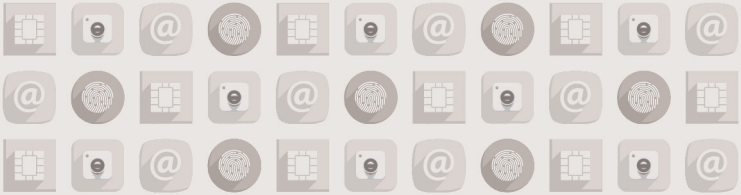
FICHAGE
INSTITUTIONNEL

Quels risques pour le citoyen ?



Ligue des **droits de l'Homme**
FONDÉE EN 1898

ÉDUCATION
SANTÉ
POLICE
JUSTICE

aedh

Humanistische Union

HUNGARIAN CIVIL LIBERTIES UNION
HCLU

Ligue des Droits de l'Homme
Action **Luxembourg** Ouvert et Solidaire

MEDEL
Magistrats Européens pour la Démocratie et les Libertés

FICHAGE
INSTITUTIONNEL

Quels risques pour le citoyen ?

Les citoyens (vous peut-être !) ignorent souvent l'étendue du fichage exercé par les institutions de l'Etat, dont eux-mêmes ou leurs proches peuvent être l'objet. Avez-vous conscience que ce fichage peut être abusif, même lorsqu'il est encadré par des lois ?

Chacun doit connaître ses droits et ses moyens de recours, et ne pas s'en remettre aux autorités publiques pour décider du bon usage de ses données personnelles.

Chacun doit exercer sa vigilance, non seulement pour sa propre personne et ses propres données, mais aussi pour ses proches et la société de manière générale.

Ce passeport vous donne des clefs pour exercer votre vigilance et vos droits. Averti, vous pourrez alors compléter votre information et entreprendre les démarches qui paraîtront nécessaires (des informations complémentaires se trouvent sur les sites indiqués en 4e de couverture).

FICHAGE
INSTITUTIONNEL

Quels risques pour le citoyen ?

Finalité et dangers des fichiers

FINALITÉ

Les bases de données en matière d'éducation ont pour finalité de faciliter la gestion et l'administration du système éducatif, notamment en organisant les inscriptions à un établissement ou à des cours, activités et services spécifiques. Elles permettent également de réaliser des statistiques à partir des données collectées.

Ces finalités ont une certaine légitimité puisqu'elles contribuent à une gestion efficace : définition du nombre de classes, du nombre d'enseignants par discipline, etc.

DANGERS ET PRÉCAUTIONS NÉCESSAIRES

Les bases de données scolaires étudiées contiennent une quantité considérable de données mises à la disposition des écoles et des autorités. Souvent, la proportionnalité au regard de la finalité poursuivie n'est pas respectée.

En effet, ne devraient être recueillies que les données strictement nécessaires à la gestion. Or certains fichiers contiennent des données sensibles telles que l'état de santé, l'état mental, les opinions religieuses ou encore les origines de l'élève. Bien évidemment, plus les données sont « sensibles », plus les mesures de sécurité devraient être renforcées. Sinon, enfants et familles pourront être victimes de discriminations, voire être mis en danger (discriminations fondées sur la religion, l'origine, etc.).

L'inscription de ces données sensibles dans un fichier lié à l'éducation ne devrait pas se faire sans le consentement des parents ou des responsables légaux puisque, hormis les étudiants et les lycéens en fin de cursus, les personnes concernées sont des mineurs : il est primordial de prêter attention à ce qu'entraîne ce consentement et de ne pas le donner sans un regard sur les données collectées.
Un faux-pas, une année scolaire difficile, peuvent, s'ils sont inscrits dans un fichier, entraîner des conséquences et des discriminations pour un élève durant tout son parcours scolaire, voire au-delà.

DURÉE DE CONSERVATION DES DONNÉES DANS LES FICHIERS ÉTUDIÉS PAR PAYS

Royaume-Uni	illimitée
France	5 ans après la radiation du dernier établissement fréquenté
Italie	fin d'année civile de fin de cycle
Luxembourg	jusqu'à 7 ans après la fin des études secondaires, à l'exception des données sur les absences, suspensions et régime linguistique spécifique (supprimées dès la fin des études secondaires)

CE QUE DIT LA LOI

La collecte des données personnelles des élèves et de leurs parents impose leur consentement, y compris lorsque ces données sont collectées dans un but statistique ou à des fins de recherche.

La réalisation de recherches et de statistiques ne requiert pas une collecte de toutes les données individuelles des élèves au niveau national, un échantillon représentatif suffit.

L'action des ONG pour des fichiers respectant mieux le principe de proportionnalité et la protection des données personnelles

En France, en 2010, les mentions de la nationalité, de la date d'arrivée en France et de la langue des parents ont été supprimées des fichiers de l'Education nationale par le Conseil d'Etat, suite à l'action d'ONG.
En Allemagne, en 2006, le projet d'utilisation du « numéro d'identification élève » a été abandonné suite à une forte mobilisation d'ONG.

NOS RECOMMANDATIONS

VOUS ÊTES UN CITOYEN, ENGAGEZ-VOUS AFIN QUE :

- les données collectées pour l'organisation des établissements scolaires ne soient pas enregistrées au niveau national mais au niveau local pertinent. Connaître les « difficultés scolaires » ou le handicap d'un élève n'est en effet utile qu'au niveau de l'établissement scolaire ou au niveau local, voire régional. L'enregistrement de l'identité de l'élève n'est pas nécessaire au niveau national ;
- les données collectées et traitées au niveau national soient conservées uniquement sous la forme de données agrégées, surtout si des données sensibles (santé, religion, etc.) sont concernées. Les données agrégées résultent d'un calcul statistique obtenu à partir d'un ensemble de données brutes individuelles groupées selon des caractéristiques communes. La seule anonymisation des données n'est pas une mesure suffisante.

VOUS OU VOTRE ENFANT ÊTES OU EST CONCERNÉ PAR UN FICHIER ÉDUCATION

DEMANDEZ À

Connaître l'usage qui sera fait des données (transparence) et la forme prise par ces usages afin de pouvoir exercer le droit d'opposition, de suppression, de rectification.

VÉRIFIEZ QUE

Les données scolaires ne soient pas utilisées pour faire des discriminations ou pour établir des profils-types des élèves. En effet, certaines bases de données permettent de définir des profils d'élèves afin de les orienter dans leur scolarité ou dans leur future activité professionnelle.

Ne donnez votre consentement à l'inscription dans les fichiers de l'Education nationale qu'après avoir vérifié la nature des données collectées et leur usage.

FICHAGE
INSTITUTIONNEL

Quels risques pour le citoyen ?

Finalité et dangers des fichiers

FINALITÉ

Les fichiers concernant les données de santé sont mis en œuvre pour assurer l'efficacité des services de santé publique, pour un suivi personnalisé des patients et des assurés, pour la coordination entre les différents professionnels de santé, ou pour connaître l'état sanitaire de la population à travers des données statistiques.

DES DONNÉES HAUTEMENT SENSIBLES, DES RISQUES AVÉRÉS

Les données de santé sont par définition des données « sensibles » parce que d'une part elles font bien évidemment état de la santé de la personne, d'autre part elles peuvent en révéler la condition sociale ou d'autres particularités personnelles. Ces données doivent donc être particulièrement protégées, ce qui ne peut être le cas lorsque de nombreuses personnes peuvent y accéder relativement facilement. Le respect du secret médical, garantie indispensable de la relation de confiance entre le patient et son médecin, est alors compromis.

Les bases de données centralisées n'assurent pas toujours une segmentation des données, ce qui permettrait pourtant un accès spécifique par les différents professionnels de santé.

L'anonymat du patient n'est pas toujours garanti, ce qui peut encourager des acteurs tiers, tels que des employeurs, des assureurs et des organismes bancaires, à tenter d'accéder à ces données dans un objectif de profit. Il y aurait alors un manquement caractérisé au respect de la vie privée, ainsi que des risques de discriminations liées à l'état de santé de la personne : refus d'attribution d'un prêt bancaire, d'accès à un emploi, refus de couverture sociale complémentaire, par exemple en cas de maladies graves.

Un exemple où les fichiers électroniques deviennent incontournables

La Finlande est sur le point de passer aux prescriptions totalement dématérialisées, ce qui signifie la fin des feuilles de soin papier et l'archivage de la totalité des données médicales dans les fichiers informatiques de santé. Il ne sera absolument plus possible d'échapper à ce système d'information. C'est une violation du droit de toute personne à ne pas être contrainte de partager ses données médicales.

DURÉE DE CONSERVATION DES DONNÉES DANS LES FICHIERS PAR PAYS

Hongrie	de 30 à 50 ans
Grèce	jusqu'à 20 ans
République Tchèque	5 ans (50 ans dans certains cas)
Italie	à vie, possibilité de suppression à la demande
Allemagne	à vie, possibilité de suppression de certaines données à la demande
Royaume-Uni	à vie
Finlande	30 mois dans le système « Prescription Centre », puis jusqu'à 10 ans dans un centre d'archivage
France	10 ans à compter de la clôture du dossier par le patient

NOS RECOMMANDATIONS

VOUS ÊTES UN CITOYEN, VOUS DEVRIEZ VOUS ENGAGER AFIN QUE :

- le dossier médical électronique soit réservé aux patients qui nécessitent des traitements lourds, coûteux et de longue durée ;
- le patient soit informé de l'enregistrement de ses données de santé et qu'il donne son consentement. Il doit pouvoir décider de l'ouverture ou non d'un dossier électronique de santé et définir quels tiers peuvent effectivement avoir accès à ses données et auxquelles. Il doit également pouvoir exercer ses droits d'accès, de modification et de refus de communication de ses données personnelles à des tiers ;
- une étude sur les avantages et les inconvénients des différents supports de données envisageables soit menée par un comité spécial indépendant ;
- les données archivées dans les fichiers de santé répondent à des mesures spécifiques de protection incluant le chiffrement des données afin d'éviter toute fuite de ces dernières sous une forme identifiable.
  Dans le cas où les données sont utilisées à des fins statistiques, elles doivent être impérativement rendues anonymes ;
- un système alternatif, comme les prescriptions papier, puisse être utilisé à la demande du patient ;
- le choix soit laissé au patient de s'inscrire ou non dans un fichier de santé.

FICHAGE
INSTITUTIONNEL

Quels risques pour le citoyen ?

Finalité et dangers des fichiers

Les fichiers sont un outil indispensable aux services de police afin d'assurer la protection des citoyens et de mener des enquêtes. Ils améliorent les possibilités de résolution des enquêtes, la capacité d'identification des coupables présumés de faits pénalement répréhensibles, afin qu'ensuite ils puissent être jugés.

Néanmoins, ces fichiers sont basés sur des critères de suspicion de culpabilité et de dangerosité incertains. Ils sont de ce fait susceptibles de violer la présomption d'innocence, le droit au respect de la vie privée, ainsi que le droit à la protection des données personnelles.

L'introduction de la biométrie dans les fichiers de police est maintenant généralisée, l'argument sécuritaire étant déterminant pour imposer cette pratique. L'extension importante de cet usage entraîne une disproportion par rapport aux finalités. C'est assez inquiétant dans un Etat de droit. Aussi l'idée que cet Etat puisse dériver vers une forme moins démocratique doit-elle faire réfléchir plus encore à la réelle pertinence de ces traitements de données.

DE LA PROTECTION À LA DISCRIMINATION, LA DÉLICATE QUESTION DES FICHIERS DE POLICE

De nombreuses situations, outre la culpabilité reconnue, entraînent une inscription dans les fichiers de police : il suffit d'être soupçonné, victime, témoin, etc. Or, en fonction des usages qui sont faits de ces fichiers et des personnes qui y ont accès, être inscrit dans certains fichiers de police peut entraîner des discriminations, avoir un impact sur la vie professionnelle…

De plus, toute inscription, fondée ou non, peut s'installer dans une durée inacceptable à cause du non-respect du principe de proportionnalité et d'une mauvaise application des règles de gestion des fichiers.

La délicate question de la transparence

Pour éviter de compromettre l'efficacité d'une enquête, des données personnelles peuvent être légitimement collectées à l'insu des personnes concernées.

Cependant, une telle opacité ne peut se justifier que sur un temps limité et jamais au-delà de l'enquête. Une personne qui n'est plus soupçonnée devrait ensuite être informée du fichage dont elle a été l'objet (nature des données collectées, nom du fichier et usage de ces fichiers). En outre, toutes les données enregistrées la concernant devraient dès la fin de l'enquête être supprimées des fichiers.

La multiplication des fichiers de police et leur extension

Les fichiers de police se sont multipliés au fil des années, collectant des données ADN, des empreintes digitales, des informations sur les immigrés et les résidents étrangers, sur des personnes concernées par une enquête de police, etc. De plus, nous laissons des traces en tous lieux, y compris ceux concernés par une enquête : cheveux, empreintes, etc. Une simple présence peut être enregistrée par les caméras de vidéosurveillance. La possibilité d'être soupçonné durant un temps par erreur est donc grande, de même que la possibilité d'être inscrit dans un fichier de police.

De nombreuses possibilités d'erreur

Ces erreurs proviennent de plusieurs facteurs : pas d'actualisation des fichiers durant ou après l'enquête (personne disculpée mais toujours enregistrée comme « dangereuse » dans un fichier de police !), données mal enregistrées (par exemple « auteur » au lieu de « victime » ou « témoin » de l'infraction !).

Ces erreurs deviennent difficiles à corriger lorsqu'elles se propagent au travers d'interconnexions entre fichiers de police, ou avec des fichiers de justice, ainsi qu'avec des fichiers européens. Par exemple, les fichiers nationaux contenant les empreintes digitales d'étrangers alimentent le système européen Eurodac, et des bases de données de supposés terroristes alimentent le Système d'information Schengen (SIS II) ; les erreurs y seront donc répercutées automatiquement.

L'impact d'une centralisation au niveau européen

Les systèmes européens, basés sur une technologie de plus en plus poussée et intrusive, conduisent à une surveillance de plus en plus généralisée. Leur centralisation présente un danger supplémentaire du fait d'un décalage entre la raison de la collecte des données et l'usage réel qui en est fait.

DURÉE DE CONSERVATION DE DONNÉES ADN PAR LA POLICE

Hongrie	20 ans pour les personnes suspectées d'infraction grave et leurs contacts
France	25 ans pour les personnes mises en cause, 40 ans pour les personnes condamnées
Royaume-Uni	indéfiniment pour les données ADN collectées avant 2012. De 2 à 5 ans pour celles collectées depuis 2012

NOS RECOMMANDATIONS

VOUS ÊTES UN CITOYEN, DEMANDEZ QUE :

- les citoyens soient correctement informés des collectes et conservations de leurs données. C'est indispensable face à la complexification des fichiers de police, l'élargissement de leur champ de collecte et de leur échelle de diffusion ;
- les citoyens aient une possibilité de recours auprès des autorités en charge des fichiers, mais aussi auprès des autorités de contrôle et devant un tribunal, afin que leurs données soient corrigées ou effacées ;
- les données soient compartimentées afin que chaque personne qui consulte le fichier n'ait accès qu'aux données qu'elle recherche (respect des principes de proportionnalité et de finalité) ;
- les données ADN des manifestants ou militants politiques ne soient pas collectées et archivées comme celles des criminels ;
- les autorités de protection des données contrôlent les caractéristiques des fichiers de police avant leur création, et aussi vérifient régulièrement les pratiques et le respect des règles de fonctionnement, en particulier leur mise à jour et la sécurité des accès ;
- la collecte de données biométriques pour la sécurisation de pièces d'identités et la collecte pratiquée lors d'enquêtes policières soient différenciées. En effet, le recoupement de ces informations, s'il augmente l'efficacité policière, accroît tout autant les risques d'erreurs judiciaires.

Vous pensez avoir été inscrit dans un fichier de police, que ce soit en tant que suspect, victime, simple témoin d'une infraction, manifestant, etc. : renseignez-vous sur la collecte de vos données personnelles dans des fichiers de police. Vérifiez que les données enregistrées soient exactes et aussi qu'il est légitime qu'elles soient toujours inscrites dans un fichier de police !

FICHAGE
INSTITUTIONNEL

Quels risques pour le citoyen ?

Finalité et dangers des fichiers

FINALITÉ

La protection de la société, motif invoqué pour justifier les fichiers de justice, ne peut en aucun cas se faire au détriment des droits fondamentaux tels que les droits au travail, au libre choix d'une activité professionnelle, à la protection des données personnelles et au respect de la vie privée.

Les fichiers administrés par les autorités judiciaires sont divers. Le casier judiciaire, qui contient les condamnations définitives d'un citoyen, est le plus fréquent dans les pays européens. On peut trouver également des fichiers thématisés par infraction allant du meurtre à l'infraction au Code de la route, des fichiers liés aux informations génétiques et biométriques, qui, partagés avec la police, facilitent la collaboration entre les services de police et le système judiciaire.

DANGERS

Les criminels et délinquants ne sont pas les seuls concernés par ces fichiers ! Etre témoin ou suspect durant un temps de la procédure suffit souvent à être inscrit dans ces bases de données, sans en être clairement et explicitement informé. Ceci rend difficile tout recours.

De plus, ces fichiers ne sont pas exempts d'erreurs qui peuvent provenir de la saisie, de l'archivage ou de la transmission de ces données.

Il est possible cependant d'exercer un droit de vérification des informations contenues dans ces fichiers. Il convient de s'adresser à l'autorité compétente pour faire corriger les données ou pour faire vérifier que celles qui peuvent être supprimées l'ont bien été.

Ces fichiers peuvent être utilisés à d'autres fins que celles requises pour la justice. Par exemple, il est nécessaire de fournir des informations du casier judiciaire pour accéder à certains emplois : c'est une source de danger pour la personne, alors que, souvent, ce n'est ni utile, ni nécessaire, ni obligatoire !

Les échanges entre pays :

ECRIS (European Criminal Records Information System)

ECRIS est un système européen d'échange d'informations sur les condamnations des ressortissants entre les Etats membres. Or, les législations nationales diffèrent : un acte puni ici ne le sera pas là, ou pas de la même façon. De plus, les informations sur les condamnations sont l'objet de traitements différents, de durées de conservation inégales entre Etats. De ce fait, les échanges peuvent entraîner des discriminations, des distorsions, augmentées des imprécisions liées à des traductions automatiques.

Comment fonctionne le système ECRIS ?

Ce sont les règles de l'Etat membre dans lequel a lieu la condamnation qui s'appliquent (pour la définition de l'infraction et la durée de conservation). Si le condamné est un étranger dans l'Etat dans lequel a lieu la condamnation, cet Etat doit transmettre les informations de la condamnation à l'Etat d'origine. Celui-ci se chargera de consigner les informations dans le casier judiciaire de l'intéressé et de communiquer, telles quelles, les données du casier à tout Etat membre qui en ferait la demande.

Par ailleurs, en cas de candidature à un emploi, un extrait de casier judiciaire pourra être demandé au candidat par l'employeur. Cette demande peut être systématique, quel que soit l'emploi visé, ou limitée à des professions spécifiques. Or, les conditions de demande et les informations communiquées varient d'un Etat à un autre. L'administration du casier judiciaire, selon la législation du pays, peut communiquer l'ensemble du casier ou simplement un extrait contenant les infractions les plus graves, ou celles de nature à avoir un impact sur l'emploi visé. Là encore, ces échanges, qui ne sont pas toujours nécessaires, peuvent entraîner des discriminations du fait des différences de législation et de pratiques entre les Etats membres.

À SAVOIR

Si vous êtes amené à demander à quelqu'un son casier judiciaire (vous êtes employeur, par exemple), vous devez savoir que l'information reçue ne doit pas être un frein à la réinsertion d'une personne, ni un instrument de contrôle ou de discrimination.

Vous êtes résident d'un pays de l'Union européenne, vous avez des droits :

- le droit à l'information sur le contenu du casier judiciaire ;
- le droit au respect de la vie privée : les fichiers et les données qui y sont enregistrées doivent respecter le principe de nécessité et de proportionnalité aux objectifs poursuivis ;
- en cas d'erreur, le droit de recours auprès des autorités de justice ou la possibilité de porter plainte auprès de l'autorité de protection des données personnelles.

Dans certains pays, l'employeur ne peut demander le casier judiciaire que dans un cadre prévu par la loi.
La France et le Luxembourg font exception car aucun cadre législatif ne limite la demande d'extrait de casier judiciaire.

LDH, Ligue des droits de l'Homme
www.ldh-france.org

AEDH, Association européenne
pour la défense des droits de l'Homme
www.aedh.eu

HU, Humanistische Union
www.humanistische-union.de

HCLU, Hungarian Civil Liberties Union
www.tasz.hu/en

ALOS-LDH, Action Luxembourg Ouvert et Solidaire
- Ligue des droits de l'Homme
www.ldh.lu

MEDEL, Magistrats européens
pour la démocratie et les libertés
www.medelnet.eu

FLASHEZ POUR TESTER VOS CONNAISSANCES

VOS DONNÉES NE SERONT PAS ENREGISTRÉES

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

QUARTR -Design CRÉATONE - Paris