux aéroports internationaux (Zurich, Bâle et Genève). Fin 2011, le canton de Zurich connaissait le nombre le plus élevé de *hits* (1713), devant Genève (872), Bâle-Ville (854) et le Tessin (606) ; le nombre le plus bas de *hits* (3) s'observe dans le demi-canton d'Appenzell Rhodes-Intérieures.



Tab. 6 – Source des données : SIRENE Switzerland Statistics 2011

3.3. Des contrepoids

[Rz 37] Les statistiques reportées attestent non seulement de l'utilité et de l'efficacité du Système d'information Schengen pour la préservation de l'ordre et de la sécurité publics, mais aussi de l'ampleur des traitements de données personnelles effectués. Ceci exige, en contrepoids, des mesures pour garantir le respect, notamment, des droits des personnes concernées en matière de traitement des données personnelles, donc de la *protection et de la sécurité des données*. Des dispositions spécifiques doivent donc éclaircir et préciser les catégories de données (signalements de personnes et d'objets) introduites dans le système, leurs conditions d'introduction, les critères et les procédures d'introduction et le traitement des différentes catégories de données, la durée de conservation et la sécurité des données, ainsi que les autorisations d'accès, les devoirs d'information, les droits de contrôle des personnes concernées et les responsabilités.

[Rz 38] A ce sujet, le chapitre 2 titre IV de la Convention CAAS prévoit, aux articles 92 à 101ter, des exigences légales strictes, précisées par des nombreuses dispositions d'exécution et instructions en matière d'utilisation du SIS (comme le manuel SIRENE[37]) ; de leur côté, les articles 102 à 118 du chapitre 3 du même titre régissent le traitement de données dans

[37] Le manuel SIRENE est un ensemble d'instructions destinées aux opérateurs des bureaux SIRENE, qui établit les règles et les procédures régissant l'échange bilatéral ou multilatéral des informations complémentaires indispensables pour mettre en oeuvre correctement certaines dispositions de la Convention CAAS (Décision d'exécution 2011/406/UE de la Commission du 1er juillet 2011 portant modification du manuel SIRENE ; JO 2011 L 186, p. 1).

ce cadre[38]. Ces dispositions impliquent leur mise en oeuvre dans le droit national.

[Rz 39] Des dispositions particulières sont consacrées à la *surveillance*, qui doit être régie par le droit national des Etats membres. Ces tâches sont confiées aux autorités nationales de protection des données.

4. Schengen et les autorités suisses de protection des données

4.1. Les autorités de surveillance et leurs compétences

[Rz 40] Pour garantir la surveillance du respect des dispositions de la Convention CAAS, chaque Etat membre doit désigner une autorité de contrôle chargée, dans le respect du droit national, d'exercer un contrôle indépendant du fichier de la partie nationale du SIS et de vérifier que le traitement et l'utilisation des données intégrées dans le système d'information ne sont pas attentatoires aux droits de la personne concernée (art. 114 par. 1 CAAS).

[Rz 41] L'ampleur et la sensibilité des traitements de données dans le cadre du SIS, compte tenu aussi du nombre important de signalements et de *hits*, exigent, en contrepoids, l'organisation de contrôles efficaces par des autorités indépendantes sur le respect des règles. Ces règles sont en effet strictes : les données pouvant être saisies et traitées dans le SIS sont clairement définies, de même que les finalités des traitements. De plus, seul un cercle restreint de personnes faisant partie de services fédéraux et cantonaux est autorisé à utiliser la partie nationale du SIS et exclusivement dans l'accomplissement des tâches prévues aux articles 95 à 100 CAAS ou pour annoncer des signalements en vue de leur enregistrement dans le N-SIS (art. 16 LSIP et 7 de l'ordonnance N-SIS)[39]. Toute utilisation du SIS fait systématiquement l'objet d'un enregistrement afin d'empêcher les abus et les données sont effacées lorsque le motif de signalement disparaît (quand leur but est atteint), de même qu'après un délai donné.

[Rz 42] En raison de la structure fédérale de la Suisse, les compétences de contrôle sont partagées entre la Confédération et les cantons. En Suisse, les activités de surveillance des traitements de données personnelles dans le SIS sont assurées par le Préposé fédéral à la protection des données et à la transparence (PFPDT) et par les autorités cantonales de protection des données (ACPD, qui disposent en général d'un préposé cantonal à la protection des données) : les deux entités sont appelées à collaborer activement dans le cadre de leurs compétences respectives (art. 55 de l'ordonnance N-SIS). Les compétences de l'autorité fédérale et des autorités cantonales se répartissent selon l'organe qui traite les données : ainsi, toutes les données personnelles dont le traitement est effectué par des organes fédéraux ou par des privés (personnes physiques et morales) sont soumises au contrôle du préposé fédéral (art. 2 al. 1, 27 al. 1 et 29 LPD, alors que toutes les données traitées par des autorités cantonales et communales sont soumises à la surveillance des autorités cantonales, selon les lois cantonales respectives sur la protection des données. Au surplus, l'article 55 al. 3 de l'ordonnance N-SIS précise que le PFPDT est l'interlocuteur national du Contrôleur européen de la protection des données.

[Rz 43] Concrètement, en matière Schengen, les autorités suisses de contrôle doivent, entre autre, veiller à garantir l'exercice effectif des droits des personnes concernées par des traitements de données personnelles. Pour ces raisons, elles ont élaboré et publié sur leurs sites web respectifs des informations générales concernant Schengen, le système SIS et les droits des personnes concernées par le traitement de leurs données personnelles dans ladite base de données, en expliquant la procédure et les modalités d'exercice des droits d'accès, de rectification et d'effacement des données au sens des articles 109 à 111 CAAS[40]. Selon l'article 114 par. 2 CAAS, toute personne a le droit de demander aux autorités de contrôle de vérifier les données la concernant intégrées dans le SIS ainsi que l'utilisation qui en est faite : la personne concernée a donc le droit de s'adresser à l'autorité de contrôle compétente (fédérale ou cantonale) pour qu'elle vérifie la conformité du traitement des données aux principes de protection des données ancrés dans la CAAS. Bien entendu, la personne concernée peut toujours exercer son droit d'accès (régi par l'article 7 LSIP, avec renvoi aux dispositions pertinentes de la LPD) directement auprès de fedpol (art. 50 de l'ordonnance N-SIS) ou de l'Office fédéral des migrations (pour les données traitées dans le SIS, art. 16 LSIP concernant les restrictions et les interdictions d'entrée qui relèvent de son domaine de compétence).

[Rz 44] L'article 55 al. 2 de l'ordonnance N-SIS dit que le PFPDT exerce en particulier la surveillance eu égard au traitement des données personnelles figurant dans le SIS. C'est lui qui exerce le contrôle indépendant du fichier du N-SIS auprès du maître du fichier, qui est un organe fédéral

[38] En revanche, les articles 126 à 130 CAAS, qui concernent aussi la protection des données, règlementent l'échange de données dans les domaines de coopération policière et judiciaire en matière pénale en dehors du SIS.

[39] En Suisse ont accès au SIS en particulier les autorités de police et de poursuite pénale, les autorités d'exécution des peines, le corps des gardes-frontière, les représentations suisses à l'étranger, les autorités compétentes en matière de migration et les offices cantonaux de circulation routière ; les droits des autorités en matière d'accès et de traitement des différentes données du SIS sont réglés de manière exhaustive dans une annexe de l'ordonnance N-SIS.

[40] Voir en particulier les sections dédiées des sites web de fedpol (www.fedpol.admin.ch), du PFPDT (www.leprepose.ch) et des préposés cantonaux à la protection des données (Canton du Tessin : (www.ti.ch/protezionedati).

(fedpol, auquel est rattaché le Bureau SIRENE Switzerland). Il vérifie aussi auprès des organes fédéraux compétents pour introduire et accéder aux données du SIS que le traitement et l'utilisation des données intégrées dans le N-SIS respectent l'article 114 par. 1 CAAS. Aux fins d'établir les faits, le PFPDT peut exiger la production de pièces, demander des renseignements et se faire présenter des traitements sur place (art. 27 al. 3 LPD). L'article 55 al. 2 de l'ordonnance N-SIS ne signifie pourtant pas que les compétences des ACPD cantonales soient absorbées par celles du PFPDT : en réalité, les autorités cantonales sont indépendantes quant à l'organisation et les modalités des inspections des utilisateurs finaux cantonaux et communaux du SIS de leurs juridictions et elles peuvent bien entendu demander directement à fedpol, en sa qualité d'autorité responsable, les logfiles que l'ACPD veut vérifier. Les autorités cantonales disposent de compétences et d'instruments juridiques analogues à l'article 27 al. 3 LPD en ce qui concerne les traitements de données du N-SIS opérés par des utilisateurs cantonaux autorisés par les articles 16 LEIS et 7 ordonnance N-SIS.

[Rz 45] L'examen des accès et l'analyse des logfiles du système SIS est un élément crucial des inspections. Les logfiles permettent en effet de garder une trace des différentes actions qui ont été menées dans un système par ses utilisateurs. Puisqu'elle informe sur l'identité de l'utilisateur, la date et l'heure de la recherche ainsi que les données introduites dans le masque de recherche, l'analyse de ces files permet de déterminer lors de contrôles si l'utilisation du système est correcte. Lorsqu'elle procède à un tel contrôle, l'autorité de surveillance demande à fedpol de pouvoir accéder aux logfiles du SIS. Elle précise dans ce but la liste des utilisateurs concernés ainsi qu'une intervalle de temps bien défini, déterminés de façon à ce que l'analyse ultérieure des logfiles reçus soit la plus pertinente possible. Les logfiles ainsi fournis permettent à l'autorité de contrôle de constater que les requêtes effectuées ont bien été journalisées. Une analyse plus détaillée – qui s'avère, dans la pratique, très onéreuse – lui permet de vérifier la plausibilité et la licéité des recherches effectuées par les utilisateurs. En cas de doute, elle procède à un contrôle plus approfondi en interrogeant directement l'utilisateur concerné sur les raisons qui l'ont poussé à faire la recherche suspecte. L'utilisateur est ainsi confronté aux informations qu'il a introduites dans le masque de recherche et doit se justifier. Les logfiles du système SIS sont conservés pendant une année. Ils sont ensuite détruits et les traces relatives à l'utilisation du système sont perdues.

4.2. Les contrôles coordonnés dans le cadre de Schengen

[Rz 46] Une première coordination de l'activité de surveillance a lieu à l'échelon international. L'article 115 CAAS institue l'*Autorité de contrôle commune Schengen (ACC/JSA)*, qui siège à Bruxelles. Cette autorité est chargée du contrôle de la fonction de support technique du SIS de première génération. Dans ce cadre, elle a pour mission de vérifier la bonne exécution des dispositions de la Convention CAAS. Elle est également compétente pour analyser les difficultés d'application ou d'interprétation pouvant survenir lors de l'exploitation du SIS, pour étudier les problèmes pouvant se poser lors de l'exercice du contrôle indépendant effectué par les autorités de contrôle nationales des Etats membres ou à l'occasion de l'exercice du droit d'accès au système ainsi que pour élaborer des propositions harmonisées en vue de trouver des solutions communes aux problèmes existants (art. 115 al. 2 et 3 CAAS). L'ACC se compose de deux représentants de chaque autorité nationale de contrôle. Ainsi, une délégation suisse qui représente la Confédération (le préposé fédéral) et les cantons (un préposé cantonal) participe régulièrement, en qualité de membre, aux séances et aux activités prévues. L'ACC décide parfois de déclencher des contrôles sollicitant des actions au niveau national. Les autorités suisses concernées sont alors appelées à exécuter un contrôle coordonné, comme cela a récemment été le cas, soulevé par la Suisse même, concernant la licéité, à la lumière de la CAAS, de la vérification systématique dans les SIS nationaux des clients séjournant dans des hôtels dans les Etats Schengen[41]. Dès la mise en fonction du SIS de nouvelle génération (SIS II), ce sera au Contrôleur européen à la protection des données (CEPD) de s'occuper de la mission de surveillance du SIS, remplaçant ainsi l'ACC. Il est prévu que le CEPD et les autorités de contrôle nationales, agissant chacun dans le cadre de leurs compétences respectives, assureront la surveillance conjointe du SIS II, conformément à l'article 46 du règlement n. 1987/2006 et à l'article 62 de la décision n. 2007/533/JAI.

[Rz 47] Une deuxième coordination a lieu au niveau national suisse dans le but d'assurer une surveillance efficace de la mise en oeuvre de Schengen en matière de protection des données. Ainsi, pour ce faire, l'article 55 de l'ordonnance N-SIS dit que les ACPD et le préposé fédéral veillent à exercer une surveillance coordonnée du traitement de données personnelles. En fait, en raison des différentes compétences constitutionnelles (accomplissement des tâches respectives), il peut arriver qu'un contrôle doive être effectué par les deux organes de surveillance (Confédération et cantons) ou en raison d'un conflit de compétence entre l'autorité fédérale et les autorités cantonales. Pour accomplir ces tâches de surveillance de manière efficace, il a été créé un *Groupe de coordination des autorités suisses de protection des données*. Présidé par le préposé fédéral et composé d'un représentant de chaque autorité de protection des données cantonale ainsi que d'un représentant du préposé fédéral, le

[41] Le préposé fédéral avait en effet demandé à l'ACC, conformément à l'article 115 par. 3 CAAS, de donner son avis sur le recours au SIS pour la vérification par recoupements à 100% des données avec les registres hôteliers nationaux. Cet avis est publié sur le site web de l'ACC (http://schengen.consilium.europa.eu).

groupe sert désormais de plateforme de coordination pour les activités de contrôle et d'information desdites autorités dans le domaine de la coopération Schengen et en particulier pour ce qui est de l'utilisation du SIS. Comme il ressort du règlement organique du 12 novembre 2009 à l'article 1 al. 2, dans le respect des compétences respectives de chacun de ses membres, le Groupe de coordination a les tâches suivantes :

- échanger les informations nécessaires à la surveillance effective des traitements de données personnelles contenues dans les banques de données de l'espace Schengen ;
- examiner les difficultés d'interprétation ou d'application des dispositions légales ;
- étudier les problèmes pouvant se poser lors d'activités de surveillance ou dans l'exercice des droits des personnes concernées ;
- formuler des propositions ou des avis harmonisés en vue de trouver des solutions communes ;
- soutenir et coordonner les activités de surveillance de chacun de ses membres.

[Rz 48] Du point de vue de la procédure, le groupe de coordination a élaboré un document définissant la coordination et la méthodologie des contrôles aux niveaux stratégique et opérationnel, qui décrit les différents rôles ainsi que les étapes et les procédures du contrôle coordonné.

4.3. Expériences suisses en matière de surveillance

[Rz 49] En ce qui concerne la surveillance, des inspections sont planifiées et mises en place auprès d'organes fédéraux et cantonaux traitant de données dans le cadre du SIS. Jusqu'à présent, cela a été le cas, au niveau fédéral, de l'Office fédéral de la police, des autorités douanières, de l'Office fédéral des migrations, des représentations diplomatiques suisses à l'étranger et, au niveau cantonal, faute de ressources suffisantes, les autorités de quelques cantons ont mis en place des contrôles seulement auprès des autorités de police et, dans une mesure encore plus faible, des autorités des migrations.

a. L'expérience de la Confédération

[Rz 50] Depuis 2008, le préposé fédéral a effectué différentes inspections, notamment auprès des ambassades suisses à l'étranger (Kiev, Le Caire, Istanbul, Moscou) et des autorités fédérales (Police judiciaire fédérale, Corps des gardes-frontière). Les recommandations émises et les propositions d'amélioration formulées concernaient principalement la formation spécifique du personnel appelé à utiliser le SIS, la sécurité technique des traitements de données personnelles, les contrats d'externalisation de prestations de traitements de données personnelles et l'effectivité des droits des personnes concernées par des traitements de données personnelles[42]. Mais en général le préposé fédéral n'a pas constaté des grands déficits.

[Rz 51] Parmi les constats intéressants, on peut remarquer l'utilisation du SIS à d'autres fins. Une personne en service avait effectué des recherches dans le N-SIS avec son propre nom de famille. Après une nouvelle analyse des logfiles du N-SIS concernant cette personne portant sur une période de sept mois, le PFPDT a constaté que celle-ci avait procédé à plusieurs reprises à des recherches dans le N-SIS avec son propre nom de famille. Le problème de l'accès au SIS à des fins non autorisées, qui a été constaté aussi par des autorités cantonales dans le cadre de leurs propres contrôles, est réel. Dans ces cas, il s'agissait d'utilisateurs qui faisaient des recherches lors de cours de formation. Ainsi, le Groupe de coordination des autorités suisses de protection des données a préparé un courrier visant à sensibiliser les utilisateurs au respect du cadre légal, notamment en ne recherchant pas dans le véritable N-SIS des signalements relatifs à des personnes de leur famille ou entourage ni à des personnalités connues : le respect des normes légales doit également être garanti lors de cours de formation, en utilisant par exemple la plateforme dédiée.

b. L'expérience d'un canton (Tessin)

[Rz 52] Le canton du Tessin est relativement petit avec ses quelques 340'000 habitants répartis dans des vallées de montagne et dans quatre agglomérations urbaines. Mais, étant un canton frontalier, il connaît tous les problèmes des régions (plus grandes) liées au transit des personnes et des marchandises, de sorte que les problèmes qui se posent au niveau national se retrouvent, en principe, à l'échelon cantonal. Les statistiques exposées ci-dessus en relation avec l'utilisation et l'efficacité du SIS corroborent ce constat et attestent l'importance de promouvoir des inspections chez les utilisateurs finaux des cantons.

[Rz 53] Au sujet des inspections, l'autorité de contrôle tessinoise a retenu comme tâche prioritaire de vérifier si l'attribution des accès au N-SIS aux utilisateurs individuels cantonaux était correcte. Ainsi le préposé a requis de fedpol la liste complète des accès individuels et l'a croisée avec la liste des collaborateurs, suivant la fonction et donc le profil, en se fondant sur les bases juridiques applicables. Il a pu constater que les autorités cantonales de police utilisent régulièrement le N-SIS par l'interface du système de recherches informatisées de police RIPOL, comme le prévoit l'article 4 al. 5 lit. a de l'ordonnance N-SIS. Les droits d'accès étaient attribués correctement, comme on a pu généralement le constater pour d'autres autorités légalement autorisées à accéder au N-SIS.

[42] Pour les détails des différentes inspections je renvoie aux rapports d'activité du PFPDT n. 16-19, 2008-2011, publiés sur le site web www.leprepose.ch.

Il a pu toutefois relever que des droits d'accès avaient été attribués à des unités, voire à des personnes qui n'y avaient pas droit, puisqu'elles ne figuraient pas dans les listes des autorités autorisées. En particulier, ces unités administratives ne savaient même pas qu'elles avaient accès au N-SIS. La raison était assez simple à identifier : ces utilisateurs avaient accès au système d'information central sur la migration SYMIC pour accomplir leur tâche légale de contrôle dans le cadre du marché du travail et en même temps ils accédaient automatiquement au N-SIS lors des recherches internationales. À l'instar de RIPOL, l'accès au N-SIS a lieu aussi par une interface, dans ce cas par SYMIC (art. 4 al. 5 lit. b de l'ordonnance N-SIS). Fedpol a corrigé la faute, prévoyant pour ces utilisateurs un profil d'accès au SYMIC sans accès automatique au N-SIS et donc vérifié, le cas échéant corrigé la même faute auprès des utilisateurs des cantons chargés de cette tâche. Les inspections ont donc permis à l'autorité de contrôle tessinoise de constater que l'accès au N-SIS par le biais d'une autre interface doit faire l'objet d'information et de sensibilisation accrues auprès des collaborateurs en tant qu'utilisateurs. Techniquement, on pourrait aussi envisager la possibilité de faire apparaître sur l'écran de l'ordinateur (éventuellement par le biais d'une fenêtre pop-up) une mention légale lors de l'accès au N-SIS via un autre masque. Le fait d'accéder automatiquement au SIS alors qu'un utilisateur a besoin seulement de consulter une base de données nationale pour accomplir sa tâche peut en effet se révéler non conforme au principe de la proportionnalité. Ce thème devrait être abordé de manière coordonnée *in primis* au niveau international, si le problème existe à ce niveau aussi.

5. Conclusions

[Rz 54] Du point de vue de la protection des données, la participation opérative de la Suisse aux accords de Schengen a bien eu des conséquences. L'adhésion au protocole additionnel à la Convention STE n. 108 du Conseil de l'Europe, entré en vigueur pour la Suisse le 1er avril 2008[43], l'exigence de garantir la cohérence et la compatibilité avec le cadre juridique de l'Union européenne en matière de protection des données pour pouvoir participer aux accords de Schengen ainsi que la reprise de la décision-cadre 2008/977/JAI ont entérinés des améliorations évidentes et une harmonisation, au moins partielle, des législations générales. On peut désormais compter, au niveau normatif suisse, sur un renforcement des pouvoirs et de l'indépendance des autorités de contrôle fédérale et cantonales et des instruments juridiques pour assurer une protection des données plus efficace.

[Rz 55] La mise en oeuvre de l'acquis et de ses développements, ainsi que la réforme en cours du cadre juridique de la protection des données au niveau de l'Union européenne[44] et du Conseil de l'Europe[45], prévoient un renforcement ultérieur de la protection des données et des moyens pour le réaliser, en augmentant encore plus les pouvoirs et les exigences en termes de compétences, indépendance et ressources des autorités de contrôle. Ces réformes et le nombre élevé des développements de l'acquis de Schengen doivent conduire à une prise de conscience de l'importance d'assurer une protection des données suffisante et efficace et à la nécessité de suivre de près cette évolution.

[Rz 56] Durant les quatre dernières années, les autorités suisses de protection des données, fédérale et de certains cantons, ont pu « tester » la mise en oeuvre de l'acquis de Schengen, et en particulier, sous différents aspects, la licéité des traitements des données, intégrés notamment dans la partie nationale du SIS, en tant qu'élément central de la coopération instaurée par l'acquis de Schengen. En général, les autorités de contrôle n'ont pas constaté de situations particulièrement délicates. Le personnel appelé à utiliser le SIS est conscient de sa mission, mais il faut tout de même améliorer la formation interne et définir clairement les rôles, ainsi que déterminer les personnes compétentes pour les contacts au sein de la justice, de la police et des départements de l'administration. De plus, il est intéressant de relever que la source potentielle de risques majeurs de violation de la protection des données consiste dans les traitements des données concernées par l'article 96 CAAS (non-admission) : c'est du moins ce que l'on peut déduire des statistiques de l'utilisation du SIS (nombre de signalements et réponses positives). Pour ce qui est du droit d'accès des particuliers aux données qui les concernent, les signaux n'indiquent pas qu'il soit très exercé ni que le sujet « Schengen », en général, réveille les passions des citoyens : en Suisse le nombre global de requêtes s'élevait en 2010 à seulement 319 (251 hits positifs, dont 121 résidents en Suisse) et en 2011 à 354 (268 hits positifs, dont 136 résidents en Suisse)[46]. Les citoyens ne

[43] Protocole additionnel du 8 novembre 2001 à la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel concernant les autorités de contrôle et les flux transfrontières de données (STE n. 179 ; RS 0.235.11).

[44] Proposition COM(2012)11 du 25 janvier 2012 de Règlement du Parlement européen et du Conseil relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (règlement général sur la protection des données, destiné a remplacer la directive 95/46/CE) et proposition COM(2012)10 du 25 janvier 2012 de Directive du Parlement européen et du Conseil relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données (destinée à remplacer la décision-cadre 2008/977/JAI).

[45] Comité consultatif de la Convention pour la protection des personnes a l'égard du traitement automatisé des données à caractère personnel (STE n. 108), document final sur la modernisation de la Convention 108, du 16 octobre 2012.

[46] Statistiques fournies par la Suisse en 2012 dans le cadre de l'enquête initiée par l'ACC/JSA Schengen auprès des Etats membres au sujet du droit

ressentent peut-être pas le besoin de l'exercer, parce qu'il n'y a pas de problèmes évidents, ou alors ils ignorent qu'ils disposent de droits. En définitive, l'expérience reste encore mineure. Dans tous le cas de figure, les autorités de contrôle sont appelées à améliorer encore la sensibilisation, bien que des informations pertinentes figurent depuis longtemps sur leur sites Internet et sur celui de fedpol, en tant qu'autorité responsable du traitement des données.

[Rz 57] Les résultats de la prochaine réforme du droit européen, l'entrée en vigueur en 2013 du nouveau cadre juridique pour le SIS II, qui remplace les articles 92 à 119 CAAS (sauf l'art. 102bis)[47], et la mise en exercice du SIS II même, avec ses fonctionnalités augmentées et améliorées[48], constitueront un banc d'essai important pour les autorités suisses de protection des données, surtout des petits cantons : malgré le fait qu'elles constituent des gouttes dans l'océan Schengen, ces autorités doivent garantir un contrôle efficace, et donc doivent disposer des ressources suffisantes, en adéquation avec les recommandations formulées par l'Union européenne à l'occasion de l'évaluation du droit suisse dans le domaine de la protection des données.

Sources officielles et documentation utile

- Bureau de l'intégration DFAE/DFE, Schengen/Dublin, brochure informative, juin 2012 http://www.europa.admin.ch
- Bureau de l'intégration DFAE/DFE, Schengen/Dublin : Développements – fiche d'information, octobre 2012 http://www.europa.admin.ch
- Office fédéral de la police fedpol, Rapport annuel 2011, juin 2012, http://www.fedpol.admin.ch
- Préposé fédéral à la protection des données et à la transparence PFPDT, Schengen et vos données personnelles – fiche d'information, février 2010, http://www.leprepose.ch
- Préposé fédéral à la protection des données et à la transparence PFPDT, Explications concernant les compétences de contrôle et activités du PFPDT dans le cadre de l'accord d'association à Schengen, 28 mai 2008, http://www.leprepose.ch
- Préposé fédéral à la protection des données et à la transparence PFPDT, Rapports d'activité 16-19, 2008-2011, http://www.leprepose.ch
- Council of the European Union, doc. 11970/12 SIRIS 36 COMIX 415 du 16 juillet 2012, SIS and SIRENE statistics http://www.statewatch.org

Michele Albertini, Dr. en droit, préposé à la protection des données du canton du Tessin, représentant suppléant de la Suisse pour les Cantons au sein de l'Autorité de contrôle commun Schengen, membre du Groupe de travail Protection des données de l'organisation d'accompagnement à Schengen/Dublin de la Conférence des Gouvernements cantonaux suisses. Ce texte constitue la version remaniée d'une conférence donnée dans le cadre de la réunion scientifique « El espacio de libertad, seguridad y justicia : Schengen y protección de datos », organisée le 3 octobre 2012 par l'Université du Pays Basque à Saint-Sébastien.

* * *

d'accès.

47 Article 52 du Règlement 1987/2006 et article 68 de la décision 2007/533/JAI.

48 Le SIS de nouvelle génération, système à grande échelle, propose une amélioration des fonctionnalités et des capacités : des données biométriques (empreintes digitales, photographies numériques) pourront désormais être saisies, des liens pourront être établis entre les signalements et les données seront accessibles aux autorités chargées de la sécurité intérieure, comme Europol, Eurojust et les offices de la circulation routière. Il est également prévu de relier le système d'information électronique sur les visas aux données sur les personnes recherchées du SIS II.