

## De quoi s'agit-il?

Dans le cadre de la coopération instaurée par les Accords de Schengen et de Dublin, les autorités des Etats parties échangent régulièrement des données concernant des personnes et des objets. Dans le cadre de Schengen, l'instrument essentiel de cet échange de données est le Système d'information Schengen (SIS; pour plus de détails, voir fiche thématique 6), banque de données informatique comportant les signalements de personnes et d'objets (véhicules, armes, etc.) recherchés. Dans le domaine couvert par Dublin, les autorités utilisent Eurodac (pour plus de détails, voir fiche thématique 5), une base de données centrale informatisée dans laquelle sont saisies les empreintes digitales de tous les demandeurs d'asile et de tous les ressortissants de pays tiers en situation irrégulière. Dans ce contexte se posent des questions liées à la protection des données. Le traitement de données personnelles doit en effet se faire dans le cadre de dispositions claires qui visent à protéger les droits fondamentaux et la sphère privée des personnes concernées.

Des dispositions juridiques claires interdisent l'utilisation abusive de données personnelles

## Les régimes de Schengen et de Dublin

Tant la Convention d'application de l'Accord de Schengen (CAAS) que le règlement dit "Dublin II" (qui remplace la Convention de Dublin) et le règlement concernant la création du système "Eurodac" contiennent des dispositions sur la protection des données. Celles-ci règlent le transfert de données au titre de la coopération prévue par Schengen et par Dublin. En outre, la directive 95/46/CE, qui traite de façon générale de la protection des données à caractère personnel, est également applicable à une grande partie des domaines couverts par Schengen et Dublin.

Les domaines couverts par Schengen et par Dublin sont soumis à des règles spécifiques de protection des données

Voici les principales règles applicables aux échanges de données dans les régimes de Schengen et de Dublin:

- Seules certaines données peuvent être échangées.  
Dans le SIS, il n'est possible d'enregistrer, outre les données permettant l'identification d'une personne (y compris les signes particuliers inaltérables), que le motif du signalement, la mesure à prendre et la mention "armé" ou "violent".  
Dans Eurodac, il n'est possible d'enregistrer, outre les empreintes digitales des demandeurs d'asile et des ressortissants de pays tiers en situation irrégulière, que le nom de l'Etat membre qui a transmis les données, le lieu et la date de la demande d'asile ou de l'arrestation et le sexe.

- Les données ne sont accessibles qu'à un nombre restreint de personnes.  
Pour le SIS, ce sont les autorités chargées des contrôles frontaliers ou des autres vérifications de police ou de douanes exercées à l'intérieur du pays. Par ailleurs, les données relatives à des ressortissants de pays tiers signalés à des fins de non-admission sont accessibles aux autorités qui délivrent les autorisations de séjour et les visas (par exemple les consulats).  
Quant à Eurodac, elle est gérée par une unité centrale créée au sein de la Commission européenne. Cette unité centrale permet, à la demande d'un Etat membre, de déterminer si une personne est ou non enregistrée dans Eurodac. Chaque Etat membre reste maître des données qu'il a transmises et est responsable de leur contenu et de leur exactitude.
- Les données ne peuvent être utilisées à une autre fin que celle prévue.
- Elles doivent être exactes et à jour.
- Elles ne sont conservées que pendant une durée limitée et doivent ensuite être effacées.
- Les personnes concernées ont le droit de consulter les données qui les concernent, d'en contrôler l'exactitude et, le cas échéant, de les faire rectifier ou effacer.
- Des autorités de contrôle indépendantes veillent à ce que les règles de protection des données soient respectées et à ce que les droits des personnes concernées ne soient pas enfreints.
- Les Etats signataires doivent désigner une autorité de contrôle chargée de la partie nationale du SIS (N-SIS). Une autorité de contrôle commune est chargée du contrôle du fichier central du SIS à Strasbourg (C-SIS).
- La Commission européenne veille au bon fonctionnement d'Eurodac.

### Les conséquences pour la Suisse

La Suisse remplit déjà, au niveau fédéral, les exigences de Schengen et de Dublin en matière de protection des données (y compris celles de la directive communautaire sur la protection des données). Dans le domaine couvert par Schengen, il faudra encore, en particulier, mettre en place une partie nationale du SIS (N-SIS) que l'on re-

Le droit fédéral en matière de protection des données est compatible avec Schengen et Dublin; au niveau cantonal, des adaptations ponctuelles seraient nécessaires

liera aux systèmes suisses d'échange de données qui existent déjà. Pour ce faire, il faudra créer une base légale formelle. Dans les domaines dans lesquels les cantons sont directement concernés par Schengen et Dublin, ceux-ci devront adopter les bases légales nécessaires. En outre, chaque canton devrait disposer d'une autorité de contrôle indépendante.