FICHAGE INSTITUTIONNEL

Quels risques pour le citoyen ?

LE FICHAGE INSTITUTIONNEL DANS 14 PAYS EUROPÉENS

Savez-vous dans quels fichiers vous pouvez être enregistré ?

ÉDUCATION

Les élèves et étudiants peuvent être enregistrés dans des fichiers nationaux dont la finalité affichée est l'administration des établissements et prestations : gestion des inscriptions et services… Les objectifs affichés ne justifient pas toujours l'enregistrement, pourtant réalisé dans certains pays étudiés, de données sur la santé, l'origine, la langue des parents, voire la religion. Les principes de nécessité ou de proportionnalité sont alors violés. Souvent, le consentement des parents ou de l'élève n'est pas demandé. Enfin, la conservation des données dure souvent bien au-delà du nécessaire. Ainsi, un « faux pas » peut poursuivre un élève durant tout son parcours.

SANTÉ

La plupart des pays étudiés ont mis en œuvre des fichiers médicaux pour la bonne gestion des systèmes de santé. Les différents systèmes d'accès aux données médicales (soit que le patient ait la possibilité de choisir de créer ou non son dossier médical personnel, de masquer ou non certaines données, de donner accès ou non aux différents praticiens) mettent en cause le respect du secret médical. La gestion centralisée, l'anonymisation « insuffisante » en cas d'utilisation statistique font craindre des violations de la vie privée et de la protection des données personnelles.
Les données de santé devraient pourtant être particulièrement protégées car ce sont des données sensibles.

POLICE

Le nombre de fichiers de police est considérable dans tous les pays étudiés : fichiers des personnes recherchées pour infractions ou soupçons d'appartenance ou de soutien à des groupes terroristes, bases de données ADN... Tous sont susceptibles de contenir des erreurs, et l'absence de mises à jour régulières peut avoir des conséquences graves en termes de discriminations quand ils sont consultés par différents acteurs, notamment les employeurs potentiels. De plus, il est souvent difficile, voire impossible, pour des citoyens indûment fichés d'obtenir la correction ou la suppression de leurs données.

JUSTICE

Dans tous les pays étudiés, il existe des fichiers des casiers judiciaires. Si leur utilisation semble nécessaire au bon fonctionnement de la justice, le fait que les employeurs et différents acteurs aient accès à de nombreuses informations qu'ils contiennent induit un risque de discrimination à l'embauche.
D'autres fichiers de justice présentent également des risques d'atteinte à la vie privée (fichiers des infractions, des condamnations, etc.).

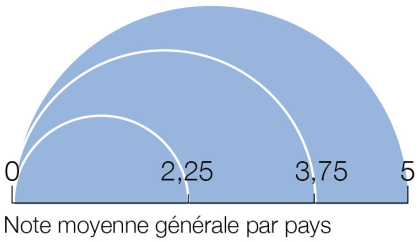
Ligue des droits de l'Homme
FONDÉE EN 1898
aedh
Humanistische Union
HUNGARIAN CIVIL LIBERTIES UNION
Ligue des Droits de l'Homme
Action Luxembourg Ouvert et Solidaire
MEDEL
Magistrats Européens pour la Démocratie et les Libertés

Le fichage institutionnel dans 14 pays européens
dans les domaines de l'Education, la Santé, la Police et la Justice

Domaines étudiés
- Justice
- Police
- Santé
- Education

Note par domaine
(composée des critères libertés menacées, transparence, recours possible, pouvoir de la DPA)
- Bonne
- Moyenne
- Non qualifié
- Mauvaise
- Très mauvaise

2 Nombre de fichiers étudiés par domaine



CONNEXIONS AVEC LES SYSTÈMES EUROPÉENS

Les données fournies par les Etats membres pour les systèmes SIS II, VIS et Eurodac sont extraites des fichiers collectant ces types de données au niveau national.

Système d'information Schengen II (SIS II)

SIS II intègre des éléments biométriques d'identification de personnes disparues, de personnes recherchées (pour les extrader, pour les juger...), de personnes placées sous surveillance, ainsi que des éléments d'identification d'objets et véhicules recherchés. Ce système suscite une multiplicité de craintes qui portent, notamment, sur sa haute capacité technologique requérant une très grande maîtrise, sur sa finalité pratique qui est de repousser les « étrangers », ou encore sur l'ignorance des personnes de leur entrée dans SIS II.

Système Eurodac

Eurodac permet l'identification et le contrôle des demandeurs d'asile et des immigrants illégaux sur le territoire de l'UE, personnes hautement vulnérables, grâce à la comparaison des dix empreintes digitales du demandeur avec celles contenues dans le système. Ce système est supposé mettre en œuvre « efficacement » le règlement qui détermine l'Etat responsable de l'examen d'une demande de protection internationale (le règlement Dublin III). Eurodac est désormais accessible aux autorités de police et à Europol, stigmatisant ce groupe déjà vulnérable et dont on collecte dix empreintes.

Système d'information Visa (VIS)

Le Système d'information sur les visas, VIS, a pour objectif de contrôler de manière identique dans les pays de l'UE l'entrée dans l'espace européen Schengen des étrangers soumis à visa, et de repérer ceux qui « oublieraient » d'en repartir à l'expiration de leur visa. Ce système repose sur la comparaison des données biométriques, en particulier des dix empreintes digitales, contenues dans le système avec celles du demandeur de visa. Il contient les données biométriques (empreintes, photographie) et biographiques (nom, emploi, durée prévue du séjour, but du voyage…). Les dix empreintes digitales sont conservées pendant cinq ans pour un visa qui ne dure que trois mois.

Système ECRIS

Le système ECRIS a été mis en œuvre pour faciliter la coopération entre les autorités judiciaires des Etats membres en vue d'échanges d'informations dans le cadre d'enquêtes pénales et/ou de procédures judiciaires.
Le système ECRIS n'est pas une base de données centralisée au niveau européen. Il organise la consultation des casiers judiciaires d'un pays membre à un autre. Cependant, l'échange d'informations est opéré dans un cadre où la définition des crimes et des délits, l'inscription des condamnations dans les casiers et leur accès ne sont pas les mêmes dans tous les pays de l'Union, ce qui peut entraîner des discriminations.

Comment protéger vos données personnelles ?

Le traitement de données personnelles ne doit pas constituer une violation de la vie privée. Les principes de base doivent être respectés, dont les principes de finalité, de proportionnalité et de loyauté. Si vous pensez que vous êtes enregistré indûment dans un fichier, vous pouvez interroger le détenteur du fichier ou, dans certains cas, votre Autorité de protection des données personnelles (DPA, voir coordonnées page suivante).

AUTORITÉS DE PROTECTION DES DONNÉES PERSONNELLES

Allemagne : Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI) / Commissaire fédéral à la protection des données et la liberté de l'information
www.bfdi.bund.de

Autriche : Österreichische Datenschutzbehörde / Autorité de protection des données autrichienne
www.dsb.gv.at

Espagne : Agencia Española de Protección de Datos (AGPD) / Agence espagnole de protection des données
www.agpd.es

Finlande : Tietosuojavaltuutetun Toimisto / Office du défenseur des droits de protection des données
www.tietosuoja.fi

France : Commission nationale de l'informatique et des libertés (Cnil)
www.cnil.fr

Grèce : Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα / Autorité hellénique de protection des données
www.dpa.gr

Hongrie : Nemzeti Adatvédelmi és Információszabadság Hatóság (NAIH) / Autorité nationale hongroise pour la protection des données et la liberté de l'information
www.naih.hu

Italie : Garante per la Protezione dei Dati Personali (GPDP) / Autorité pour la protection des données personnelles
www.garanteprivacy.it

Luxembourg : Commission nationale pour la protection des données (CNPD)
www.cnpd.public.lu
+ Autorité de contrôle spécifique des fichiers de la Police, de la Douane, du Service de renseignement, de l'Armée et de la Justice (dite « Autorité de contrôle », loi du 2 août 2002, art. 17.2)

Pologne : Generalny Inspektor Ochrony Danych Osobowych (GIODO) / Inspecteur général à la protection des données
www.giodo.gov.pl

Portugal : Comissão nacional de protecção de dados (CNPD) / Commission nationale de la protection des données
www.cnpd.pt

République tchèque : Úřad pro ochranu osobních údajů / Office pour la protection des données
www.uoou.cz

Royaume-Uni : Information Comissioner's Office (ICO) / Office du commissaire à l'information
ico.org.uk

Slovénie : Informacijske pooblaščenke / Commissaire à l'information
www.ip-rs.si

Cette publication a été éditée avec le soutien financier du programme Fundamental Rights de la Commission européenne.