

MEMORIAL

Journal Officiel
du Grand-Duché de
Luxembourg



MEMORIAL

Amtsblatt
des Großherzogtums
Luxemburg

RECUEIL ADMINISTRATIF ET ECONOMIQUE

B — N° 50

15 décembre 1997

S o m m a i r e

PROTECTION DES DONNEES A CARACTERE PERSONNEL

Commission consultative prévue par l'article 30 de la loi modifiée du 31 mars 1979 réglementant l'utilisation des données nominatives dans les traitements informatiques – Nomination.....	page 946
Autorité de contrôle prévue par l'article 12-1 de la loi modifiée du 31 mars 1979 réglementant l'utilisation des données nominatives dans les traitements informatiques. – Nominations ..	946
Autorité de contrôle prévue par l'article 12-1 de la loi modifiée du 31 mars 1979 réglementant l'utilisation des données nominatives dans les traitements informatiques. – PREMIER RAPPORT RENDANT COMPTE DE L'EXECUTION DE SA MISSION PENDANT LA PERIODE DU 30 SEPTEMBRE 1993 AU 29 MARS 1996	947
Autorité de contrôle commune de Schengen. – RAPPORT D'ACTIVITE (mars 1995 à mars 1997)	958

Commission consultative instituée par la loi modifiée du 31 mars 1979 réglementant l'utilisation des données nominatives dans les traitements informatiques. - Nomination. - Par arrêté grand-ducal du 11 octobre 1997, Monsieur Jean-Paul *Reiter*, attaché auprès du Ministère de la Justice, a été nommé secrétaire de la commission consultative prévue à l'article 30 de la loi modifiée du 31 mars 1979 réglementant l'utilisation des données nominatives dans les traitements informatiques en remplacement de Monsieur Sylvain *Wagner*, conseiller de direction première classe auprès du Ministère de la Justice, démissionnaire, dont il termine le mandat.

Autorité de contrôle instituée par la loi modifiée du 31 mars 1979 réglementant l'utilisation des données nominatives dans les traitements informatiques. - Nominations. - Par arrêté grand-ducal du 11 octobre 1997, Monsieur Georges *Wivenes*, avocat général, a été nommé président de l'autorité de contrôle prévue à l'article 12-1 de la loi modifiée du 31 mars 1979 réglementant l'utilisation des données nominatives dans les traitements informatiques en remplacement de Monsieur Claude *Nicolay*, premier avocat général, démissionnaire, dont il termine le mandat.

Par le même arrêté grand-ducal, Monsieur Jean-Paul *Reiter*, attaché auprès du Ministère de la Justice, a été nommé secrétaire de l'autorité de contrôle prévue à l'article 12-1 de la loi modifiée du 31 mars 1979 réglementant l'utilisation des données nominatives dans les traitements informatiques en remplacement de Monsieur Sylvain *Wagner*, conseiller de direction première classe auprès du Ministère de la Justice, démissionnaire, dont il termine le mandat.

Autorité de contrôle instituée par l'article 12-1 (4) de la loi modifiée du 31 mars 1979 réglementant l'utilisation des données nominatives dans les traitements informatiques

***Premier rapport
rendant compte de l'exécution de sa mission
pendant la période du 30 septembre 1993 au 29 mars 1996***

SOMMAIRE

1. Introduction
 2. Composition de l'autorité de contrôle
 3. Bilan de l'autorité de contrôle
 4. Contrôles effectués
 5. Activités internationales
 6. Conclusion
- Annexe

1. Introduction

La loi du 9 août 1993 modifiant la loi modifiée du 31 mars 1979 réglementant l'utilisation des données nominatives dans les traitements informatiques a institué dans son article 12-1, paragraphe (4) une autorité de contrôle qui «est chargée de contrôler l'exploitation des banques de données [de police] constituées tant en application d'une disposition de droit interne qu'en application d'une convention internationale».

L'organisation et le fonctionnement de l'autorité de contrôle font l'objet du règlement grand-ducal du 9 août 1993.

La principale mission de l'autorité de contrôle est de veiller à ce que les traitements automatisés de données à caractère personnel effectués par les organes de la Gendarmerie et de la Police pour les besoins de la prévention, de la recherche, de la constatation et de la poursuite des infractions soient conformes aux dispositions légales qui les régissent.

Pour l'exercice de sa mission, l'autorité de contrôle:

- est informée immédiatement de la création d'une banque de données de police;
- a un accès direct aux banques de données visées;
- peut procéder, quant aux traitements effectués, à des vérifications sur place;
- peut se faire communiquer tous renseignements et documents utiles;
- peut charger ses membres à procéder à des missions de contrôle spécifique;
- fait opérer les rectifications et radiations nécessaires.

Par ailleurs, la loi a investi l'autorité de contrôle de la mission d'exercer, pour compte des personnes concernées, leur droit d'accès à des données traitées dans les banques de données de police (droit d'accès indirect). A cet effet, le paragraphe (5) de l'article 12-1 nouveau de la loi du 31 mars 1979 dispose que l'autorité de contrôle «procède aux vérifications et investigations utiles, fait opérer les rectifications nécessaires et informe l'intéressé que la banque ne contient aucune donnée contraire aux conventions, à la loi, à ses règlements d'exécution ou aux conditions imposées par le ministre».

Annuellement, l'autorité de contrôle présente au ministre ayant dans ses attributions le répertoire national des banques de données un rapport rendant compte de l'exécution de sa mission. Pour des raisons d'ordre matériel, liées au démarrage des travaux de l'autorité de contrôle, celle-ci n'a pas été en mesure de présenter son premier rapport à l'issue d'une année d'activités. Eu égard d'autre part au fait que la Convention d'application de l'Accord de Schengen n'a été définitivement mise en vigueur qu'en date du 26 mars 1995, l'autorité de contrôle a cru opportun et utile de retarder la publication de son premier rapport, afin de pouvoir y inclure ses expériences lors de la première année d'exploitation du SIS. Voilà pourquoi le présent rapport couvre une période de deux ans et demi, soit la moitié du premier mandat de l'autorité de contrôle.

Contrairement à ce que prévoit la loi pour le rapport rendant compte de l'exécution de la mission de la commission consultative instituée par l'article 30 de la loi du 31 mars 1979, elle ne précise pas que le présent rapport soit publié. Pour des raisons évidentes de transparence et d'indépendance, l'autorité de contrôle propose toutefois au ministre ayant dans ses attributions le répertoire national des banques de données, en l'occurrence le ministre de la Justice, d'inviter le gouvernement, après avoir pris connaissance du présent rapport, à décider de sa publication.

Dans cet ordre d'idées, l'autorité de contrôle aimerait évoquer l'article 3 du règlement grand-ducal du 9 août 1993 relatif à son organisation et à son fonctionnement qui dispose: «Les délibérations et propositions de l'autorité de contrôle sont transmises au ministre ayant dans ses attributions le répertoire national des banques de données».

De l'interprétation de l'autorité de contrôle, il ne peut s'agir de faire envoyer ses délibérations et propositions aux destinataires respectifs via le ministre compétent. Si cette procédure devait être d'application, elle mettrait largement en cause l'indépendance du contrôle voulu par le législateur. Par conséquent, l'objet de l'article 3 en question ne peut être compris que conférant au ministre de la Justice le droit d'être informé à tout moment des délibérations et propositions de l'autorité de contrôle. Cette information serait donc complémentaire à celle prévue par l'article 12-1, paragraphe (4), dernier alinéa de la loi du 31 mars 1979 qui prévoit, comme indiqué ci-dessus, que l'autorité de contrôle «présente chaque année au ministre ayant dans ses attributions le répertoire national des banques de données un rapport rendant compte de l'exécution de sa mission».

2. Composition de l'autorité de contrôle

Le paragraphe (4) de l'article 12-1 de la loi du 31 mars 1979, telle que modifiée par la loi du 9 août 1993, prévoit que l'autorité de contrôle est composée «du procureur général d'Etat ou d'un délégué de son parquet qui la préside, de deux membres choisis par le ministre ayant dans ses attributions le répertoire national des banques de données parmi les membres de la commission visée à l'article 30 et du secrétaire de cette commission».

La composition de l'autorité de contrôle a fait l'objet de l'arrêté grand-ducal du 29 septembre 1993 portant:

- nomination des membres de l'autorité de contrôle prévue au paragraphe (4) de l'article 12-1 de la loi modifiée du 31 mars 1979 réglementant l'utilisation des données nominatives dans les traitements informatiques;
- désignation des représentants à l'autorité de contrôle commune prévue à l'article 115 de la Convention d'application de l'Accord de Schengen.

Ont été nommés membres de l'autorité de contrôle pour un mandat d'une durée de cinq ans:

Monsieur Claude Nicolay, avocat général, délégué du procureur général d'Etat, président;

Monsieur René Faber, secrétaire général e.r. de Techno-ARBED, membre;

Monsieur Jean Wagner, conseiller-informaticien première classe auprès du centre commun de la sécurité sociale, membre;

Monsieur Sylvain Wagner, conseiller de direction première classe au ministère de la Justice, secrétaire.

Conformément à l'article 115 de la Convention d'application de l'Accord de Schengen du 14 juin 1985, signée à Schengen, le 19 juin 1990, approuvée par la loi du 3 juillet 1993, le même arrêté grand-ducal a désigné comme représentants de l'autorité de contrôle à l'autorité de contrôle commune chargée du contrôle de la fonction de support technique du système d'information Schengen:

Messieurs René Faber et Sylvain Wagner, préqualifiés, représentants effectifs;

Messieurs Claude Nicolay et Jean Wagner, préqualifiés, représentants suppléants.

3. Réunions de l'autorité de contrôle

Depuis son institution, et jusqu'au 29 mars 1996, l'autorité de contrôle s'est réunie à seize reprises.

Cinq de ces réunions étaient des réunions communes avec le commandant de la Gendarmerie et le directeur de la Police ou leurs représentants.

D'autre part, elle a eu, en date du 24 janvier 1994, une entrevue avec le ministre de la Justice, ministre ayant dans ses attributions le répertoire national des banques de données.

4. Contrôles effectués

4.1.

Le premier acte de l'autorité de contrôle [ci-après dénommée «l'AC»] a été de demander aux responsables des forces de l'ordre, sur base de l'article 12-1, paragraphe (4) de la loi modifiée du 31 mars 1979 réglementant l'utilisation des données nominatives dans les traitements informatiques [ci-après dénommée «la loi»] qui prévoit que l'autorité de contrôle est informée immédiatement de la création d'une banque de données visée par le présent article», de lui communiquer la liste des banques de données en exploitation.

Il a été constaté qu'outre la banque de données des «personnes ayant subi un avertissement taxé en matière de circulation routière», dont la création et l'exploitation ont été autorisées par le règlement grand-ducal du 7 mars 1986, les forces de l'ordre exploitent différentes autres banques de données qui

- soit rentrent dans le cadre de la banque de données nominatives de police générale INGEPOL, dont la création et l'exploitation ont été autorisées par le règlement grand-ducal du 2 octobre 1992,

- soit constituent des banques de données constituées, conformément à l'article 12-1, paragraphe 2 de la loi, «dans le cadre d'une ou de plusieurs affaires pénales» et qui «peuvent être autorisées par le ministre ayant dans ses attributions le répertoire national des banques de données, après avoir entendu en son avis la commission consultative prévue à l'article 30» de la loi.

Concernant cette deuxième catégorie de banques de données, l'AC a exprimé l'avis que la finalité des banques de données en question doit être strictement liée à une, sinon à plusieurs affaires pénales de même nature. L'AC estime en effet qu'il serait inadmissible que par le biais de ces banques de données «ad hoc», les restrictions imposées par le règlement grand-ducal du 2 octobre 1992 relatif à la création et l'exploitation d'une banque de données nominatives de police générale puissent être contournées.

Quant à l'autorisation ministérielle prévue par la loi qui, le cas échéant, doit respecter le caractère urgent d'une demande d'autorisation, elle doit toutefois nécessairement revêtir la forme d'un arrêté ministériel, indiquant clairement les conditions de création (et d'exploitation) à respecter, de même que la durée de validité de l'autorisation, en général, et la durée de conservation des données enregistrées, en particulier, sans que pour autant, et cela pour des raisons évidentes, la publication de l'arrêté ministériel au Mémorial ne soit requise.

Dans ce contexte, l'autorité de contrôle a interprété l'article 12 de la loi qui dispose: «En ce qui concerne les banques de données intéressant la sûreté de l'Etat, la Défense nationale et la sécurité publique, le Gouvernement en conseil peut les dispenser de l'inscription au répertoire national visé à l'article 13», en ce sens que le gouvernement en conseil peut accorder une dispense générale, valable pour toute banque de données à autoriser en application de l'article 12-1, paragraphe (2) de la loi.

4.2.

Après avoir été informée que la banque de données nominatives de police générale INGEPOL, pour des raisons d'ordre technique et budgétaire, n'est pas sur le point d'être créée et exploitée, sauf diverses applications ponctuelles rentrant dans le cadre général de la banque de données en question, l'AC s'est essentiellement consacrée, au cours des deux premières années de ses activités, à suivre de près, et ce avant sa mise en exploitation définitive, la conception et la réalisation de la banque de données nominatives constituant la partie nationale du système d'information Schengen (N.SIS), telle qu'autorisée par le règlement grand-ducal du 9 août 1993.

Ce faisant, l'AC n'a pas perdu de vue lors de son examen des problèmes en relation avec le N.SIS, et notamment celui des motifs d'interrogation, que les mêmes solutions pourront de toute vraisemblance trouver leur application lors des interrogations de la partie recherche de personnes et d'objets de la banque de données INGEPOL, quand celle-ci sera opérationnelle.

Il est rappelé à cet effet, que les agents des forces de l'ordre (terminaux mobiles installés dans les véhicules et terminaux installés dans les brigades et commissariats), alors qu'ils accéderont au «système», ne sauront en définitive s'ils font leur recherche dans la banque de données N.SIS ou dans la partie recherche de la banque de données INGEPOL. La logique du «système» guidera les recherches des agents vers celle des banques de données intégrées dans le «système» qui leur permettra, le cas échéant, d'obtenir un «hit».

4.3.

Les contrôles de l'AC se sont par la suite axés sur trois points essentiels de la Convention d'application de l'Accord de Schengen. Ces contrôles se sont opérés en étroite collaboration avec les forces de l'ordre, et lors de réunions communes auxquelles assistaient soit le commandant de la Gendarmerie et le directeur de la Police, soit leurs représentants, soit lors de visites au service informatique des forces de l'ordre à Luxembourg-Verlorenkost.

4.3.1. La liste des accès autorisés au N.SIS

(article 101 (4) de la Convention d'application de l'Accord de Schengen)

L'article 3 du règlement grand-ducal du 9 août 1993 autorisant la création et l'exploitation d'une banque de données nominatives de la partie nationale du système d'information Schengen (N.SIS) dispose:

«(1) Conformément à l'article 101 paragraphes 1er et 2 de la Convention, les propriétaires du N.SIS [la Gendarmerie et la Police, sous l'autorité du commandant de la Gendarmerie et le directeur de la Police] sont autorisés à communiquer à d'autres administrations, services et organismes publics les données relatives:

- a. aux contrôles frontaliers et autres vérifications de police et de douanes exercées à l'intérieur du pays;
- b. à la délivrance des visas et à l'examen des demandes de visas;
- c. à la délivrance des titres de séjour et à l'administration des étrangers.

(2) La communication de données se limitera à celles qui sont nécessaires à l'accomplissement des missions légales et réglementaires respectives des administrations, services et organismes publics en question.

(3) Conformément à l'article 101 paragraphe 4 de la Convention, une liste énumérera de façon exhaustive les administrations, services et organismes publics en question et leurs missions légales et réglementaires respectives. Copie de cette liste sera remise aux propriétaires du N.SIS.»

L'AC avait demandé au commandant de la Gendarmerie et au directeur de la Police, chargés en tant que propriétaires de la banque de données d'établir la liste des instances autorisées à accéder au SIS conformément à l'article 101 de la Convention d'application de l'Accord de Schengen, de lui soumettre pour approbation, avant de l'envoyer aux mêmes fins au comité exécutif Schengen, la liste définitive des accès à autoriser sur base de l'article 3 du règlement grand-ducal du 9 août 1993.

Après avoir exprimé à deux reprises ses objections quant aux bases légales («missions légales et réglementaires») auxquelles se réfèrent différents services et organismes publics pour avoir accès à certaines catégories de données traitées dans le N.SIS, l'AC recevait, en date du 14 avril 1995, de la part des propriétaires de la banque de données, la liste définitivement arrêtée, telle qu'elle avait été remise entre temps aux instances compétentes. Même si la liste en question n'avait pas été approuvée en due forme par l'AC avant son envoi au comité exécutif Schengen, l'AC n'avait plus d'autres remarques à formuler, la liste définitive ayant été établie en tenant compte de toutes ses observations et objections précédemment formulées.

Cette liste est jointe en annexe au présent rapport.

4.3.2. L'enregistrement des consultations, ainsi que du motif d'interrogation, de la banque de données (article 103 de la Convention d'application de l'Accord de Schengen)

L'article 5 du règlement grand-ducal du 9 août 1993 précité dispose:

«(1) Lors de chaque consultation du N.SIS, le nom de l'agent qui a procédé à l'interrogation, la date et l'heure, ainsi que le motif de l'interrogation doivent être enregistrés.

(2) Les données relatives à ces enregistrements ne sont accessibles qu'à l'autorité de contrôle instituée par l'article 12-1 paragraphe (4) de la loi modifiée du 31 mars 1979, ainsi qu'au commandant de la Gendarmerie et au directeur de la Police ou aux agents spécialement désignés par ces derniers aux fins de contrôle interne.

(3) Ces données sont effacées si l'autorité de contrôle décide que l'utilité de leur enregistrement est devenue caduque.»

Il faut savoir qu'il est prévu que tous les agents de la Gendarmerie et de la Police, mais également ceux des Douanes, ont à tout moment accès au système, pendant et en dehors de leurs heures de service. D'autre part, les agents accédant au système à l'aide des terminaux mobiles intégrés dans leurs véhicules de service, circulent rarement avec l'ordre d'exécution d'une mission définie, arrêtée par le supérieur hiérarchique. Dans la majorité des cas, ils circulent aux fins d'un «contrôle préventif dans le cadre d'une mission de routine». L'AC était consciente de la difficulté de prévoir, pour les agents présents sur le terrain, l'enregistrement d'un motif d'interrogation précis, adapté à la finalité de l'interrogation, alors que leur mission est nullement définie avec précision.

Afin de résoudre le problème, l'AC a proposé de se référer à une certaine «hiérarchie» des principes.

Le principe de base est celui de la subdivision fonctionnelle qui conditionne l'accès au système. Ainsi, au ministère de la Justice, les agents du service des étrangers ne sont pas autorisés à interroger les mêmes données que les agents du service des armes prohibées, le procureur général d'Etat peut accéder à moins de données que les membres des parquets de Luxembourg et de Diekirch, ... Ainsi, en ce qui concerne les forces de l'ordre, les fonctions des agents sur le terrain ne sont pas nécessairement celles des officiers de police judiciaire et vice versa.

Sur le principe de la subdivision fonctionnelle vient se greffer le principe du traitement autorisé. Le système ne doit permettre l'accès d'un agent des forces de l'ordre ou d'une administration qu'aux seules données qu'il est autorisé de traiter (interrogation ou création, modification et suppression d'un signalement). Il était donc proposé que pour chaque traitement autorisé, le système affiche un écran de motifs possibles (maximum 12) parmi lesquels l'agent serait obligé de choisir celui qui correspond à la finalité de son accès au système.

Le problème des motifs d'interrogation se pose donc essentiellement dans le chef de ceux des utilisateurs (Gendarmerie, Police, Douanes [= forces de l'ordre]; terminaux fixes et mobiles), dont l'accès au système est «illimité» (articles 95 - 100 de la Convention). Il est de moindre importance dans le chef de ceux (ministère des Affaires étrangères, ministère de la Justice, parquet général, parquet Luxembourg, parquet Diekirch [= administrations], mais également service spécial Gendarmerie-Aéroport) auxquels il n'est concédé qu'un accès «dans l'accomplissement de leurs missions légales et réglementaires» respectives, donc un accès limité. Il existe donc une étroite relation entre les catégories de signalement du SIS et les motifs d'interrogation.

Se basant sur cette «hiérarchie» des principes, l'AC est venue aux conclusions suivantes:

1. Afin de prévenir des accès abusifs au système, il serait hautement souhaitable que les agents ne puissent interroger la banque de données N.SIS (et la banque de données INGEPOL) que pendant leurs heures de service, et que toute interrogation en dehors des heures de service soit exclue. Comme il doit nécessairement exister un plan de service («Schichtplan») au sein des forces de l'ordre, il est proposé de faire gérer ce plan par le système, ce qui permettrait au système de refuser d'office tout accès, pour quelque motif que ce soit, émanant d'un agent hors service.

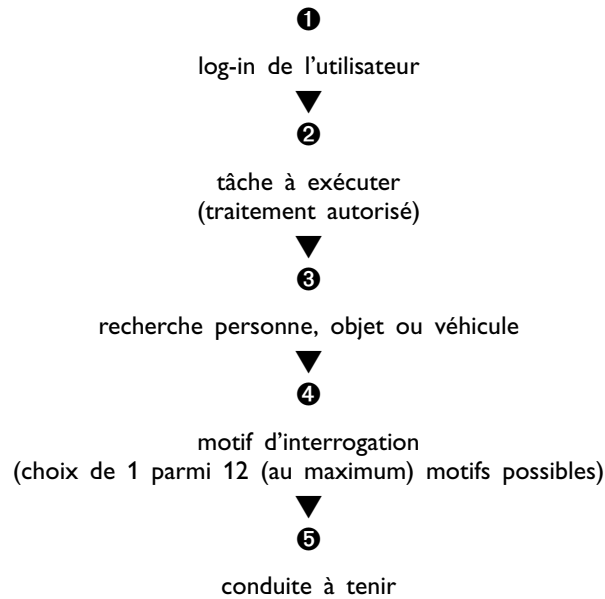
2. Dans la mesure du possible, les missions des agents, et notamment de ceux opérant sur le terrain, sont à définir à priori, et de la façon la plus précise possible. Cela permettrait d'exclure l'usage de motifs d'interrogation «passe-partout» et exigerait le recours à des motifs d'interrogation rentrant dans la définition de la mission à exécuter.

3. Les motifs d'interrogation sont prédéfinis et affichés. L'agent n'a donc nullement besoin d'entrer un texte, même pas standard. En contrepartie, les motifs d'interrogation doivent être définis le plus précisément possible, et les agents sont à inviter par instruction de service, à utiliser le motif d'interrogation adéquat, voire le plus adéquat.

4. Il est dans la logique des choses que, si par exemple, trois motifs d'interrogation ne sont possibles, l'écran n'en affichera que trois.

5. De l'avis de l'AC, toute interrogation du système devrait donc se faire selon le schéma suivant (et pour les forces de l'ordre, terminaux fixes et mobiles confondus, et pour les administrations):

951



Si l'interrogation se fait suivant ce schéma, cela entraîne que pour chaque nouvelle recherche de personne, d'objet ou de véhicule, rentrant dans la même tâche à exécuter (troisième étape), l'indication du motif d'interrogation est à répéter. Cela entraîne également que pour toute nouvelle tâche à exécuter, il y a lieu pour l'agent de revenir jusqu'à la deuxième étape.

L'AC communiquait ses conclusions relatives aux motifs d'interrogation au commandant de la Gendarmerie et au directeur de la Police, tout en les invitant, en tant que copropriétaires de la banque de données N.SIS, à lui soumettre dans les meilleurs délais les «écrans à motifs» à élaborer pour examen et avis.

Par ailleurs, il avait été convenu que l'AC se concerterait avec les copropriétaires de la banque de données «avant que la firme UNILOG ne soit contactée en vue de la programmation d'un logiciel adéquat». Cette concertation n'a pas eu lieu.

Concernant les motifs d'interrogation de la banque de données INGEPOL, l'AC proposait aux forces de l'ordre de prévoir la solution suivante:

- Partie archives INGEPOL: pas de nécessité d'enregistrement d'un motif d'interrogation, l'accès à cette partie de la banque de données de police générale n'étant permise que de l'accord exprès du procureur général d'Etat ou du membre de son parquet désigné à cette fin.
- Partie documentaire INGEPOL: indication d'un motif précis qui peut prendre la forme, soit d'un texte standard («poursuite de l'enquête, PV n° du»), soit d'un texte libre («enquête dans le cadre de la prévention»).
- Partie recherche de personnes et d'objets INGEPOL: prévoir les plus grandes facilités, afin de ne pas entraver les actions sur le terrain; motifs abrégés, touches programmées (solution identique à celle retenue pour la banque de données N.SIS).

4.3.3. Les mesures à prendre afin de garantir la sécurité du N.SIS

(article 118 (1) de la Convention d'application de l'Accord de Schengen)

Pour le contrôle de ces mesures, l'AC a suivi en principe le schéma donné par l'article 118, paragraphe (1) de la Convention d'application de l'Accord de Schengen, tout en y apportant, pour les besoins du présent rapport, quelques aménagements. Ainsi, les contrôles de la sécurité peuvent être regroupés en cinq rubriques:

- le contrôle à l'entrée des installations (accès physique aux installations techniques);
- le contrôle des supports de données, y compris le transport de ces supports;
- le contrôle de l'intégration et de l'introduction des données;
- le contrôle de l'utilisation des données, y compris le contrôle de l'accès aux données;
- le contrôle de la transmission des informations.

4.3.3.1. Le contrôle à l'entrée des installations

La situation, telle qu'elle existe à l'entrée du nouveau bâtiment de la Gendarmerie à Luxembourg-Verlorenkost peut être décrite comme suit:

- L'accès au nouveau bâtiment (entrée principale + garage), de même qu'à l'un ou l'autre service installé dans l'ancien bâtiment, n'est possible que moyennant carte magnétique. Chaque passage des cartes dans le système d'ouverture des postes est enregistré sur le disque dur d'un PC installé au poste central de gardiennage occupé 24 heures sur 24.
- L'accès à la salle des machines (ordinateurs), de même que l'accès à la chambre forte du service armurerie et au poste central de gardiennage, ne peut se faire que moyennant trois autres lecteurs de badge. Ici aussi, chaque entrée et chaque sortie (du moins pour la salle des machines) est enregistrée.

- Outre l'identité du porteur de la carte, l'ordinateur enregistre le numéro de l'«ouvreur» de porte qui est activé, de même que le moment exact de son activation. Par ailleurs, il enregistre une porte d'entrée qui reste ouverte pendant une période anormalement longue, donc celui qui a laissé la porte ouverte.
- Les cartes magnétiques (quatre catégories: agents de la Gendarmerie, agents de la Police, agents de la Gendarmerie n'ayant pas leur affectation à Luxembourg-Verlorenkost (service de renseignement, garage du gouvernement, brigades, ...) et agents à l'étranger et autres) permettent un accès différencié dans les locaux équipés d'un lecteur de badge. A cet effet, les cartes magnétiques renseignent sur l'identité de leur porteur et ses accès autorisés.

Les «faiblesses» du système que l'AC a détectées:

- Moyennant une seule carte, plusieurs personnes, étrangères au service ou même étrangères au bâtiment, peuvent accéder en un lieu sécurisé par lecteur de badge. Il n'existe pas de tourniquet mécanique qui ne permettrait que le passage d'une seule personne à la fois.
- Il devrait être exclu que la (les) porte(s) d'accès à la salle des machines, alors qu'elles sont équipées d'un lecteur de badge distinct pour la sortie, puissent rester ouvertes! Un simple fermoir de porte mécanique remédierait à cet état des choses. Par ailleurs, un système d'alarme signalant le non fonctionnement de ces fermoirs devrait être installé.
- Outre la salle des machines et la chambre forte (armurerie), les autres locaux des bâtiments de la Gendarmerie (bureaux, salles de réunion, RIFO (Réseau d'Information des Forces de l'Ordre), couloirs, ...) sont librement accessibles, sans qu'il n'y ait une séparation entre l'une ou l'autre «zone» des bâtiments. Cela vaut également pour les bureaux ou autres locaux où sont installés des terminaux reliés au N.SIS.
- Un nombre limité de personnes (chefs hiérarchiques, service de sécurité, pompiers, ...) peuvent se munir d'un passe-partout, qu'elles peuvent se procurer au poste central de gardiennage. Il s'agit d'une clé de sécurité permettant d'ouvrir toutes les portes, en dépit des lecteurs de cartes. Il y a lieu de se demander si l'ordinateur enregistre également ces entrées et sorties!
- Le programme de l'ordinateur ne permet pas de refuser l'accès en fonction du plan de service («Schichtplan»).
- Par ailleurs, ce PC est mal adapté à ses fonctions de «contrôleur» central:
- il ne dispose pas de mémoire, de façon que, si par malchance il est déconnecté, toutes les données enregistrées sont effacées;
- vu sa capacité d'enregistrement limitée, les responsables ignorent quelle est l'étendue de l'historique des accès enregistrés;
- il n'est pas fait de back-up systématique des enregistrements.

4.3.3.2. Le contrôle des supports de données, y compris le transport de ces supports

Les supports magnétiques sur lesquels se trouvent enregistrées les données traitées dans le SIS, se trouvent exclusivement dans la salle des ordinateurs; alors que ces derniers ne sont pas utilisés, ils sont enfermés dans une chambre forte. Cela vaut de même pour les supports «back-up». Seuls les informaticiens en charge de l'exploitation du système (trois personnes), ont un accès autorisé aux supports de données. En particulier, les agents du bureau SIRENE sont exclus de cette autorisation.

Rappelons que le bureau SIRENE (Supplément d'Information Requis à l'Entrée Nationale) constitue le service national de coordination du SIS. L'organisation et les missions de ce service sont définies par le «Manuel SIRENE», élaboré de commun par tous les pays Schengen, dans le but d'arriver à une uniformisation des missions. Ces missions sont essentiellement de double nature:

- la transmission des informations supplémentaires relatives aux signalements intégrés dans le SIS;
- la liaison permanente avec les services nationaux de coordination du SIS des autres pays Schengen.

Il a été souligné que ces supports de données ne sont soumis à aucun transport en dehors du bâtiment de la Gendarmerie de Luxembourg-Verlorenkost. Cela s'explique par le fait que tous les accès au système se font via les ordinateurs du STTI (Service de Traitement et de Transmission de l'Information), commun à la Gendarmerie et la Police, et que le Luxembourg, vu l'exiguïté de son territoire n'a nullement besoin de confectionner des copies techniques pour les besoins d'autres utilisateurs du système.

La question se pose toutefois de savoir s'il ne serait pas utile de déposer une copie de sécurité dans un autre endroit, tel que le fait actuellement le Centre informatique de l'Etat en ce qui concerne les données gérées pour l'Etat luxembourgeois. La réponse à cette question peut être négative, alors que le système SIS, de par sa nature même est un système constamment tenu à jour par le support technique de Strasbourg qui, en cas de catastrophe ayant pour conséquence la destruction du N.SIS luxembourgeois, pourrait faire parvenir dans les meilleurs délais une nouvelle copie du système aux autorités luxembourgeoises. Cette faculté, de même que la particularité de système consistant dans la mise à jour permanente des données intégrées dans le système, rendent inutile la confection d'une copie de sécurité qui par ailleurs, serait probablement contraire à l'esprit de la Convention d'application de l'Accord de Schengen.

4.3.3.3. Le contrôle de l'intégration et de l'introduction des données

Les agents du bureau SIRENE sont les seuls habilités à introduire, modifier et effacer des données dans le système Schengen. Etant donné que la banque de données N.SIS est exploitée en mode «read only», aucune introduction et modification, ni aucun effacement ne peut se faire directement dans la banque de données elle-même. Toute prise de connaissance d'informations dans la banque de données est conditionnée par le contrôle d'accès au système.

Les opérations d'introduction, de modification et d'effacement précitées se font toutes à l'aide d'un fichier intermédiaire appelé «fichier de référence». Dans ce fichier, outre les informations destinées au système SIS, sont mentionnés la date et l'heure de l'opération, le service responsable pour le signalement, l'opérateur SIRENE, le PC ou le terminal sur lequel l'opération a été faite. Par ailleurs, ce n'est qu'après validation des signalements par le responsable du bureau SIRENE que les informations sont introduites dans ce «fichier de référence» et transmises à Strasbourg aux fins de la mise à jour du système.

Les données enregistrées dans le «fichier de référence» ne sont modifiées et effacées qu'au moment où ces opérations deviennent nécessaires dans le C.SIS. Les informations propres à l'organisation luxembourgeoise sont enregistrées par ailleurs, aux fins de contrôle de l'accès au système, dans le WORM spécialement prévu à cette fin.

Les principes d'organisation mis en place pour garantir le contrôle de l'intégration et de l'introduction des données peuvent, de façon générale, être jugés satisfaisants.

4.3.3.4. Le contrôle de l'utilisation des données, y compris le contrôle de l'accès aux données

Lors d'une de ses missions de contrôle, l'AC constatait que les propriétaires de la banque de données avaient étendu l'écran des motifs possibles d'un maximum proposé de 12 à 17. Il lui fut expliqué que l'extension du nombre des motifs devait permettre, non seulement un meilleur maniement des motifs en question, mais surtout un contrôle plus rigoureux de l'emploi de ces motifs.

L'AC a pu constater que la connexion à l'application se fait en principe suivant le schéma retenu et que pour chaque consultation l'utilisateur doit indiquer un motif. Elle a dû toutefois se rendre compte qu'aucun contrôle n'est fait sur le bien-fondé du motif employé. Aussi juge-t-elle opportun que les propriétaires de la banque de données fassent une vérification ex-post pour être en mesure de détecter des anomalies ou des abus éventuels. A titre d'exemple, mentionnons que l'AC a constaté que le motif «contrôle aux frontières extérieures (aéroport) est utilisé non seulement par des opérateurs utilisant les terminaux situés à l'aéroport, mais également par des opérateurs travaillant sur d'autres terminaux.

Des données de types différents sont reprises dans le N.SIS comme des informations entre autres sur des personnes disparues, sur des personnes recherchées par la Justice, sur des personnes non admissibles. Tous ces renseignements ne doivent pas être accessibles à toutes les administrations et services ayant accès à l'application. Des tables d'autorisation d'accès permettent de gérer les droits d'accès des différentes administrations. Pour les grandes administrations, telles que la Gendarmerie, la Police et les Douanes, tous les fonctionnaires ont le droit de consulter toutes les informations intéressant leur administration, même si dans l'exécution de ses missions spécifiques, un tel agent n'a nullement besoin d'accéder à de telles données. L'AC est d'avis qu'il serait hautement opportun de limiter l'accès aux données traitées dans le N.SIS aux agents ayant effectivement besoin des informations en question pour la bonne exécution de leurs missions, d'une part, et aux informations strictement nécessaires à l'exécution de leurs missions, d'autre part. En ce qui concerne la banque de données INGEVOL, le contrôle d'accès devra, en tout état de cause, être beaucoup plus sélectif et restrictif.

Comme indiqué plus haut, l'article 5 du règlement grand-ducal du 9 août 1993 dispose que lors de chaque consultation le nom de l'agent qui a procédé à l'interrogation doit être enregistré. Or, il faut relever, que dans un certain nombre de bureaux, plusieurs agents se partagent un même terminal. Le premier agent qui se connecte au système doit bien déclarer son identité. Une fois le log-in fait, l'utilisateur ne se déconnecte généralement plus, et les autres agents utilisant ce même terminal travaillent sous l'identité du premier utilisateur. Cette façon de procéder est manifestement contraire aux dispositions de l'article 5.

Afin de remédier à cet état des choses, plusieurs solutions peuvent être envisagées. Une première consiste à équiper chaque agent d'un terminal ce qui représente un coût non négligeable. Une autre solution serait que l'application déconnecte d'office chaque terminal après une certaine période de non activité. On force ainsi chaque agent de faire à chaque fois le log-in ce qui n'est pas non plus la solution idéale. L'AC propose une troisième solution, dont le coût est moindre et qui reste conviviale pour les utilisateurs: chaque terminal ou PC est à doter d'un lecteur de badge, et tant que l'agent n'a pas introduit sa carte d'identification dans ce lecteur de badge, l'application ne fournit aucun renseignement.

4.3.3.5. Le contrôle de la transmission des informations

L'article 1er du règlement grand-ducal du 9 août 1993 dispose en son paragraphe (2):

«Les propriétaires et gestionnaires prennent toute mesure nécessaire, et notamment celles prévues à l'article 118 de la Convention, afin de garantir la sécurité du N.SIS et de sa liaison avec le support technique du système d'information Schengen.»

Dès sa première réunion avec les forces de l'ordre, l'AC a exigé des copropriétaires de la banque de données N.SIS, que non seulement les données, mais également la transmission des données soit sécurisée au plus haut degré, à savoir celui préconisé par la Convention d'application de l'Accord de Schengen. L'AC faisait en effet remarquer que, étant donné que le règlement grand-ducal du 9 août 1993 fait expressément référence aux mesures prévues par l'article 118 de la Convention d'application de l'accord de Schengen, il incombait aux copropriétaires de démontrer que les mesures de sécurité prévues ou à prévoir pour le N.SIS luxembourgeois atteignent le niveau de sécurité prévu par l'article 118 en question, niveau de sécurité prévu par ailleurs à Strasbourg pour le support technique du système d'information Schengen, le C.SIS, dont l'installation a été réalisée par le ministère de l'Intérieur français. En fait, la sécurité du système d'information Schengen (C.SIS, les différents N.SIS y reliés, de même que les liaisons entre C.SIS et les différents N.SIS) n'est garantie que si elle est identique à chaque endroit du système. Un maillon fragile dans la chaîne SIS mettrait en péril la sécurité de tout le système.

Voilà pourquoi l'AC informait les copropriétaires de la banque de données N.SIS en date du 15 mars 1994 qu'elle «s'est décidée à exiger que les données transmises sur le réseau N.SIS, y inclus le réseau radio, soient cryptées. De l'avis de l'autorité de contrôle, ce n'est que par ce moyen technique que tout détournement de données peut être, si ce n'est exclu, du moins rendu hautement improbable.»

Lors d'un contrôle des installations techniques au nouveau siège de la Gendarmerie à Luxembourg-Verlorenkost, l'AC a été informée que:

- concernant la partie internationale du SIS, les transmissions opérées à destination du support technique à Strasbourg, de même que les informations reçues de la part du support technique, d'une part, les transmissions de données entre bureaux SIRENE, d'autre part, se font par le biais de lignes louées et cryptées, donc sécurisées et ne devraient pas poser de problèmes;
- concernant la partie nationale, il y a lieu de distinguer entre le réseau des terminaux mobiles et celui des stations fixes du réseau de communication des forces de l'ordre (RCDFO).

Si le réseau des terminaux mobiles, selon les dires des responsables des forces de l'ordre, est hautement sécurisé, même sans cryptage des informations, étant donné qu'il s'agit d'un réseau unique en Europe livré par une firme spécialisée, le réseau des stations fixes du RCDFO pose des problèmes pour le moment, étant donné que les transmissions s'opèrent via le réseau public LUXPAC, nullement sécurisé. Deux solutions peuvent être envisagées pour résoudre ces problèmes: soit cryptage des lignes LUXPAC, soit installation d'un réseau «privé» des forces de l'ordre.

Les préférences des responsables des forces de l'ordre vont dans la direction de la deuxième solution. Aussi ont-ils demandé à l'AC de soutenir cette proposition, afin que le gouvernement mette à disposition, de préférence pour l'exercice 1995, mais au plus tard pour l'exercice 1996 les crédits budgétaires nécessaires.

L'AC appuie les forces de l'ordre dans leur souhait de voir la transmission de leurs données être sécurisée à un niveau technique tel qu'un détournement de données puisse être rendu hautement improbable. Voilà pourquoi elle soutient également l'invitation des responsables des forces de l'ordre au gouvernement de prévoir les crédits nécessaires pour que le cryptage des données transmises sur le réseau N.SIS (lignes téléphoniques louées), y inclus le réseau radio, puisse être assuré.

L'AC constate avec regret que le budget de l'Etat pour l'exercice 1996 ne contient toutefois aucun crédit pour l'amélioration, voire la création de la sécurité nécessaire aux transmissions des données des forces de l'ordre. Elle espère vivement que les crédits en question seront inscrits de façon prioritaire dans le projet de budget pour l'exercice 1997.

5. Activités internationales

5.1. ACC(P) Schengen

Visée par l'article 115 de la Convention d'application de l'Accord de Schengen du 14 juin 1985, l'«Autorité de contrôle commune Schengen» est la première autorité de contrôle à avoir été instaurée par un instrument international. Elle se compose de deux représentants de chaque autorité nationale de contrôle des Parties contractantes de l'Accord de Schengen qui disposent d'une législation en matière de protection des données à caractère personnel et d'une ou de telle(s) autorité(s) nationale(s). Pour le moment, il s'agit de l'Allemagne, de la Belgique, de l'Espagne, de la France, du Luxembourg, des Pays-Bas et du Portugal. Continuent à rester sur la touche: la Grèce et l'Italie.

Alors que le Luxembourg assumait la présidence Schengen au cours du premier semestre 1992, le Groupe central Schengen, lors de sa réunion du 12 mai 1992, marquait son accord avec une note qui lui avait été adressée par le Comité d'orientation Schengen, dans laquelle ce comité proposait de mettre en place une autorité de contrôle commune provisoire, composée des autorités de contrôle nationales en matière de protection des données des Parties contractantes, avec la mission d'effectuer, dans le sens de l'article 115 de la Convention, des contrôles en matière de protection et de sécurité des données à caractère personnel au cours de la phase d'initialisation, c'est-à-dire, pendant la phase précédant la phase opérationnelle du système d'information Schengen (SIS). Quant à la représentation au sein de cette autorité provisoire des pays ne disposant pas encore d'autorité de contrôle nationale (à l'époque: la Belgique, l'Espagne, l'Italie et le Portugal), le Groupe central estimait que ces pays pourraient participer aux travaux de cette autorité à titre d'observateurs.

La première réunion de l'autorité de contrôle commune provisoire eut lieu à Bruxelles, au secrétariat général BENELUX, assumant le secrétariat Schengen, en date du 29 juin 1992. Lors de cette réunion, le président de la commission consultative instituée par l'article 30 de la loi modifiée du 31 mars 1979 réglementant l'utilisation des données nominatives dans les traitements informatiques, représentant, de pair avec le secrétaire de la même commission, le Luxembourg au sein de l'autorité de contrôle commune provisoire, fut élu, à l'unanimité des autorités de contrôle nationales représentées, premier président de l'autorité.

Après s'être dotée d'un règlement intérieur qui confirme que l'autorité de contrôle commune élit elle-même son président, et que par là, la règle de la présidence tournante ne s'applique pas à elle, ce qui revêt toute son importance dans le contexte du contrôle indépendant qui lui incombe de par la Convention d'application de l'Accord de Schengen, l'autorité de contrôle commune provisoire s'attacha à ses missions qui consistaient notamment à examiner l'utilisation de données réelles lors des phases de test du système d'information Schengen, de même que les mesures de sécurité mises en place pour garantir la confidentialité des données à caractère personnel traitées dans le système. Dans ce contexte, elle a visité, en mars 1994, le site d'implantation de l'ordinateur central du système à Strasbourg.

Dès leur désignation par arrêté grand-ducal du 29 septembre 1993, les représentants de l'autorité de contrôle ont pris la relève des représentants précédemment désignés au sein de l'autorité de contrôle commune provisoire Schengen.

Après la mise en application définitive du système d'information Schengen en date du 26 mars 1995, l'autorité de contrôle commune «définitive» s'est substituée à l'autorité de contrôle commune provisoire. Depuis sa réunion de constitution en date du 17 mai 1995, elle s'est réunie à cinq reprises.

Composée des représentants des autorités de contrôle nationales des Parties contractantes mentionnées ci-dessus, elle s'est fixée comme première mission l'adaptation du règlement intérieur adopté par l'autorité de contrôle commune provisoire à ses propres missions. Actuellement, l'autorité analyse de quelle façon elle pourrait établir la meilleure coopération possible avec les autorités de contrôle nationales en matière d'exercice du droit d'accès aux données traitées dans le SIS.

5.2. Groupe La Haye

D'autre part, l'autorité de contrôle participe activement à un groupe de travail avec lieu de réunion à La Haye, institué sous l'égide de la Conférence européenne des commissaires à la protection des données à caractère personnel. Ce groupe est en charge d'examiner toutes les propositions d'instrument juridique dans les domaines de la police et des douanes, ainsi que des autres domaines couverts par le troisième pilier du Traité sur l'Union européenne (système d'information européen (SIE), franchissement des frontières extérieures, visa unique, identification des demandeurs d'asile (EURODAC), EUROPOL, ...).

C'est dans ce contexte qu'ont eu lieu en 1994 des visites au siège du futur EUROPOL à la Haye et au siège de l'Organisation internationale de police criminelle (OIPC-INTERPOL) à Lyon.

6. Conclusion

Un an après la mise en vigueur de la Convention d'application de l'Accord de Schengen - et donc du SIS - l'AC constate qu'elle n'a pas été saisie d'une seule demande d'exercice du droit d'accès aux données traitées dans le N.SIS, banque de données constituée «pour la prévention, la recherche, la constatation et la poursuite des infractions». En conséquence, elle n'a pas procédé à des vérifications sur base de l'article 12-1, paragraphe (5) de la loi du 31 mars 1979.

L'AC a choisi de se concentrer, dans un premier temps, sur le respect des dispositions conventionnelles, légales et réglementaires au niveau de la conception et de l'organisation fonctionnelle de la partie nationale du système d'information Schengen.

Globalement, les contrôles effectués ont donné un résultat satisfaisant . . .

L'AC est toutefois arrivée à la conclusion que le Luxembourg ne respecte pas les obligations qui découlent de l'article 118, paragraphe (1), sub lettre a. de la Convention d'application de l'Accord de Schengen, et donc de l'article 1er, paragraphe (2) du règlement grand-ducal du 9 août 1993.

Les déficiences décrites dans ce rapport amènent l'AC à conclure que la sécurité physique du N.SIS est loin d'être garantie. L'AC estime que cette situation devrait être une source de préoccupation majeure pour le gouvernement.

L'AC a de sérieux doutes sur la question de savoir si l'utilisation des données et l'accès aux données sont conformes aux prescriptions conventionnelles et réglementaires. Il a été dit plus haut que l'article 5 du règlement grand-ducal du 9 août 1993 n'est pas toujours respecté en ce qui concerne l'enregistrement du nom de l'agent qui procède à l'interrogation. Il est permis de douter que l'obligation réglementaire faite à l'agent d'indiquer le motif de l'interrogation, soit toujours respectée à la lettre.

Ce doute se fonde sur deux éléments.

1. L'attitude des propriétaires de la banque de données n'est pas faite pour inciter leurs subordonnés à se conformer à cette obligation. Par lettre du 15 mars 1996 ils ont informé l'AC de leur position en ces termes: «Nous restons d'ailleurs toujours opposés au principe de l'introduction d'un motif pour la consultation d'un fichier de recherches, alors que les personnes contenues dans ce fichier sont signalées par une autorité judiciaire ou administrative dans le but d'être détectées, arrêtées, interdites de séjour, etc. ... , et qu'il ne s'agit en l'occurrence nullement d'une banque de données susceptible de donner lieu à des abus suite à la consultation ou par le fait de la consultation de celle-ci».

2. L'AC a constaté l'utilisation de motifs qui ne pouvaient correspondre à la mission de l'agent procédant à l'interrogation de la banque de données. Il n'est toutefois pas exclu que le recours à de «faux motifs» soit dû à des erreurs attribuables au rodage du système et à l'inexpérience des agents pendant les premiers (douze) mois d'utilisation. L'AC a l'intention de suivre cette question de près à l'avenir.

Rapport adopté à l'unanimité des membres de l'autorité de contrôle lors de sa réunion en date d'aujourd'hui. Luxembourg, le 22 avril 1996.

Pour la commission,
 Claude Nicolay Sylvain Wagner
 président secrétaire

Annexe: Liste des accès autorisés au N.SIS

Vu pour être publié au Mémorial, Recueil administratif et économique.

Luxembourg, le 11 novembre 1997.
 Le Ministre de la Justice,
Marc Fischbach

POLICE

Droits d'accès aux données – Tableau récapitulatif conformément aux demandes des administrations

[illegible]

POLICE

Droits d'accès aux données – Tableau récapitulatif
conformément aux demandes des administrations[illegible]

Autorité de contrôle commune Schengen

Rapport d'activité (mars 1995 à mars 1997)

SOMMAIRE

Préface

Chapitre 1. Rappels

- 1.1. Les textes (Accord, Convention d'application, convention d'adhésion, accords de coopération)
- 1.2. Les instances communes pour l'application de la Convention
- 1.3. L'objectif et l'architecture du système d'information Schengen
 - . les informations enregistrées
 - . les destinataires des informations
 - . l'architecture du SIS
- 1.4. Les bureaux SIRENE

Chapitre 2. La protection des données à caractère personnel

- 2.1. Une loi et une autorité nationale de contrôle : conditions préalables à l'application de la Convention
- 2.2. Les champs d'application respectifs de la Convention et du droit national
 - . les droits des personnes à l'égard du SIS
 - . le contrôle du SIS
 - . les échanges d'informations hors le SIS

Chapitre 3. L'Autorité de contrôle commune et les conditions de son indépendance

- 3.1. La composition de l'ACC
- 3.2. Les missions de l'ACC
- 3.3. Les conditions de l'indépendance
 - . l'adoption d'un règlement intérieur
 - . l'obtention d'une ligne budgétaire propre
 - . l'élaboration d'un rapport d'activité
 - . l'information sur le fonctionnement de la Convention

Chapitre 4. Les missions entreprises

- 4.1. Les missions achevées
 - 4.1.1. Le comparatif des règles de protection des données applicables dans les Etats Schengen
 - 4.1.2. L'examen du fondement juridique des bureaux SIRENE et du contenu du manuel SIRENE
 - 4.1.3. La coopération entre les autorités de contrôle nationales. L'avis du 26 novembre 1996 sur l'exercice du droit d'accès et la coopération pour la vérification des données
 - 4.1.4. Le contrôle du C.SIS
 - . la visite sur place de l'ACCP et l'avis du 18 mai 1994
 - . le contrôle de l'ACC, la visite sur place du 11 février 1997 et l'avis du 27 mars 1997
 - 4.1.5. L'avis sur le projet pilote relatif aux véhicules volés
 - 4.1.6. L'avis sur l'accord de coopération concernant le traitement des infractions routières et l'exécution des sanctions pécuniaires en ce domaine

- 4.2. Les missions en cours
 - 4.2.1. Le guide des droits des personnes pour l'accès au SIS
 - 4.2.2. L'interprétation de l'article 102.2 relatif à la duplication technique des données du SIS
 - 4.2.3. L'interprétation de l'article 103 relatif au contrôle de l'admissibilité de l'interrogation du SIS
 - 4.2.4. L'interprétation de l'article 102.1 relatif au principe de finalité pour l'utilisation des données du SIS

Chapitre 5. L'avenir

- 5.1. La transparence dans les relations entre les instances Schengen
 - . l'information de l'ACC sur le fonctionnement de la Convention
 - . l'achèvement du protocole d'exercice des contrôles du C.SIS
 - . la consécration définitive de l'autonomie budgétaire de l'ACC
- 5.2. La transparence à l'égard du citoyen
 - . sur les objectifs
 - . sur l'élargissement des limites de la Convention de Schengen et la complexité croissante des mécanismes de contrôle des règles de protection des données

Préface

Parmi les grands projets de coopération policière, les accords de Schengen et le système d'information du même nom font figure de laboratoire d'essai.

Or si la Convention d'application de Schengen comporte des dispositions satisfaisantes relatives aux droits des personnes, à la sécurité des données et au contrôle du système informatisé, les reports successifs de mise en application du texte ont bien failli laisser le système qui, au nom de l'efficacité montait en puissance, prendre de vitesse l'application des principes.

Cette situation était préoccupante alors que se développaient déjà d'autres projets de coopération européenne à l'occasion desquels l'impératif d'efficacité ne manquait pas d'être invoqué au premier chef.

Elle aurait pu être préjudiciable au contrôle en matière de protection des données, si une autorité de contrôle commune provisoire n'avait pas été mise en place en 1992.

A l'évidence, l'échange d'informations et la coopération policière, judiciaire et douanière sont devenus, en contrepartie de la libre circulation des personnes, des moyens nécessaires pour lutter contre le terrorisme, le trafic de stupéfiants et la grande criminalité, assurer la sécurité et contrôler les flux migratoires. Tel est le cas, au-delà de Schengen, des conventions d'Europol et de Dublin.

Néanmoins il importe que le ou les chapitres consacrés à la protection des informations relatives aux personnes physiques et aux instances de contrôle communes ou nationales compétentes en ce domaine, ne soient pas une clause de style.

Ce premier rapport d'activité qui porte sur deux années est avant tout le récit inachevé d'une négociation menée pas à pas avec les Etats-parties pour ancrer dans la réalité, conformément à la lettre de la convention, l'indépendance et l'autorité d'une instance de contrôle créée pour veiller au respect des droits des personnes sujets des échanges d'informations.

Ainsi, davantage qu'un laboratoire d'essai, l'autorité de contrôle commune de Schengen, dans son rôle de précurseur, est une figure de proue.

Alex Türk
Mars 1997

Chapitre 1. Rappels

1.1. Les textes

L'Accord de Schengen a été signé le 14 juin 1985 par les gouvernements des Etats de l'Union économique du Benelux, la République fédérale d'Allemagne et la République française. Il a été appliqué à titre provisoire le jour suivant celui de sa signature (article 32) et est entré en vigueur le 2 mars 1986.

Expression de la volonté de créer un espace commun de circulation des marchandises et des personnes pour éviter le renouvellement des incidents nés, un an plus tôt, de la grève du zèle des douaniers italiens (arrêt des camions étrangers aux frontières, mise en place de barrages de protestation en France, perturbation de l'ensemble du réseau routier européen), l'Accord de Schengen visait avant tout à supprimer graduellement les contrôles aux frontières communes des Etats signataires. Et de fait, seuls 7 des 33 articles de l'accord concernent la coopération policière et la lutte contre l'immigration.

A l'inverse, signée par les mêmes Parties contractantes le 19 juin 1990, la Convention d'application de l'Accord de Schengen a développé à des fins de contrôle aux frontières extérieures communes la collaboration policière, douanière et judiciaire, contrepartie jugée nécessaire, dans le contexte des débats nationaux sur l'insécurité et l'immigration, à l'ouverture décidée cinq ans auparavant.

L'une des mesures fondamentales de ce dispositif de coopération a été la création d'un système informatisé commun, le système d'information Schengen (titre IV de la Convention).

La mise en place de ce système a induit, par l'effet de textes nationaux et internationaux imposant le respect de principes de protection des données, la création, en référence aux modèles nationaux d'autorités de contrôle indépendantes compétentes dans ce domaine, d'une autorité de contrôle commune.

La Convention d'application, soumise à ratification, approbation ou acceptation pour entrer en vigueur et, pour être mise en vigueur, au fait que «les conditions préalables à son application soient remplies et que les contrôles aux frontières extérieures soient effectifs» est entrée en vigueur le 1er septembre 1993 et a été mise en application le 26 mars 1995. La date initialement prévue était le 1er janvier 1993.

Ouverte à l'adhésion d'autres Etats membres des Communautés européennes (article 140), la Convention a permis l'élargissement de l'espace Schengen à l'Italie, l'Espagne, le Portugal, la Grèce et l'Autriche, même si, à ce jour, seuls l'Espagne et le Portugal remplissent toutes les conditions pour alimenter le SIS, accéder aux informations qu'il contient et participer à part entière aux réunions de toutes les instances Schengen et notamment, de l'Autorité de contrôle commune.

Plus récemment, le 1er mai 1996, les cinq pays de l'Union nordique, liés par l'accord de l'Union nordique des passeports qui a instauré la libre circulation des personnes entre leurs territoires et les îles Feroe, ont obtenu le statut d'observateur.

Le 19 décembre 1996, le Danemark, la Finlande et la Suède, pays membres de l'Union européenne, ont signé l'accord d'adhésion à Schengen.

L'Islande et la Norvège, qui ne sont pas membres de l'Union européenne, se sont vu proposer, par un accord de coopération du même jour, un statut de membre associé aux termes duquel la Convention, s'applique sur leur territoire, à l'exception des dispositions relatives au contrôle des marchandises, sans qu'ils puissent prendre part formellement aux décisions. Ces deux Etats participeront donc pleinement au fonctionnement du système d'information Schengen.

1.2. Les instances communes pour l'application de la Convention

Les Parties contractantes ont, pour l'application de la Convention, créé deux instances.

- Le Comité exécutif, composé d'un ministre responsable de la mise en oeuvre de la Convention dans chaque Etat-partie, est chargé de la mission générale de veiller à l'application correcte de la Convention et dispose par ailleurs de compétences particulières (article 131).
- L'Autorité de contrôle commune (ACC), composée de deux représentants de chacune des Autorités nationales de contrôle des Etats-parties a pour mission de vérifier la bonne exécution des dispositions de la Convention à l'égard de la fonction de support technique du SIS (article 115). Elle dispose également de compétences plus générales en matière de protection des données.

En dehors de ces deux instances, l'organisation de Schengen est structurée autour d'un Groupe central dont dépend un Comité d'orientation SIS ainsi que divers groupes de travail dont certains sont créés par la Convention.

Les instances Schengen sont assistées par un secrétariat, fonction assumée par le Secrétariat général de l'Union économique du BENELUX dont le siège est à Bruxelles.

1.3. L'objectif et l'architecture du système d'information Schengen

L'intégralité du titre IV de la Convention est consacré au système d'information Schengen (SIS).

L'article 93 de la Convention précise que le SIS a pour objet de préserver l'ordre et la sécurité publics, y compris la sûreté de l'Etat, et l'application des dispositions de la convention sur la circulation des personnes à l'aide des informations transmises par le système.

Les informations enregistrées

L'article 94 énumère limitativement les catégories de données qui peuvent être enregistrées dans le système. Les articles 95 à 100 spécifient les finalités qui justifient l'intégration des signalements.

Les catégories de données se rapportent à des personnes, objets et véhicules.

S'agissant des personnes, peuvent être intégrés les éléments relatifs à l'état civil et les alias, les signes physiques particuliers, objectifs et inaltérables, l'indication éventuelle qu'elles sont armées ou violentes et la conduite à tenir en cas de découverte.

Est interdite la mention d'informations dites sensibles révélant l'origine raciale, les opinions politiques, les convictions religieuses ou autres convictions, ainsi que celles relatives à la santé ou à la vie sexuelle. Les finalités qui justifient le signalement d'une personne dans le SIS sont les suivantes.

- a. Quelle que soit la nationalité de la personne :
 - arrestation aux fins d'extradition (article 95) ;
 - recherche en cas de disparition, recherche de mineurs ou de personnes devant être internées sur décision d'une autorité compétente (article 97) ;
 - arrestation pour comparution, même en qualité de témoin, devant la justice dans le cadre d'une procédure pénale ou pour exécution d'une peine privative de liberté (article 98) ;
 - surveillance discrète et contrôle spécifique pour la répression d'infractions pénales, la prévention de menaces pour la sécurité publique ou pour la prévention de menaces graves pour la sûreté de l'Etat (article 99).
- b. Pour les étrangers, soit toute personne autre que des ressortissants des Etats membres des Communautés européennes (définition dans l'article 1er, 6ème alinéa) :
 - non admission sur le territoire résultant d'une décision administrative ou judiciaire prise dans le respect des règles de procédure nationales ou sur le fondement d'une menace à l'ordre public ou à la sécurité et sûreté nationales ou sur celui du non-respect des réglementations nationales sur l'entrée et le séjour des étrangers (article 96).

S'agissant des objets, seuls peuvent être intégrés les éléments, incluant le nom de leur propriétaire, qui se rapportent aux véhicules, armes à feu, documents et billets de banque volés, détournés ou égarés qui sont recherchés aux fins de saisie ou de preuve dans une procédure pénale (article 100).

S'agissant des véhicules, peuvent également être enregistrées des données relatives à ceux qui sont recherchés aux fins de surveillance discrète ou de contrôle spécifique (article 99 déjà cité). Cette catégorie permet l'enregistrement d'informations concernant les conducteur et occupants des véhicules surveillés.

Les destinataires des informations

Les articles 92 et 101 de la Convention précisent que les autorités désignées par les Parties contractantes peuvent accéder, par une interrogation automatisée ou non, :

- à l'ensemble des données enregistrées dans le SIS lors des contrôles de frontière et des vérifications et autres contrôles de police et de douane effectués à l'intérieur du pays conformément au droit national ;
- à la seule catégorie des signalements aux fins de non admission pour la délivrance des visas, des titres de séjour et l'administration des étrangers dans le cadre des dispositions de la Convention concernant la circulation des personnes.

La liste des autorités qui peuvent interroger directement les données intégrées dans le SIS doit être communiquée au Comité exécutif (article 101.4).

L'architecture du système d'information Schengen

Si plusieurs des articles du titre IV prescrivent le respect de telle ou telle mesure d'ordre technique, la description générale du système figure dans l'article 92.

Le système d'information Schengen (SIS) est composé d'une partie nationale (N.SIS) auprès de chacune des Parties contractantes et d'une fonction de support technique (C.SIS) créée et entretenue en commun dont la responsabilité est assumée par la République française.

La fonction de support technique, installée à Strasbourg, a pour objet de rendre matériellement identiques tous les N.SIS. Pour cela le C.SIS comprend un fichier de données qui assure l'identité des fichiers nationaux par la transmission en ligne d'informations.

La transmission de données est effectuée conformément aux protocoles et procédures établis en commun par les Parties contractantes pour la fonction de support technique.

L'article 118.4 précise les mesures de sécurité qui doivent être prises pour la fonction de support technique. Ces mesures sont identiques à celles requises pour chaque N.SIS (Article 118.1 à 3).

1.4. Les bureaux SIRENE

Les bureaux SIRENE (Supplément d'Informations Requis à l'Entrée Nationale) sont une création des Etats-parties non expressément prévue par la Convention.

Chargés de procéder dans chaque Etat Schengen, sur la base du SIS, à des échanges d'informations complémentaires, ils servent également d'intermédiaires lors des diverses consultations d'Etat à Etat sur la conduite à tenir en cas d'exécution d'un signalement.

Leurs missions et actions sont définies de manière concrète dans un manuel commun dit «manuel SIRENE». Pour l'essentiel, elles consistent en des consultations préalables à la création de signalements, des échanges d'informations et en la surveillance des signalements multiples et l'établissement d'ordres de priorité.

Chapitre 2. La protection des données à caractère personnel

2.1. Une loi et une autorité nationale de contrôle : conditions préalables à l'application de la Convention

Les Etats parties ont posé plusieurs conditions préalables à l'application sur leur territoire de la Convention. Le caractère impératif de leur respect est rappelé dans l'acte final.

Au nombre de ces conditions figure l'obligation pour chaque Etat-partie de se doter, avant toute transmission de données à caractère personnel, d'une autorité nationale de contrôle indépendante (articles 114 et 128) et d'une loi de protection des données.

Plus précisément, s'agissant du traitement automatisé ou non de données transmises en application de la Convention, la Convention comporte les prescriptions suivantes :

- a. Pour le traitement automatisé de données transmises en application du titre IV relatif au SIS :

Article 117

Chaque Partie contractante doit prendre au plus tard au moment de l'entrée en vigueur de la Convention les dispositions nationales nécessaires pour réaliser un niveau de protection des données à caractère personnel qui soit au moins égal à celui des principes découlant de la Convention du Conseil de l'Europe du 28 janvier 1981 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, ce dans le respect de la Recommandation R (87) 15 du 17 septembre 1987 du comité des ministres du Conseil de l'Europe visant à réglementer l'utilisation des données à caractère personnel dans le secteur de la police.

La transmission de données à caractère personnel ne peut avoir lieu que lorsque les dispositions de protection des données à caractère personnel sont entrées en vigueur sur le territoire des Parties contractantes concernées par la transmission.

- b. Pour le traitement automatisé d'autres données transmises en application de la Convention à l'exception de celles relatives aux demandes d'asile :

Article 126

Exigence, au moment de l'entrée en vigueur de la Convention, d'un niveau de protection des données à caractère personnel au moins égal à celui des principes découlant de la Convention du Conseil de l'Europe du 28 janvier 1981 sus-citée et transmission des données également subordonnée à l'effectivité de cette protection sur le territoire des Parties contractantes concernées par la transmission.

Article 129

Pour la transmission des seules données relatives à la coopération policière, les Parties contractantes doivent réaliser un niveau de protection des données à caractère personnel qui respecte les principes de la Recommandation R (87)15 du 17 septembre 1987 du Comité des ministres du Conseil de l'Europe déjà mentionnée.

- c. Pour les données transmises en application de la Convention provenant d'un fichier ou intégrées dans un fichier à l'exception de celles qui se rapportent aux demandes d'asile, au SIS ou à l'entraide judiciaire en matière pénale :

Article 127

Application des dispositions de l'article 126 et, pour la transmission de données relatives à la coopération policière, niveau de protection des données qui respecte les principes de la Recommandation R (87) sus-citée.

- d. Enfin, s'agissant des données transmises qui figurent dans des dossiers, seules s'appliquent, à une exception près, les dispositions spécifiques de protection des données de l'article 126.3 sous le contrôle, le cas échéant, de l'autorité nationale compétente (article 128.2).

2.2. Les champs d'application respectifs de la Convention et du droit national

La Convention opère, pour la protection des données à caractère personnel, une répartition complexe entre le champ d'application de ses dispositions et celui des droits nationaux des Etats-parties.

Les droits des personnes à l'égard du SIS

La règle peut s'énoncer ainsi : pour autant que la Convention ne prévoit pas de dispositions particulières, le droit de chaque Partie contractante est applicable.

La Convention précise la nature des droits qui sont reconnus aux personnes et les limites éventuelles qui y sont apportées. Sous réserve du respect de ces dispositions, les droits des personnes s'exercent dans le respect du droit national de chaque Etat-partie.

a. Droit d'accès et de communication (article 109)

Toute personne peut accéder aux informations la concernant intégrées dans le SIS. Pour cela elle peut former une demande auprès des instances compétentes de chacun des Etats-parties.

Si le droit national le prévoit, l'auteur de la demande peut se voir communiquer les informations qui le concernent. Toutefois en application du «principe de propriété des données», la communication est subordonnée au fait que l'Etat saisi qui n'est pas l'auteur de l'intégration donne préalablement à l'Etat signalant l'occasion de prendre position.

La communication des informations peut être refusée si elle peut nuire à l'exécution du signalement ou si elle s'avère nécessaire à la protection des droits et libertés d'autrui. Dans tous les cas, la communication est refusée si la personne est signalée aux fins de surveillance discrète.

b. Droit de rectification (article 110)

Toute personne peut, pour les données qui la concernent, faire rectifier celles qui sont entachées d'erreur de fait ou faire effacer celles qui sont entachées d'erreur de droit. Dans la pratique, l'exercice de ce droit est largement facilité par la communication des informations figurant dans le système.

c. Droit d'engager une action en rectification, en effacement, en information ou en indemnisation (article 111)

Toute personne doit pouvoir, sur le territoire de chaque Partie contractante, faire valoir ses droits devant une juridiction ou toute autre autorité compétente. Les décisions définitives sont exécutées par l'Etat-partie concerné.

d. Droit de demander une vérification des données (article 114.2)

Toute personne peut demander à une autorité nationale de contrôle de vérifier les données la concernant intégrées dans le SIS ainsi que l'utilisation qui en est faite. Si les données ont été intégrées par un autre Etat que celui auprès duquel la demande est introduite, le contrôle est effectué en étroite coordination avec l'autorité de contrôle de l'Etat signalant.

Si un état exhaustif des demandes introduites auprès des Etats Schengen pour l'exercice des droits mentionnés ci-dessus n'a pas encore été établi, il ressort des éléments d'information dont dispose l'ACC que, pour chaque Etat, le nombre de ces demandes varie entre un et quarante pour les deux années écoulées.

Le contrôle du système d'information Schengen

La Convention énonce les principes de protection des données qui, sans préjudice du droit national de chaque Partie contractante, sont applicables lors du traitement des données intégrées dans le SIS (article 104). Elle opère, pour le contrôle de leur respect, un partage entre l'Autorité de contrôle commune et les autorités nationale de contrôle (articles 114 et 115).

Les principes énumérés par la Convention sont les suivants.

a. Principe de finalité pour l'enregistrement des données et, sauf exceptions limitativement énumérées, pour leur utilisation: extradition, non-admission, personnes disparues, témoins, personnes citées ou condamnées, objets volés, personnes et véhicules sous surveillance discrète ou contrôle spécifique (articles 94 à 100 et 102 déjà cités).

b. Interdiction de traiter de données sensibles et énumération limitative des données enregistrées (article 94 déjà cité).

c. Définition des destinataires : accès limité aux autorités nationales compétentes dans certains domaines et pour le seul accomplissement de leurs missions (article 101 déjà cité).

d. Interdiction de copier les signalements d'une autre Partie contractante dans un fichier national et limitation des duplications à des fins techniques (article 102).

e. Obligation d'enregistrement de toute dixième transmission de données aux fins de contrôle de l'admissibilité (article 103).

f. Fixation d'une durée de conservation des données (articles 112 et 113).

g. Obligation de conserver les données effacées durant une année dans la fonction de support technique aux fins de contrôle a posteriori de leur exactitude et de la licéité de leur intégration (article 113.2).

S'agissant du contrôle du système, la Convention précise que chaque Etat-partie doit charger une autorité nationale de contrôler, de manière indépendante et dans le respect du droit national (article 114), le fichier de la partie nationale du système d'information (N.SIS). Il revient à ces autorités de vérifier le respect des dispositions de protection des données prévues par la Convention et celles qui s'y ajoutent le cas échéant en vertu du droit national.

En revanche, le contrôle de la fonction de support technique (C.SIS) est confié à l'Autorité de contrôle commune qui doit agir dans le respect de la Convention de Schengen, de la Convention du Conseil de l'Europe sur la protection des données, de la Recommandation du Conseil de l'Europe pour les données dans le secteur de la police et conformément au droit français.

Les échanges d'informations hors le SIS

Le titre VI (articles 126 et suivants) de la Convention intitulé «protection des données à caractère personnel» est consacré aux règles applicables aux échanges d'informations qui ne donnent pas lieu à un enregistrement dans le SIS mais interviennent pour l'application de la Convention (infra 2.1. b et c).

Les principes retenus (finalité, limitation des destinataires, exactitude des données ...) sont applicables sans préjudice des dispositions du droit national de protection des données qui régit notamment l'exercice des droits des personnes concernées.

Le contrôle du respect des règles énoncées par la Convention incombe aux autorités nationales.

L'ACC a un rôle résiduel : elle peut, à la demande des Parties contractantes émettre un avis sur les difficultés d'application et d'interprétation que soulèvent ces règles.

Chapitre 3. L'Autorité de contrôle commune et les conditions de son indépendance

3.1. Composition de l'Autorité de contrôle commune

L'article 115.1 de la Convention précise que l'Autorité de contrôle commune (ACC) est composée de deux représentants de chaque autorité nationale de contrôle.

Le choix de ses représentants au sein de l'ACC revient à chaque autorité nationale qui, en la personne de son président ou de son directeur, procède à leur désignation auprès du secrétariat de l'ACC et de son président. L'ACC prend acte des désignations effectuées.

Les autorités nationales de contrôle n'étant pas composées sur un modèle unique (certaines sont des organismes collégiaux, d'autres non), leurs représentants sont, selon le cas, membre du collège, commissaire ou directeur, responsable ou agent d'un service ou personnalité extérieure.

La Convention ne prescrivant pas de durée pour le mandat des membres de l'ACC, l'appréciation de celle-ci revient à chaque autorité nationale.

L'Autorité de contrôle commune a été officiellement installée après la mise en application de la Convention le 26 mars 1995.

Toutefois, sous l'impulsion de M. *Faber*, commissaire à la protection des données du Luxembourg qui fut son premier président, une Autorité de contrôle commune provisoire (ACCP) a été mise en place dès le mois de juin 1992 avec l'accord des ministres Schengen.

A cette époque, certains Etats-parties, après les tests techniques réalisés avec des données fictives, envisageaient d'intégrer progressivement dans le SIS des données à caractère personnel réelles. Dès lors, l'utilité d'une concertation avec l'organisme commun chargé du contrôle du respect des règles de protection des données devenait incontestable.

L'ACCP, composée d'un ou deux représentants des autorités nationales de contrôle des cinq Etats à l'origine des accords et d'un ou deux experts indépendants désignés par les Etats adhérents sur le territoire desquels la Convention n'était pas encore applicable adopta un règlement intérieur provisoire qui prescrivait la règle du consensus pour l'accomplissement de ses missions. Elle élaborait un questionnaire sur la nature des règles de protection des données applicables dans chacun des Etats Schengen au regard de la Convention et tout particulièrement du SIS et procéda à une première visite de la fonction de support technique à Strasbourg.

Elle se réunit à douze reprises entre le 29 juin 1992 et le 22 février 1995 dans les locaux du secrétariat de Schengen à Bruxelles et une fois à Strasbourg les 15 et 16 mars 1994.

Elle joua un rôle de pionnier qui rendit plus aisée la tâche de l'ACC lorsqu'elle fut officiellement installée. Il est fait référence à ses travaux lors de la présentation de ceux de l'ACC qui les ont complétés.

Peu après sa constitution, l'Autorité de contrôle commune a tenu, entre le 17 mai et le 14 décembre 1995, cinq réunions sous la présidence de M. *Von Pommer Esche*, Allemagne, président de l'ACCP, afin notamment d'élaborer son règlement intérieur définitif. Elle a procédé le 14 décembre 1995 à l'élection, pour un an renouvelable, de son président, M. *Türk*, France, sénateur, membre de la Commission nationale de l'informatique et des libertés et de son vice-président, M. *Labescat*, Portugal, avocat, membre de la Commission nationale de protection des données.

M. *Türk*, président et M. *Labescat*, vice-président ont été réélus pour un an le 5 décembre 1996.

L'ACC s'est réunie neuf fois en 1996 et à trois reprises depuis le début de l'année 1997, tenant sa première session officielle à Strasbourg les 10 et 11 février 1997.

Elle a institué deux groupes de travail qui se sont réunis, pour le premier à deux reprises à La Haye et Paris, et pour le second et à quatre reprises à Bruxelles et Madrid.

3.2. Les missions de l'ACC

Si la mission principale de l'ACC est de contrôler la fonction de support technique du SIS, mission qu'elle a seule le pouvoir d'accomplir (article 115.2), un rôle de conseil et d'harmonisation des pratiques ou des doctrines nationales lui est également confié.

La Convention d'application de l'Accord de Schengen précise ses missions à l'égard du SIS dans les articles suivants.

Article 106.3 : l'ACC rend un avis en cas de désaccord entre deux Parties sur l'existence d'une erreur de droit ou de fait entachant un signalement. Il s'agit d'un cas obligatoire de saisine par la Partie qui n'est pas à l'origine du signalement.

Article 115.3 :

- l'ACC analyse les difficultés d'application ou d'interprétation pouvant survenir lors de l'exploitation du SIS;
- l'ACC étudie les problèmes pouvant se poser lors de l'exercice du contrôle indépendant effectué par les autorités de contrôle nationales des Parties contractantes ;
- l'ACC étudie les problèmes pouvant se poser à l'occasion de l'exercice du droit d'accès au système ;
- de manière plus générale, l'ACC élabore des propositions harmonisées en vue de trouver des solutions aux problèmes existants.

Article 115.4 : l'ACC établit des rapports qui sont transmis aux instances auxquelles les autorités de contrôle nationales transmettent leurs rapports.

Article 118.2 : l'ACC reçoit communication des mesures particulières prises par chaque Partie contractante en vue d'assurer la protection des données lors de la transmission de données à des services situés en dehors des territoires des Parties contractantes.

S'agissant des échanges d'informations hors SIS :

Article 126.3.f) : l'ACC peut, à la demande des Parties contractantes, émettre un avis sur les difficultés d'application et d'interprétation de l'article 126 relatif au traitement des données transmises, hors SIS, en application de la Convention.

Article 127 : l'ACC peut, dans les conditions et selon les modalités prévues par l'article 126, émettre un avis en cas de transmission de données provenant d'un fichier non automatisé et d'intégration de données dans un tel fichier.

Dans les faits, entre décembre 1995 et mars 1997, l'ACC a concentré ses efforts sur l'obtention des garanties de son indépendance ainsi que sur deux missions qui sont apparues prioritaires (coopération entre autorités nationales de contrôle pour l'exercice du droit d'accès des personnes au SIS et contrôle de la fonction de support technique).

3.3. Les conditions de l'indépendance

Si l'article 115 n'indique pas expressément que l'ACC est une autorité indépendante, ses membres sont les représentants d'autorités nationales chargées d'exercer, dans chaque Etat-partie, un contrôle indépendant du N.SIS. De surcroît, on peut rappeler que dans la Recommandation R(87)15 du 17 septembre 1987 visant à réglementer l'utilisation de données à caractère personnel dans le secteur de la police, explicitement mentionnée par l'article 115, il est souligné (point 1.1) que l'autorité de contrôle chargée de veiller au respect des principes énoncés doit être indépendante.

La nécessité d'être indépendante est immédiatement apparue à l'ACC, ce d'autant que lors de la mise en place de l'ACCP, certains choix, tels celui d'élire un président plutôt que d'adopter la règle instituée entre les Etats-parties d'une présidence tournante tous les six mois, furent discutés par ces derniers.

Les conditions de son indépendance et, par voie de conséquence de sa crédibilité et de celle des Etats Schengen, ont donc été clairement exprimées par l'ACC dès son installation.

Au nombre de ces conditions comptent tout particulièrement l'adoption d'un règlement intérieur, l'obtention d'une ligne budgétaire autonome avec, en contrepartie l'élaboration d'un rapport d'activité.

L'adoption d'un règlement intérieur

Lors de l'élaboration de son règlement intérieur, l'ACC a consacré la règle de l'élection de son président et de son vice-président, instauré des règles de quorum et de majorité pour l'adoption de ses actes et précisé que ses membres, les observateurs, les experts et les membres du secrétariat étaient tenus de respecter la confidentialité.

Elle a tranché diverses questions relatives à ses missions, aux conditions nécessaires pour être membre ou observateur, à la publicité de ses actes et au recours à des experts en tant que de besoin pour l'exercice de ses missions.

Dégager ces éléments de doctrine s'est avéré essentiel par la suite.

S'agissant de ses missions, l'ACC a précisé qu'elle pouvait remplir, outre les missions qui lui sont dévolues par la Convention, d'autres missions relatives à la protection des données à caractère personnel liées à l'application de la Convention.

Elle a rappelé qu'elle pouvait se saisir d'office ou intervenir à la demande d'une autorité de contrôle nationale, d'une Partie contractante ou d'une instance du système Schengen conformément aux dispositions de la Convention.

L'ACC a ensuite, à l'issue d'une analyse juridique de la Convention, précisé que seuls pouvaient être considérés comme membres à part entière les représentants des autorités nationales de contrôle des Etats-parties sur le territoire desquels la Convention était applicable, les ratifications ayant été opérées et les conditions préalables remplies.

Elle a en revanche prévu d'accueillir, avec le statut d'observateur sans voie délibérative, les représentants des autorités nationales de contrôle ou experts indépendants des Parties contractantes sur le territoire desquelles la Convention n'était pas encore mise en vigueur.

Ainsi sont membres de l'ACC depuis son installation officielle, les représentants des autorités nationales de contrôle de l'Allemagne, la Belgique, l'Espagne, la France, le Luxembourg, les Pays-Bas et le Portugal.

Ont le statut d'observateur :

- les représentants de l'Italie qui, les instruments de ratifications ayant, à deux exceptions près, été déposés, ne disposait pas d'une loi de protection des données et d'une autorité nationale de contrôle. Cette situation vient de changer avec l'entrée en vigueur le 9 janvier 1997 de la loi n° 675 du 31 décembre 1996 sur la protection des personnes et autres sujets à l'égard du traitement de données à caractère personnel et la mise en place le 5 mars 1997 de l'autorité nationale de contrôle;
- les représentants de l'autorité nationale de contrôle autrichienne, pays pour lequel le dépôt par tous les Etats-parties des instruments de ratification n'était pas effectué. Cette situation devrait changer à bref délai;
- les représentants de la Grèce qui, le processus de ratification n'étant pas achevé, ne disposait pas de loi de protection des données. Cette situation vient de changer avec le vote de la loi sur la protection de l'individu à l'égard du traitement des données à caractère personnel du 20 mars 1997.

Sont accueillis depuis le mois de mars 1997 en qualité d'observateurs, les représentants des autorités nationales de contrôle du Danemark, de la Finlande et de la Suède.

Auront également très prochainement le statut d'observateur, les représentants de la Norvège et de l'Islande.

L'ACC a en effet décidé d'amender son règlement intérieur avant la fin du premier semestre de l'année 1997 de façon à modifier les conditions nécessaires pour obtenir la statut d'observateur.

S'agissant de la publicité de ses actes, l'ACC a considéré que ses réunions devraient se tenir à huis clos mais a décidé de déterminer au cas par cas les destinataires de ses actes et de se prononcer sur la publicité éventuelle de ces derniers, sans préjudice de l'article 115.4 qui prescrit que ses rapports sont transmis aux instances auxquelles les autorités de contrôle nationales transmettent leurs rapports. Cette décision lui permet notamment de rendre les diverses instances Schengen destinataires de ses actes.

Enfin, l'ACC a précisé qu'elle pourrait créer des groupes de travail et faire appel à des experts. Cette disposition a été utilisée notamment lors du contrôle du C.SIS en octobre 1996.

L'obtention d'une ligne budgétaire propre

L'ACC a dès le 18 octobre 1995 demandé, pour l'année 1996, l'attribution d'une ligne budgétaire propre qui lui permette de remplir en toute indépendance les missions qui lui incombent. Sa demande examinée un mois après par le Groupe central n'a pas reçu d'écho favorable. Aussi a-t-elle réitéré le 14 décembre avec fermeté sa demande au Groupe central ainsi qu'au Comité exécutif.

L'obtention d'une ligne budgétaire s'est rapidement révélée être un enjeu de principe autour duquel les positions de l'ACC et des Etats Schengen, tout particulièrement de la France et l'Allemagne, se sont cristallisées pendant toute l'année 1996.

Dans une note du 4 avril 1996 relative à ses missions, à son programme d'action, l'ACC a élaboré un projet de budget à l'intention du Comité exécutif et du Groupe central.

Dans ce document, l'ACC, rappelant que les frais de déplacements de ses membres pour les réunions de travail à Bruxelles continueraient à être pris en charge par les autorités nationales de contrôle, a demandé que lui soient garantis :

- la mise à disposition d'un secrétariat notamment pour tenir le registre de ses actes, de salles de réunion et d'un service de traduction et d'interprétation dans toutes les langues des Etats Schengen ;
- des crédits suffisants pour faire appel à des experts en tant que de besoin pour l'exercice de ses missions notamment dans le cadre d'une consultation pour avis ou d'un contrôle ;
- des crédits suffisants pour élaborer un rapport annuel d'activité qui rendrait compte de l'emploi de ses ressources ;
- le remboursement des frais de déplacement de ses membres pour la tenue d'une session annuelle à Strasbourg et, le cas échéant, d'autres missions particulières.

Le montant total du budget demandé s'élevait à 4.250.000 BEF.

Examiné par différentes instances Schengen entre le 3 juillet 1996 et le 28 janvier 1997, le projet de budget de l'ACC, après un parcours égrené d'échanges de lettres, de discussions, de réunions bilatérales officieuses et de rencontres officielles a enfin été accepté dans son principe et, en pratique, adopté par le Groupe central avec quelques modifications dont certaines en accord avec l'ACC, telle la suppression du poste relatif au secrétariat. Il est à noter que l'ACC a reçu l'assurance, avant de donner son accord, que les documents nécessaires à l'exercice de ses missions seraient traduits dans des délais satisfaisants.

Cette décision a été annoncée à l'ACC le 10 février 1997, veille de sa première session officielle à Strasbourg et le projet de budget révisé d'un montant de 2.839.950 BEF, soumis à l'approbation définitive du Comité exécutif par procédure écrite en mars 1997, lui a été transmis.

Le président de l'ACC a informé le Groupe central le 17 février de la vive surprise des membres de l'Autorité devant la suppression du poste relatif à la session annuelle à Strasbourg et indiqué qu'ils considéraient que ce fait pouvait compromettre l'accomplissement des missions de l'ACC et le principe de son indépendance. Il a néanmoins précisé que l'ACC s'accommoderait provisoirement de ce budget, étant entendu que celui-ci ferait l'objet d'une évaluation en fin d'exercice afin notamment de tenir compte des possibilités d'adaptation des budgets nationaux des autorités de contrôle pour prendre en charge, en sus des déplacements de leurs représentants pour les réunions de travail à Bruxelles, les frais de missions particulières décidées par l'ACC. Il a également été précisé que ce budget devrait être revu de façon à tenir compte de l'élargissement de l'ACC à cinq nouveaux pays.

L'élaboration d'un rapport d'activité

Bien que l'obligation ne lui en soit pas faite par la Convention, l'ACC a décidé en avril 1996 d'élaborer un rapport annuel d'activité. Elle a tenu, par un tel rapport, à rendre compte, de manière transparente, de l'accomplissement de ses missions et de l'utilisation de son budget.

Ce premier rapport s'avère être bi-annuel en raison des difficultés diverses et notamment budgétaires que l'ACC a rencontrées depuis son installation officielle. Il deviendra, pour l'avenir, annuel.

Au premier chef, les destinataires de ce rapport sont le Comité exécutif et le Groupe central ainsi que, conformément à l'article 115.4, les autorités nationales de contrôle qui ont pour charge de le remettre à leurs instances nationales et de le rendre public selon les voies suivies pour leurs propres rapports.

L'information sur le fonctionnement de la Convention

A plusieurs reprises, dès 1995 et avec plus d'insistance avant la préparation du contrôle du C.SIS, l'ACC a demandé que lui soient communiqués, pour l'exercice de ses missions, divers documents indispensables à sa connaissance de l'application de la Convention et du fonctionnement du SIS. Elle a fréquemment rencontré des difficultés pour les obtenir en temps utile et n'a pu jusqu'à présent, en dépit de ses réclamations être rendue destinataire, au fur et à mesure de leur élaboration, de certains d'entre eux et notamment de ceux émanant du Comité d'orientation et du groupe de travail permanent (GTP).

Chapitre 4. Les missions entreprises

La Convention prévoit que l'ACC rend des avis ou établit des rapports. Depuis l'entrée en application de la Convention, l'ACC a examiné 180 notes, adopté 6 avis et un rapport, réserve faite du rapport d'activité.

4.1. Les missions achevées

4.1.1. Le comparatif des règles de protection des données applicables dans les Etats Schengen

L'élaboration d'un questionnaire permettant de connaître avec le plus de précisions possibles la situation de chaque Etat Schengen au regard des dispositions de la Convention en matière de protection des données, a été décidée par l'ACCP en 1993 (questionnaire SCH/Aut-cont (94) 16 et document de synthèse SCH/Aut-cont (96) 19).

Ce document a été enrichi par l'ACC sur certains points, tel celui des conditions d'exercice du droit d'accès dans chaque Etat-partie.

Instrument pratique de droit comparé, le questionnaire porte sur les textes internationaux et nationaux applicables en matière de protection des données et, plus généralement de droits et libertés des personnes. Il s'articule autour des thèmes plus spécifiques suivants : transparence (déclaration de création du N.SIS, publicité), fondement juridique du bureau SIRENE et instance ayant la compétence centrale pour le N.SIS, mécanismes de contrôle (composition et compétences de l'autorité nationale de contrôle), droits des personnes à l'égard du traitement de leurs données (droit d'accès, de rectification, d'effacement, d'indemnisation, voies de recours), mesures de sécurité prises pour le N.SIS, fichiers nationaux utilisés pour alimenter le SIS et autorités habilitées à le consulter directement.

Il est destiné à être renseigné par chaque délégation membre de l'ACC ou observateur au sein de l'Autorité. L'Italie et les pays nordiques se verront demander de répondre aux questions qu'il comporte au cours de l'année 1997, ainsi que la Grèce, ultérieurement, sur la base de sa récente loi de protection des données.

4.1.2. L'examen du fondement juridique des bureaux SIRENE et du contenu du manuel SIRENE

Le fondement juridique des bureaux SIRENE

L'absence, dans la Convention, de fondement juridique spécifique pour les bureaux SIRENE a conduit l'ACCP à demander à chacune de ses délégations de préciser si son bureau national avait été désigné, sur le fondement de l'article 108 de la Convention pour exercer la compétence centrale pour le N.SIS, ou si un texte national autonome l'avait créé et, dans cette hypothèse, d'indiquer le lien qui l'unissait à l'instance centrale.

L'ACCP a pris acte que, à l'exception de la Belgique, les Etats appliquant la Convention (Allemagne, Espagne, France, Luxembourg, Pays-Bas, Portugal) n'avaient pas attribué à leur bureau SIRENE, sur le fondement de l'article 108, la compétence centrale pour le N.SIS, mais l'avaient créé sur le fondement d'un texte national (France, Pays-Bas, Portugal) ou considéraient que divers textes nationaux sur la police ou en relation avec la Convention de Schengen suffisaient à asseoir son existence juridique (Allemagne, Espagne, Luxembourg).

Elle a constaté qu'à l'exception de la Belgique (rattachement du bureau SIRENE, instance ayant la compétence centrale pour le N.SIS, au ministère de la Justice) et du Portugal (rattachement de l'instance centrale, distincte du bureau SIRENE, au service des étrangers et des frontières du ministère de l'Intérieur), les autres Etats Schengen avaient confié la compétence centrale du N.SIS à leurs services de police ou de gendarmerie et rattaché leur bureau SIRENE à ces services.

L'ACCP a souligné auprès des Etats-parties à la Convention de Schengen l'intérêt qui se serait attaché, pour des raisons de transparence, à prévoir la création et les attributions des bureaux SIRENE dans le texte même de la Convention.

Le contenu du manuel SIRENE

L'ACCP a examiné à plusieurs reprises en 1993 et 1994 le contenu du projet de manuel SIRENE.

Ce manuel commun aux Etats Schengen décrit la procédure devant permettre de transmettre, à un utilisateur ayant eu une réponse positive à une interrogation du SIS, les informations complémentaires nécessaires à son action.

4.1.3. La coopération entre les autorités de contrôle nationales

L'avis sur l'exercice du droit d'accès et la coopération pour la vérification des données

L'ACC a, en vertu de l'article 115.3, adopté un avis sur les principes de la coopération entre autorités nationales de contrôle sur le fondement de l'article 114.2.

Cet avis a été l'occasion d'examiner la coordination entre les dispositions relatives à l'exercice du droit de vérification des données intégrées dans le SIS et de l'utilisation qui en est faite et les dispositions de l'article 109 relatif au droit d'accès.

Cet avis a été transmis au Comité exécutif et au Groupe central ainsi qu'aux autorités nationales de contrôle. Ces dernières se sont vu proposer de constituer un annuaire de correspondants destiné à faciliter la mise en oeuvre de la coopération.

Première autorité nationale à avoir été saisie, le jour même de l'entrée en application de la Convention, d'une demande de droit d'accès au SIS et de plusieurs autres par la suite, la Commission nationale de l'informatique et des libertés française avait appelé l'attention de l'ACC sur les difficultés rencontrées pour vérifier de manière efficace, dans les N.SIS au regard de la Convention, la pertinence de l'enregistrement de données par un autre Etat-partie.

L'ACC a, en conséquence, créé un groupe de travail composé des représentants allemands, belges, néerlandais et français et l'a chargé d'examiner les problèmes posés et de proposer une solution harmonisée pour les résoudre. Le groupe de travail s'est réuni informellement à deux reprises et a soumis à l'Autorité de contrôle commune un projet d'avis le 21 juin 1996.

Adopté le 26 novembre 1996, cet avis rappelle en préliminaire que la Convention distingue dans ses articles 109 et 114 respectivement le droit d'accès et de communication et le droit de demander une vérification des données et de l'utilisation qui en est faite.

Le droit applicable étant le droit national de la Partie contractante saisie, l'autorité compétente pour traiter ces demandes est :

- pour l'accès et la communication, le responsable du fichier pour les pays de droit d'accès direct et l'autorité de contrôle pour les pays de droit d'accès indirect ;
- pour la vérification des données et de leur utilisation, dans les deux cas, l'autorité de contrôle.

Lorsque les données ont été intégrées par une autre Partie contractante que celle qui est saisie, l'article 109 subordonne la communication au fait que la Partie signalante ait été en mesure de prendre position et l'article 114 prévoit que la vérification est réalisée en étroite coordination avec l'autorité de contrôle de la Partie signalante.

La coopération entre autorités de contrôle n'est donc prévue expressément que dans le cadre d'une demande de vérification et l'article 114.2 ne prévoit pas de communication à la personne concernée.

L'avis comporte, après ces rappels, les considérations suivantes.

L'autorité de contrôle nationale saisie d'une demande de droit d'accès et de communication devant entraîner des vérifications (droit français, belge, ...) ou directement saisie d'une demande de vérification peut, lorsque les données personnelles ont été introduites par une autre Partie contractante, requérir l'autorité de contrôle de cette Partie afin de procéder au contrôle des données en étroite coordination avec elle. En aucun cas, une telle demande de coopération ne dessaisit l'autorité de contrôle requérante ni ne modifie le droit national applicable au traitement de la demande.

L'autorité de contrôle nationale requise procède aux vérifications qui lui sont demandées par l'autorité requérante. Cette dernière fournit à l'autorité requise tous éléments, en sa possession, utiles à l'exercice de ses vérifications.

A l'issue de ses vérifications, l'autorité de contrôle requise transmet à l'autorité de contrôle requérante l'ensemble des informations recueillies au cours de ses investigations.

Si l'autorité de contrôle requérante a visé dans sa demande de coopération fondée sur l'article 114.2, l'article 109 qui prévoit la communication éventuelle au demandeur des informations le concernant enregistrées dans le SIS, l'autorité requise joint, dans la mesure du possible, l'avis de son gouvernement sur la communicabilité de ces informations.

4.1.4. Le contrôle du C.SIS

La visite sur place de l'ACCP et l'avis du 18 mai 1994

Le 16 mars 1994, l'ACCP a procédé à une visite sur place du site hébergeant le C.SIS à Strasbourg. A cette époque, le système d'information Schengen n'était pas encore opérationnel et son fonctionnement n'a pas été contrôlé. Seules les installations, le bâtiment et les ordinateurs ont fait l'objet d'une vérification.

Deux rapports ont été établis par les délégations néerlandaise et française à l'issue de cette visite qui portaient sur :

- la protection physique (bâtiments et site, installations, protection physique des accès, protection contre l'incendie, l'inondation, le vol et le vandalisme, organisation, procédure et instructions) ;
- la protection opérationnelle (mesures et procédures destinées à garantir l'intégrité des données et de contrôler l'accès aux fichiers et réseaux) ;
- la protection organisationnelle (gestion, séparation des fonctions, procédures, responsabilités et compétences) ;
- la protection de la continuité du traitement des données (mesures et procédures pour garantir un bon déroulement des processus de traitement et prévention des dommages qui pourraient résulter d'un mauvais déroulement des processus).

Après l'examen des rapports, l'ACCP a estimé que, dans leur ensemble, les mesures prises et les procédures adoptées étaient, tout particulièrement pour la protection physique, satisfaisantes au regard des prescriptions de l'article 118.1 de la Convention.

Toutefois, elle a adopté, dans un avis du 18 mai 1994, trois recommandations à l'attention du Groupe central afin qu'il soit veillé lors de la mise en application de la Convention :

- à la mise en place d'une séparation physique entre les installations du C.SIS et celles du ministère de l'Intérieur français hébergées sur le même site ;
- à la conservation et au transport en toute sécurité des back-up de toutes les données ;
- à l'accroissement de la fiabilité des liaisons entre le C.SIS et les N.SIS afin d'exclure ou de réduire très fortement le risque d'interruption des lignes.

L'avis de l'ACCP adressé au Groupe central a été transmis pour examen approfondi au Comité d'orientation dont les conclusions, adoptées par le Groupe central, ont été en retour portées à la connaissance de l'ACCP le 13 septembre 1994.

De ces conclusions, il ressortait qu'il était satisfait aux exigences de l'ACCP grâce aux mesures appropriées déjà mises en oeuvre et qu'il serait tenu le plus grand compte de ces exigences dans le cadre des développements techniques actuels et futurs.

Le contrôle de l'ACC, la visite sur place du 11 février 1997 et l'avis du 27 mars 1997

L'ACC a décidé le 26 mars 1996 d'effectuer, conformément à l'article 115.2, un contrôle du C.SIS.

Elle a institué à cet effet le 21 juin 1996 un groupe de travail chargé d'effectuer le contrôle et, au préalable, :

- d'étudier les documents techniques pertinents relatifs au C.SIS;
- de définir les investigations à mener ;
- de déterminer les compétences techniques requises des experts.

Ce groupe, composé, sous la présidence de M. *Faber*, Luxembourg, de trois autres membres de l'ACC (M. *Von Pommer Esche*, Allemagne, M. *Cueva*, Espagne, Mme *Carblanc*, France) et de trois experts des autorités nationales de contrôle (M. *Lopez* et M. *Perez*, Espagne, M. *Ngo*, France) s'est réuni le 6 septembre au secrétariat général de Schengen et a soumis ses propositions d'investigations à l'ACC qui les a adoptées le 12 septembre. Il a tenu une deuxième réunion au secrétariat de Schengen le 2 octobre afin de procéder à la répartition entre les experts et les autres membres du groupe des investigations à mener.

Le responsable du C.SIS et le Groupe central ont été informés de la composition définitive du groupe de contrôle le 3 octobre et un questionnaire documentaire relatif au C.SIS leur a été transmis le même jour.

Le contrôle a été effectué dans la semaine du 7 octobre. Il a pris fin le 10 sur la demande des autorités françaises qui ont demandé aux experts du groupe de cesser leurs investigations, seuls les membres de l'ACC étant, selon eux, habilités à y procéder. Cette décision a suscité une réaction immédiate extrêmement vive du président de l'ACC et de l'ensemble de ses membres. Cet incident a été à l'origine de plusieurs rencontres entre le Groupe central et l'ACC pour éviter le renouvellement de tels faits et, plus largement, évoquer les problèmes rencontrés par l'ACC pour obtenir une ligne budgétaire propre et exercer ses missions dans des conditions satisfaisantes (voir 5.1).

Sur le fond, pour réaliser le contrôle, le groupe a adopté la méthodologie suivante :

- établissement de listes de vérification provisoires ;
- élaboration d'un questionnaire pour obtenir des informations générales sur le système et ses composants, sa documentation, l'organisation et la composition de l'équipe du support technique (équipe d'exploitation du C.SIS);
- adaptation des listes de vérification aux caractéristiques spécifiques du C.SIS sur la base des réponses au questionnaire et de la documentation mise à disposition sur place.

L'évaluation à laquelle le groupe a procédé n'a pu être complète en raison du grand nombre de documents à vérifier dans un délai très court, de l'impossibilité d'emporter des copies de ces documents pour les étudier à l'extérieur du centre et de la fin prématurée du contrôle. Son rapport n'a donc porté que sur les aspects qui avaient pu faire l'objet d'une vérification et d'un contrôle suffisants pour permettre au regard de la Convention et notamment de son article 118, une appréciation fondée.

Les contrôles ont porté sur les points ci-après.

a. Contrôles généraux pour déterminer si l'unité de support du C.SIS a adopté, utilise et suit des méthodes et procédures appropriées afin que ses ressources en matière de technologie de l'information offrent des garanties raisonnables sur le plan de la sécurité:

- gestion et organisation
- structure organisationnelle et séparation des fonctions
- normes, règles et procédures
- logiciel des systèmes
- exploitation des équipements
- sécurité logique au niveau du système d'exploitation, du système de communication, du système de gestion de la base de données (SGBD)
- système d'audit du système d'exploitation, du système de communication et du SGBD
- sécurité physique (sécurité du périmètre et contrôle d'accès au site et aux bureaux, contrôle de l'accès physique aux équipements et aux équipements de communication)

b. Contrôles spécifiques pour vérifier que le fichier C.SIS et le mode de fonctionnement de l'unité de support technique qui assure sa gestion sont conformes aux dispositions de la Convention:

- intégrité des fichiers C.SIS et N.SIS (article 92.2)

- contenu (données intégrées dans la base de données, autorités qui les introduisent, identification univoque, indicateurs de validité, dates existantes)
- effacement automatique de données à caractère personnel (112.3)
- Etats interconnectés (articles 117 et 118.1.f)
- supports informatiques amovibles (stockage, étiquetage, inventaire, déplacement sur le lieu de stockage et hors du périmètre contrôlé, effacement des supports réutilisables, évacuation des supports non réutilisables)
- introduction des données (article 118.1. c et g)
- transport (article 118.1. h)

L'évaluation de ces contrôles généraux et spécifiques a conduit le groupe de contrôle à émettre plusieurs recommandations.

Le rapport du groupe a été examiné par l'ACC le 8 novembre et adopté le 5 décembre 1996 puis a été transmis au Groupe central et aux autorités françaises responsables de la fonction de support technique en les invitant à faire connaître leurs observations.

Le 11 février 1997, l'ACC a tenu sa session annuelle à Strasbourg et s'est rendue sur le site du C.SIS afin notamment de permettre à tous ses membres de prendre connaissance des modalités de fonctionnement du C.SIS et de procéder à un échange d'informations avec les représentants du Groupe central et les responsables de la fonction de support technique.

Au regard des diverses constatations effectuées et après avoir eu connaissance des observations des Etats Schengen, l'ACC a adopté le 27 mars 1997 le rapport définitif de contrôle.

Elle a considéré que la Convention était respectée sur différents points et notamment les suivants :

- les mesures de sécurité prises pour protéger les bâtiments abritant le C.SIS sont satisfaisantes ;
- la base de données ne contient que des données introduites par les Parties contractantes conformément aux articles 92.3 et 113.2 ;
- la base de données ne contient pas d'autres données à caractère personnel que celles prévues par l'article 94.3 de la Convention ;
- l'utilisation des indicateurs de validité est conforme à l'article 94.4.

Elle a en revanche estimé que les cinq points suivant justifiaient d'être mis en évidence et assortis de propositions de recommandations.

1. Les fichiers des Parties contractantes à la Convention ne sont pas identiques. Un nombre important de différences ont été constatées entre les fichiers de la France et du Luxembourg et ceux des autres pays ; ces différences remontaient au mois d'avril 1996 et, six mois plus tard n'étaient toujours pas complètement rectifiées.

La procédure de détection des différences actuellement appliquée est inappropriée : sa fréquence (tous les six mois environ) et sa durée (plusieurs mois) ne permettent pas de détecter et de rectifier rapidement les différences existant entre les fichiers.

Les explications fournies pour justifier les différences mises en évidence par la procédure de comparaison des bases de données (différences au niveau de la conception des bases de données) impliqueraient le non-respect systématique (en raison de la conception) des dispositions de l'article 92.2 ; dans ce cas, en effet, les fichiers des Parties contractantes ne pourraient jamais être «matériellement identiques» comme l'exige cet article.

2. Il a été constaté qu'en l'absence d'audit extérieur évaluant le niveau requis de sécurité pour le système informatique, les responsables de la fonction de support technique ont décidé d'adopter un certain niveau de sécurité ; que pour autant les mesures techniques requises pour garantir ce niveau de sécurité n'étaient pas toujours mises en oeuvre et que les règles préétablies étaient insuffisamment précises et insuffisamment diffusées.

3. Trop de personnes bénéficient d'un profil maximum (super utilisateur) leur permettant d'accéder et de modifier le contenu de n'importe quel fichier du système informatique (système d'exploitation, base de données et réseau) et d'inhiber toute trace de leur action.

4. Les fonctions de traçage permettant de vérifier a posteriori les actions entreprises par les différents utilisateurs, quel que soit leur profil (date, heure, terminal, identifiant de l'utilisateur, type d'action) ne sont pas mises en oeuvre de manière satisfaisante.

5. Il a été constaté une sécurité insuffisante dans la gestion et le transport des supports magnétiques où sont conservées les données du SIS.

Aussi, l'ACC a-t-elle fait les recommandations suivantes.

1. Procéder à une analyse complète des différences détectées entre les fichiers des N.SIS et le C.SIS et proposer des actions permettant d'éliminer rapidement ces différences afin d'éviter qu'elles ne se reproduisent à l'avenir.

Modifier la procédure de comparaison des fichiers de telle sorte que les différences que peut présenter le contenu des fichiers nationaux puissent être détectées et corrigées rapidement.

2. Faire procéder à une certification ITSEM/ITSEC et appliquer les mesures de sécurité préconisées ; à tout le moins, garantir au minimum, le niveau de sécurité prévu.

3. Limiter l'accès privilégié au système au strict minimum, un compte «super-utilisateur» permettant d'effectuer tout type d'opérations sur les données de la base, sans aucune restriction.

4. Activer systématiquement les fonctions de traçage permettant de vérifier a posteriori toutes les opérations effectuées sur le C.SIS.

5. Recourir de manière systématique à des méthodes de cryptage lorsque les données doivent être conservées sur supports magnétiques.

Enfin, l'article 118 étant applicable à chaque N.SIS et au C.SIS pris séparément, l'ACC a insisté sur la nécessité, pour porter une appréciation globale pertinente du respect par l'ensemble des Etats Schengen des prescriptions de la Convention relatives au SIS, de compléter le contrôle du C.SIS par un contrôle de chaque N.SIS réalisé sur des bases techniques identiques.

4.1.5. L'avis sur le projet pilote relatif aux véhicules volés

Le Groupe central a transmis à l'ACC le 10 février 1997 une demande d'avis émanant du groupe de travail I «police et sécurité» relative à la participation des pays non intégrés dans le SIS à un projet pilote en matière de vol de véhicules.

Après avoir noté que ce projet tendait à permettre aux pays non intégrés dans le SIS d'interroger celui-ci par le biais de leurs officiers de liaison, l'ACC a demandé des informations complémentaires sur la nature des informations échangées et leur mode de transmission.

Ces éléments lui ayant été donnés, l'ACC a, dans un avis rendu le 7 mars 1997, rappelé que :

- les informations relatives à la marque, au type, à la couleur et aux caractéristiques techniques d'un véhicule ne constituaient pas en soi des données à caractère personnel s'il n'y avait pas de lien entre ces informations et le numéro d'immatriculation, le propriétaire ou le conducteur du véhicule;
- les échanges d'informations policières au départ des fichiers nationaux entre les Parties contractantes intégrées au SIS et les autres Etats où la Convention n'était pas encore appliquée, relevaient, via les mécanismes de la coopération bilatérale ou multilatérale, des législations en matière de protection des données et du contrôle des autorités de contrôle nationales.

S'agissant des informations directement ou indirectement nominatives enregistrées dans le SIS, l'ACC a estimé qu'elles n'étaient pas accessibles et ne pouvaient pas être consultées directement par les autorités des Parties contractantes sur le territoire desquelles la Convention n'était pas encore mise en application, conformément aux articles 101 et 126.1 de la Convention.

4.1.6. L'avis sur l'accord de coopération concernant le traitement des infractions routières et l'exécution des sanctions pécuniaires en ce domaine

Le Groupe central a transmis à l'ACC le 10 février 1997 une demande d'avis émanant du groupe de travail III «coopération judiciaire» portant sur un projet d'accord sur les infractions routières.

Le texte prévoit d'une part l'accès aux informations et données figurant dans les registres d'immatriculation des Parties contractantes et, d'autre part, un système de notification directe et de coopération ainsi que l'exécution effective par chaque Etat-partie des décisions émanant d'une autorité d'une autre Partie contractante, sous réserve de certains cas limitant ou excluant l'application d'une sanction pécuniaire.

Ce projet est fondé sur la déclaration commune des ministres et secrétaires d'Etat du 19 juin 1990 aux termes de laquelle les Parties contractantes s'engagent à entamer ou poursuivre des discussions dans divers domaines dont celui des poursuites contre les infractions en matière de circulation routière et l'exécution réciproque des peines d'amendes.

Il constitue un instrument juridique international distinct mais complémentaire de la Convention de Schengen et référence est faite à son titre VI relatif aux règles de protection des données applicables en cas de transmission d'informations non inscrites dans le SIS.

L'ACC, après avoir examiné les dispositions de protection des données prévues par le projet d'accord, a rendu un avis le 27 mars 1997 dans lequel elle demande que les principes suivants soient intégrés ou explicités :

- le droit de toute personne d'exiger la rectification ou l'effacement de données la concernant qui sont entachées d'une erreur de fait ou de droit ;
- le principe de la coopération entre les autorités de contrôle nationales mentionnées à l'article 128.1 en vue de garantir les droits d'accès, de rectification ou d'effacement ;
- la compétence de l'ACC pour émettre des avis sur les aspects communs en matière de protection des données à caractère personnel découlant de l'application de l'accord.

4.2. Les missions en cours

Les principales missions engagées par l'ACC et encore en cours sont les suivantes.

4.2.1. Le guide des droits des personnes à l'égard du SIS

Ayant constaté que les dispositions de la Convention de Schengen relatives à la protection des données personnelles et notamment au droit d'accès au SIS étaient largement méconnues, l'ACC a décidé de faire élaborer un dépliant destiné au public afin d'informer largement les personnes de leurs droits et de leur donner toutes informations pratiques utiles.

L'ACC a décidé de consacrer une partie de son budget à la réalisation de ce guide, dans chacune des langues des Etats Schengen, dans le courant de l'année 1997 et à sa mise à disposition des personnes dans les postes consulaires, les aéroports et diverses administrations nationales.

4.2.2. L'interprétation de l'article 102.2 relatif à la duplication technique des données du SIS

L'article 102.2 précise que les données intégrées dans le SIS «ne peuvent être dupliquées qu'à des fins techniques, pour autant que cette duplication soit nécessaire pour l'interrogation directe par les autorités nationales habilitées».

L'ACC, sur la demande de la Commission de la vie privée belge, a engagé, au regard de cet article, une discussion sur l'interprétation de la notion de duplication de données à des fins techniques et sur celle d'interrogation directe notamment par rapport au mode d'interrogation automatisée visé par l'article 92. Elle a également commencé à évaluer les conséquences de la duplication sur CD Rom de tout ou partie d'un N.SIS notamment à des fins d'interrogation par les représentations diplomatiques et consulaires.

L'examen des conditions d'application de l'article 102.2 soulève en effet des questions relatives à la mise à jour des informations dupliquées et à la sécurité des transmissions effectuées vers des services situés en dehors des territoires des Parties contractantes.

L'ACC qui n'a pas, contrairement aux prescriptions de l'article 118.2, été rendue destinataire des mesures particulières prises pour assurer la sécurité des données dans un tel cas, rendra dans le courant de l'année 1997, un avis sur les pratiques suivies par les Etats Schengen pour l'application de l'article 102.2 et proposera une solution harmonisée compatible avec les règles de protection des données fixées par la Convention.

4.2.3. L'interprétation de l'article 103 relatif au contrôle de l'admissibilité de l'interrogation du SIS

La délégation allemande a appelé l'attention des autres membres de l'ACC sur les difficultés apparues pour l'application de l'article 103 de la Convention relatif à l'enregistrement dans chaque N.SIS, par l'instance gestionnaire du fichier, de toute dixième transmission de données à caractère personnel.

L'article 103 de la Convention ne faisant aucune distinction entre les différentes catégories de signalement, le contrôle de l'admissibilité de l'interrogation du système doit pouvoir porter sur l'ensemble d'entre elles (articles 95 à 100).

L'ACC qui a engagé une étude des solutions techniques adoptées par chaque Etat-partie pour le respect de l'article 103 rendra un avis dans le courant de l'année 1997 sur l'interprétation de cet article et recommandera l'adoption d'une procédure harmonisée.

4.2.4. L'interprétation de l'article 102.1 relatif au principe de finalité pour l'utilisation des données du SIS

La délégation allemande a également appelé l'attention de l'ACC sur les difficultés que soulève au regard de l'article 102.1 la conservation de dossiers relatifs à des signalements après exécution de ceux-ci.

L'article 102.1 interdit en effet aux Parties contractantes d'utiliser les données prévues aux articles 95 à 100 pour d'autres fins que celles énoncées pour chacun des signalements visés à ces articles.

Or l'instance centrale pour la partie allemande du SIS, après exécution de la recherche, conserve, dans son système national de police judiciaire, les signalements du SIS dont elle considère qu'ils concernent des malfaiteurs opérant à l'échelle internationale.

L'ACC rendra un avis sur cette question très importante au regard du principe de finalité des données avant la fin de l'année 1997.

Chapitre 5. L'avenir

De son expérience et notamment des difficultés rencontrées pour asseoir son autorité et son indépendance et exercer ses missions dans des conditions matérielles satisfaisantes, l'ACC tire l'enseignement qu'une réelle transparence est indispensable entre toutes les instances Schengen pour l'application effective et efficace de la Convention.

Par ailleurs, l'ACC considère que les objectifs poursuivis dans la Convention de Schengen, l'élargissement de celle-ci par la conclusion d'accords complémentaires ainsi que la complexité des mécanismes de contrôle des règles de protection des données, justifient un effort d'information à l'égard du citoyen.

5.1. La transparence dans les relations entre les instances Schengen

Certaines des difficultés évoquées dans ce rapport auraient été évitées si la Convention avait été plus explicite à propos des pouvoirs conférés à l'ACC et sur son autonomie budgétaire.

Pour autant, l'ACC souhaite que trois mesures simples soient adoptées par le Comité exécutif pour régler définitivement les difficultés qu'elle a rencontrées pour exercer ses missions dans des conditions satisfaisantes.

L'information de l'ACC sur le fonctionnement de la Convention

L'ACC, pour exercer de manière éclairée ses missions, doit pouvoir disposer d'une information régulière et systématique quant aux objectifs poursuivis par les Etats Schengen notamment lors de la conclusion d'accords complémentaires, ainsi qu'à l'égard du fonctionnement du SIS et ses modifications techniques prévisibles, tel le projet SIRENE phase II. Elle doit également être destinataire des rapports mensuels relatifs au fonctionnement du C.SIS afin d'être en mesure d'exercer de la manière la plus efficace possible ses contrôles.

Ses diverses demandes en ce sens n'ayant été satisfaites qu'au cas par cas et avec un délai d'exécution assez long, l'ACC insiste pour que désormais on lui fournisse de manière systématique l'information et les documents dont elle a besoin.

L'achèvement du protocole d'exercice des contrôles du C.SIS

Aux termes de l'article 115 de la Convention, le contrôle du C.SIS est effectué par l'ACC conformément aux dispositions de la Convention de Schengen, à celles de la Convention du 28 janvier 1981 du Conseil de l'Europe, en tenant compte de celles de la Recommandation R(87) 15 du 17 septembre 1987 du comité des ministres du Conseil de l'Europe et en conformité avec le droit national de la Partie contractante responsable de la fonction de support technique.

Lors de l'exécution au mois d'octobre 1996 du contrôle du C.SIS, des difficultés déjà mentionnées sont apparues. L'ACC se félicite de la réelle volonté de coopération qu'ont manifestée le Groupe central et les autorités françaises pour élaborer un protocole pour l'exercice des contrôles du C.SIS.

Ce protocole dont l'élaboration a été engagée avant la fin de l'année 1996 porte sur la procédure à suivre pour informer les Etats Schengen et les responsables français de la réalisation d'un contrôle, sur la qualité des personnes qui peuvent y procéder, sur le niveau d'habilitation requis pour accéder à des documents classifiés notamment secret défense, sur la prise de copie de tous documents utiles et notamment classifiés et sur les modifications techniques à apporter au C.SIS pour les besoins du contrôle des experts de l'ACC.

L'ACC souhaite que ce protocole soit adopté au plus tôt et qu'il soit notamment tenu le plus grand compte de sa demande tendant à pouvoir disposer d'un «compte utilisateur» qui lui permette d'accéder directement, sans pouvoir de modification, au système d'exploitation et aux bases de données.

La consécration définitive de l'autonomie budgétaire de l'ACC

Si le principe de la création d'une ligne budgétaire pour l'exercice de ses missions a été adopté par le Groupe central et par le Comité exécutif en mars 1997, l'ACC, qui s'en félicite, sous les réserves déjà formulées, souhaite que soit également acquise l'augmentation du montant de ce budget pour tenir compte de l'accroissement du nombre de ses membres.

Elle attend également que les difficultés qu'elle rencontre pour faire traduire en temps utile ses documents de travail par le secrétariat Schengen trouvent une solution acceptable qui ne l'oblige pas à utiliser les sommes réservées aux frais exceptionnels de traduction à l'extérieur de documents spécifiques.

5.2. La transparence à l'égard du citoyen

Sur les objectifs

Traités internationaux classiques conclus entre des Etats membres de la Communauté européenne, l'Accord et la Convention d'application de Schengen ont, sous réserve de mesures d'accompagnement, supprimé les contrôles à leurs frontières intérieures avant l'entrée en vigueur, qui était prévue au 1er janvier 1993, de l'article 7 A du Traité des Communautés européennes instituant un espace sans frontières intérieures dans lequel les personnes circulent librement.

L'objectif des Parties contractantes selon les premiers considérants de la Convention d'application et l'article 134 coïncide avec celui du Traité des Communautés européennes complété par l'Acte unique européen. A terme une législation communautaire et un nouveau système (le Système d'Information Européen -SIE-) devaient se substituer aux Accords de Schengen et s'appliquer sur le territoire de tous les Etats membres de l'Union européenne.

Aujourd'hui le cadre intergouvernemental qui a toujours prévalu dans les relations entre les Parties contractantes et les institutions européennes est-il conforté par l'élargissement des limites initiales de la Convention au-delà des territoires des pays membres de l'Union européenne ou faut-il y voir une étape de l'intégration au sein de celle-ci de nouveaux Etats ?

C'est à tout le moins l'expression du succès que rencontre «l'espace libre Schengen» et sa contrepartie de mesures communes à des fins de contrôle, dont le SIS.

Cela étant, l'extension opérée, ainsi que d'autres projets d'accords prévoient des échanges supplémentaires d'informations dont les conséquences, pour le citoyen, ne sont pas actuellement lisibles.

Sur l'élargissement de la Convention de Schengen et la complexité des mécanismes de contrôle des règles de protection des données

Sur le fondement de la déclaration commune des ministres et secrétaires d'Etat du 19 juin 1990, des accords complémentaires mais distincts de la Convention de Schengen tendent en effet à accroître les domaines de coopération des Parties contractantes (véhicules volés, infractions routières).

Lorsque ces échanges ne donnent pas lieu à une inscription dans le SIS, les règles de protection des données qui leur sont applicables sont définies de manière moins précise avec un renvoi pour l'essentiel d'entre elles, et notamment celles relatives aux droits des personnes, au droit national de chaque Etat-partie.

Il en résulte une plus grande complexité des mécanismes de contrôle du respect de ces règles et un risque d'absence d'harmonisation de leur interprétation et de leur application.

Or, l'ACC n'est pas en mesure de limiter ce risque efficacement car, hors le SIS, son rôle est secondaire et sa saisine en principe conditionnée par une demande des Parties contractantes.

Si les gouvernements sont libres de fixer les objectifs de leur coopération dans le domaine de la police et de la justice, s'il leur appartient de déterminer les mécanismes de contrôle chargés de veiller au respect de leurs engagements, il leur revient encore d'informer le citoyen des droits qu'ils lui reconnaissent pour garantir le respect des libertés publiques et individuelles.

Alors que dans le champ du droit communautaire, une directive a harmonisé les lois nationales en matière de protection des données, rien de tel n'a été engagé par les gouvernements dans celui de la coopération policière et judiciaire.

Instruments internationaux distincts sans lien juridique les uns avec les autres, les conventions de coopération, telles Schengen et Europol, comportent des règles de protection des données élaborées au cas par cas et les personnes n'ont d'autre choix, pour exercer les droits qui leurs sont reconnus, que d'explorer un dédale juridique.

A cet égard, l'ACC souhaite qu'un rapprochement puisse être opéré, dès sa mise en place, avec l'Autorité de contrôle commune d'Europol et que des actions d'information communes soient conduites.

Un tel rapprochement pourrait peut-être résulter d'un accord distinct mais complémentaire des deux conventions.

Il permettrait utilement à ces autorités, de partager leur expérience dans le contrôle du respect des règles de protection des données, et de restituer au citoyen une vision plus globale des droits qui lui sont garantis dans le cadre des objectifs poursuivis par chaque convention.

A une époque où la coopération policière et judiciaire est renforcée, où la création de systèmes d'information communs favorise la transmission rapide d'informations et de nouvelles méthodes de travail, telles le contrôle à distance (non-admissibilité, surveillance discrète) et l'anticipation par l'analyse de renseignements, le souci légitime de transparence envers le citoyen doit être une préoccupation prioritaire, non seulement de l'ACC et des autres instances de contrôle communes et nationales, mais également des gouvernements.

Vu pour être publié au Mémorial, Recueil administratif et économique.

Luxembourg, le 11 novembre 1997.

Le Ministre de la Justice,

Marc Fischbach
