Présentation des interventions

Retrouvez le colloque sur www.univ-orleans.fr/lefichier

Transparence et réforme de la police, archéologie du fichier de police de Guillauté à Bertillon

Dominique MESSINEO

Maître de conférences en histoire du droit
Université d'Orléans

La communication a pour ambition de revenir sur trois moments historiques de constitution de fichiers de police entre 1749 et 1914, afin d'appréhender la manière dont ceux-ci entendent produire efficacement de l'ordre. Ces dispositifs de sécurité agissant en lieu et place du système juridique, jugé inopérant pour harmoniser la société traduisent la volonté de la pacifier en recourant à de sous-systèmes normatifs tels que la discipline ou l'hygiénisme social. De sorte que le fichier de police se caractérisera constamment par un regard méfiant sur le droit, le disqualifiant comme discours et pratique organisant légitimement la mise en scène du grand théâtre social. Le fichier de police, dont l'omniscience est au cœur de sa logique, aura pour objectif dans un premier temps d'immobiliser la circulation grandissante des personnes au XVIIIe siècle, de connaître et de reconnaître avec certitude les récidivistes au XIXe siècle, puis enfin de prévenir et de prédire les conduites à risques en ce début de XXe siècle. Ce faisant, le modèle politique de contrôle social véhiculé par le fichier de police aura glissé lentement d'un idéal formé par la discipline à un autre, davantage centré sur la répression et par conséquent sécuritaire.

Les fichiers des services de renseignement

Fouad Eddazi
Maître de conférences en droit public
Université d'Orléans

Les fichiers des services de renseignement apparaissent, indubitablement, comme des instruments essentiels au bon accomplissement des missions assignées aux services (DGSE, DGSI…). Les données contenues dans ces fichiers visent la protection des intérêts fondamentaux de la Nation, par la prévention et l'anticipation des menaces susceptibles d'y porter atteinte.

Si la fondamentalité opérationnelle des fichiers n'est pas sujette au débat, leur régulation juridique est par contre très complexe. Cette complexité s'explique par l'ambivalence constante de ces fichiers.

En premier lieu, les fichiers des services des renseignements sont ambivalents du fait de leur positionnement particulier par rapport aux notions de secret et de transparence, ce qui rend difficile leur identification. A cet égard, il faut souligner une dichotomie fondamentale entre les fichiers propres aux services de renseignement, caractérisés par un secret absolu, et les fichiers partagés avec les services de renseignement, marqués par une transparence opaque.

En deuxième lieu, l'ambivalence des fichiers des services de renseignement découle du fait qu'ils se rattachent simultanément à la logique du pouvoir d'Etat et aux contraintes bureaucratiques classiques. Assurément, il est incontestable que les fichiers des services manifestent la volonté de puissance de l'Etat, ce qui se traduit notablement par l'extension considérable des techniques de renseignement alimentant les fichiers, ainsi que des motifs justifiant leur mise en œuvre. Cependant, les services de renseignement demeurant organiquement des administrations, des problématiques bureaucratiques se posent à eux dans la gestion administrative de leurs fichiers.

En troisième lieu, le caractère ambivalent des fichiers des services de renseignement naît de de leur inscription dérogatoire dans l'Etat de droit, d'où un contrôle tempéré porté à leur égard. Effectivement, les exigences de l'Etat de droit imposent que les fichiers des services de renseignement soient contrôlés. Toutefois, le secret et le pouvoir d'Etat caractérisant ces fichiers exigent que cette soumission échappe aux canons du droit commun, d'où le constat d'un contrôle s'inscrivant dans un droit d'exception.

I. Entre secret et transparence : la délicate identification des fichiers des services de renseignement

A) Les fichiers propres aux services de renseignement : le secret absolu

B) Les fichiers partagés avec les services de renseignement : une transparence opaque

II. Entre puissance de l'Etat et contrainte bureaucratique : de l'alimentation à la gestion des fichiers des services de renseignement

A) L'alimentation des fichiers des services de renseignement : une manifestation de la puissance de l'Etat

B) La gestion du fichier de renseignement, manifestation de contraintes bureaucratiques

III. Entre Etat de droit et droit d'exception : le contrôle tempéré des fichiers des services de renseignement

A) Les avancées de l'Etat de droit en matière de contrôle

B) La persistance d'un droit d'exception amoindrissant la portée du contrôle

INTERPOL ET SES FICHIERS

Jean Frayssnet
Professeur émérite
Université d'Aix-Marseille
Membre et Rapporteur de la Commission de contrôle des fichiers d'Interpol

Créée en 1923 dans sa première forme, l'Organisation internationale de police criminelle (OIPC), plus connue sous la dénomination d'Interpol, est l'organisation internationale de police la plus importante du monde avec 190 pays membres, un personnel de 800 personnes, basé pour l'essentiel à Lyon où se situe le siège de l'organisation, disposant d'un budget de 80 millions d'euros.
Selon l'article 2 du statut de 1956 modifié, l'OIPC a pour but « d'assurer et de développer l'assistance réciproque la plus large de toutes les autorités de police criminelle, dans le cadre des lois existant dans les différents pays et dans l'esprit de la Déclaration universelle des droits de l'Homme, d'établir et de développer toutes les institutions capables de contribuer efficacement à la prévention et à la répression des infractions de droit commun ».
Interpol est concerné par toutes les formes de criminalité : criminalité classique, criminalité financière, cyber-criminalité, criminalité de l'environnement, de la propriété intellectuelle, de la traite des personnes, de la lutte contre le terrorisme etc…
A partir de la collecte des données, de leur formatage et centralisation, de leur exploitation par des traitements et des experts, de leur diffusion mondiale grâce à des fichiers accessibles par les polices des états membres, Interpol joue un rôle essentiel dans la connaissance et la lutte de toutes les formes de criminalités en offrant un efficace outil de coopération internationale dans le respect de la souveraineté des Etats. Le secteur de la police criminelle étant sensible, on comprend que les fichiers d'Interpol soient l'objet d'enjeux variés.

I – Les fichiers au coeur de l'action d'Interpol

- Les principes de mise en commun et de partage des informations ; le rôle des Bureaux centraux nationaux (BCN), le respect de la souveraineté des états.
- Les règles internes de gestion des données et des fichiers : le règlement sur le traitement des données (RTD).
- Les infrastructures : I/24/7 (système de communication), I-Link ; centre de commandement et de coordination.
- Les fichiers généraux, les notices et diffusions
  - les fichiers des personnes recherchées, des empreintes digitales, des profils génétiques, des documents de voyages volés et perdus, des véhicules volés, des œuvres d'art.
  - les différentes notices et les diffusions.
- les fichiers spécialisés, pour le suivi de secteurs particuliers et la préparation d'actions particulières sur le terrain (ex : terrorisme, contrefaçon, piraterie maritime, drogue, Pink-panthers etc.) ; exploitation et analyse des données, expertises.

II – Les fichiers d'Interpol, objets d'enjeux variés

- Les enjeux technologiques et méthodologiques : exploitation des données ; qualité et nature des données ; big-data, data-mining, logiciels prédictifs, forensic, sécurité et fiabilité.
- les enjeux politiques : les fichiers, curseurs des relations entre les états-membres et Interpol ; à qui sont les données ? ; problème de gouvernance ;

Les risques de politisation et d'instrumentalisation d'Interpol : l'article 3 du statut de 1956 modifié pose : « toute activité ou intervention dans des questions ou affaires présentant un caractère politique, militaire, religieux ou racial est rigoureusement interdite à l'organisation » ; référence à la 2ème guerre mondiale ; la distinction difficile entre politique et criminalité ; le partenariat avec le secteur privé.

- Les enjeux juridiques : les fichiers et les activités d'Interpol doivent s'inscrire dans le respect des droits de l'Hommes et des règles de la protection des données personnelles. A cette fin création d'une institution originale : la Commission de contrôle des fichiers d'Interpol, organe indépendant doté de trois compétences ; le droit d'accès et de contestation des données fichées ; un pouvoir consultatif en théorie mais décisionnel en fait ; la doctrine de la CCF ; la montée des pressions ; le privilège de juridiction.

Les divergences transatlantiques dans l'exploitation des fichiers privés pour la lutte contre le terrorisme : droit positif et prospective

Philippe Ch.-A. GUILLOT
Professeur de relations internationales à l'École de l'Air

Comment les fichiers privés peuvent-ils être exploités par les autorités publiques dans le cadre de la prévention du terrorisme ? Différentes conceptions du bon équilibre entre la liberté individuelle et les mesures sécuritaires opposent d'un côté l'Union européenne et ses États membres qui consacrent la protection des données à caractère personnel comme un droit fondamental et, de l'autre côté, les États-Unis d'Amérique qui font relativement peu de cas du respect de la vie privée en dépit du quatrième Amendement et de la théorie de la *privacy*. La coopération entre l'Europe et les États-Unis en matière de lutte contre le terrorisme doit donc concilier des approches divergentes, voire contradictoires.

La communication, en un premier temps, revient sur les péripéties ayant entouré deux types d'accords euro-américains concernant les fichiers de passagers aériens (*Passenger name Record* – P.N.R.) et ceux des messageries bancaires (*SWIFT-Terrorist Finance Tracking Program*) qui ont donné lieu non seulement à une controverse « transatlantique », mais aussi à un conflit au sein des institutions de l'Union européenne du fait des différences d'appréciation sur les concessions à faire par la Commission et le Conseil, d'une part, et, d'autre part, par la Cour de justice et le Parlement, lesquels s'avèrent d'ardents défenseurs de la protection des données à caractère personnel – opposition qui perdure face au projet de directive visant à créer un P.N.R. européen – alors même que certains États membres ont adopté des mesures permettant à leurs services de sécurité d'avoir accès aux données des passagers aériens, à l'instar du « système API-P.N.R. France ».

En un second temps, la communication élargit la question à l'équilibre à construire dans le cas du recueil de métadonnées auprès des entreprises de communications électroniques et des fournisseurs d'accès à l'internet par certains États membres (notamment la France avec les dispositions de la loi de programmation militaire et de celle relative renseignement), inspiré des pratiques de la *National Security Agency* que le récent *USA Freedom Act* vient pourtant de restreindre, et le droit fondamental à la protection des données personnelles tel qu'interprété par l'arrêt de la Cour de justice *Digital Rights Ireland* & *Seitleinger* du 8 avril 2014.

En guise de conclusion, la communication plaide pour une approche de la lute antiterroriste plus respectueuse de la protection des données personnelles.

LE CONTROLE DU JUGE INTERNATIONAL SUR LA COLLECTE, LE STOCKAGE ET L'UTILISATION MASSIFS DE DONNEES A CARACTERE PERSONNEL

Julien CAZALA
Maitre de conférences HDR en droit public
Université d'Orléans détaché sur un poste d'expert technique international du Ministère des affaires étrangères auprès de l'Université Galatasaray (Istanbul)

Les données à caractère personnel sont régulièrement collectées, stockées, utilisées à des fins commerciales mais aussi dans le cadre de la conduite des politiques publiques. Celles-ci constituent un formidable outil d'acquisition de connaissances permettant une prise de décision plus efficace et plus rationnelle. Ce développement de l'utilisation des données à caractère personnel s'accompagne de menaces pour la vie privée des individus. C'est particulièrement le cas lorsque ces données sont acquises dans le cadre de programme de surveillance de masse dont les contours ne sont pas toujours précisés.

Notre contribution vise à présenter la manière dont le juge international fait face au contentieux relatifs à ces programmes de collecte, stockage et utilisation massifs de données à caractère personnel. La pratique juridictionnelle internationale est encore peu développée et se limite pour l'heure au continent européen à travers l'action de la Cour européenne des droits de l'homme et de la Cour de justice de l'Union européenne. Les deux juridictions régionales reconnaissent aux États une large marge d'appréciation dans la définition des exigences de sécurité nationale justifiant ces mesures de surveillance mais le contrôle n'en est pas moins strict et le caractère massif de la surveillance semble, par nature, être contraire aux engagements des États européens en matière de protection des droits de l'homme.

La garantie du droit au respect de la vie privée face au fichier

Vanessa Barbé
Maître de conférences
Université d'Orléans

Classiquement considérée comme une sphère d'intimité dans laquelle une personne publique ou privée ne peut pénétrer sans y avoir été invitée, la garantie de la vie privée semble nécessaire dans une société démocratique, particulièrement en matière de conservation et de traitement des données personnelles.

Pour la Cour européenne des droits de l'homme, « *la notion de vie privée est une notion large non susceptible d'une définition exhaustive* » (CEDH 29 avril 2002, *Pretty c/ Royaume-Uni*). Dans l'arrêt *Gardel c/ France* du 17 décembre 2009, elle y inclut la droit à la protection des données personnelles : « *la mémorisation par une autorité publique de données relatives à la vie privée d'un individu constitue une ingérence au sens de l'article 8 (sur le droit au respect de la vie privée). […] La protection des données à caractère personnel joue un rôle fondamental pour l'exercice du droit au respect de la vie privée et familiale consacré par l'article 8 de la Convention. La législation interne doit donc ménager des garanties appropriées pour empêcher toute utilisation de données à caractère personnel qui ne serait pas conforme aux garanties prévues dans cet article* ».

Toutefois le droit au respect de la vie privée est un droit fondamental récent qui ne semble pas bénéficier d'une protection aussi extensive que d'autres droits comme la liberté d'aller et venir ou la liberté d'expression. En effet, il est souvent considéré comme le corollaire de la liberté individuelle, mais paradoxalement, alors que les atteintes à la liberté individuelle sont contrôlées en amont par un juge, ce n'est pas le cas des atteintes au droit au respect de la vie privée.

La présente contribution vise à s'interroger sur les évolutions et les fondements des droits constitutionnel et européen qui excluent la compétence judiciaire en tant qu'autorité de contrôle préalable des atteintes à la vie privée causées par la collecte et la conservation de données dans les fichiers, et sur la pertinence de l'intervention d'une autorité administrative indépendante qui est en revanche considérée comme une garantie nécessaire et suffisante.

Fichiers et manifestation de la vérité dans le procès pénal

Vincent Sizaire
Maître de conférences associé
Université Paris Ouest Nanterre La défense

Ayant connu un essor remarquable depuis une quinze années, la place des fichiers pénaux ou para-pénaux dans le procès pénal ne manque pas de questionner. Ces outils sont souvent présentés par le législateur comme un vecteur de modernisation, d'efficacité voire d'efficience de la réponse pénale.

Mais, du point de vue de l'Etat de droit, ils constituent avant tout une atteinte à la vie privée qui, dans une société démocratique, se doit d'être strictement nécessaire et proportionnée. C'est pourquoi il convient d'analyser non seulement la réalité de leur apport à la constatation et à l'élucidation des infractions, mais également les conditions dans lesquelles les fichiers sont utilisés à cette fin.

C'est ainsi que nous pouvons observer que si leur contribution à la manifestation de la vérité est réelle, le cadre dans lequel elle intervient reste toutefois insuffisant pour garantir la proportionnalité et, partant, l'efficacité de cette utilisation.

Réflexions sur la nature et les fonctions du fichier en droit pénal

Sébastien Pellé
Professeur de droit privé
Université de Pau et des Pays de l'Adour

L'intervention propose de s'interroger sur la nature et les fonctions de l'inscription sur un fichier en droit pénal.

La réponse n'est pas évidente en raison de la multiplication du nombre des fichiers qui peuvent intervenir à des stades différents de la procédure. Entre punition et prévention des infractions, la nature juridique de l'inscription sur un fichier est pourtant décisive puisqu'elle commande son régime juridique et, par conséquent, le niveau de protection des libertés individuelles. Au regard des finalités du droit pénal, l'interrogation invite ainsi à revenir sur la distinction entre la peine au sens strict et la mesure de sûreté.

Au-delà, et en considérant certains types de fichiers en particulier (comme le FIJAIS), il s'agit de proposer une réflexion globale à partir de l'idée de surveillance post-peine. Le fichage ne serait alors que l'une des manifestations d'une politique pénale plus large.

LES FICHIERS ADMINISTRATIFS, INSTRUMENTS DE L'ACTION PUBLIQUE

Jacques Chevallier
Professeur émérite de l'Université Panthéon-Assas (Paris 2)
CERSA-CNRS

Présente dès l'édification des États modernes, la technique des fichiers n'a cessé de s'étendre et de se perfectionner : aucune administration quelle qu'elle soit ne saurait désormais se passer d'un instrument nécessaire au bon exercice de ses missions. Si l'informatisation donne au fichage administratif une portée nouvelle, les fichiers administratifs même numérisés continuent à remplir les trois types de fonctions inhérentes à leur institution et autour desquelles ce propos sera construit. Ce sont d'abord des *instruments cognitifs*, qui permettent d'accumuler et de stocker les informations nécessaires au déploiement de l'action publique et à la constitution d'une mémoire administrative (I). Ce sont aussi des *instruments de contrôle et de surveillance*, via la collecte d'informations nominatives concernant tout ou partie de la population (II). Ce sont enfin des *instruments de gestion*, destinés à rationaliser la fourniture de prestations de service public (III). Ces trois fonctions ne sont pas exclusives l'une de l'autre : un même fichier peut tout à la fois être un moyen de connaissance de la réalité sociale, servir au contrôle ou à la surveillance d'une frange de la population et être utilisé pour la fourniture de prestations.

Le fichier, levier de la performance des collectivités territoriales

Spieth Gregory
Maître de conférences en Sciences de Gestion
Université d'Orléans

Le secteur public français a longtemps été analysé autour d'une bureaucratie administrative reposant sur une vision du citoyen assujetti prenant essentiellement la forme d'un administré-contribuable ayant des droits et des devoirs. Les relations entre l'administration et les habitants sont alors règlementaires, unilatérales (mesures descendantes) et coercitives. C'est la puissance publique détentrice du savoir et de la légitimité qui oriente les actions publiques en fonction des besoins qu'elle détermine pour les bienfaits de la population. Le resserrement des contraintes budgétaires liées à la crise financière amène les responsables locaux à envisager une rationalisation de la gestion publique. En effet, la complexité croissante des systèmes d'action publique implique une multiplication des coopérations institutionnelles. C'est donc dans l'optique d'une rénovation de la gouvernance, que la sphère publique tente depuis quelques années de modifier les frontières de son organisation. Cette redéfinition managériale des indicateurs de la performance publique permet de prendre en considération la spécificité des configurations locales. Cette réorganisation correspond, non seulement au souci de rationaliser les services, mais aussi à rapprocher le décideur de son lieu d'action. Cette recherche de proximité se retrouve dans les réponses aux attentes de la population, dans la recherche d'une meilleure satisfaction des citoyens et dans l'assurance d'une meilleure cohérence des décisions prises.

La gestion de la relation avec l'usager/client intervient donc comme une variable importante dans le management des collectivités territoriales. Ainsi, l'utilisation des capacités de traitement et d'archivage des technologies de l'information et de la communication (TIC) *via* le fichier informatique, s'inscrit dans le cadre d'une rationalité tournée vers le citoyen. En réalité, l'impact des TIC peut être analysé selon deux courants. Une approche tend à présenter les TIC comme prétexte à questionner des pratiques déjà existantes. La conceptualisation de l'administration électronique n'est alors qu'une actualisation de procédés anciens. Une autre approche partagée par la présente contribution s'attache à faire reconnaître le potentiel réel offert par les TIC. Ainsi, comme toutes les techniques d'information, le fichier numérique suggère des transformations des cadres conceptuels. Son développement provoque une forte diminution des coûts de transmission de l'information et une extension des possibilités de traitement de l'information. Ces évolutions technologiques influent sur la coordination productive de deux manières. Au sens strict, à structure productive donnée, le développement de l'utilisation du fichier numérique diminue le coût de l'échange de données et d'informations entre les administrations et les usagers, tout comme il modifie les conditions d'exercice du contrôle à distance. Plus largement, le développement de l'utilisation du fichier modifie les techniques de production des services, c'est-à-dire non seulement la division des tâches mais aussi la façon dont ces tâches sont exécutées. Les nouvelles possibilités offertes par la modernisation technique des systèmes d'information, amènent les collectivités territoriales à se pencher sur le rôle d'un citoyen à la fois usager, client et contribuable dans la gestion des services publics. Ces nouvelles approches du public supposent donc, de la part de l'administration, de dépasser la conception classique - c'est-à-dire asymétrique, inégale et unilatérale - de son pouvoir pour se tourner, vers une approche collaborative de la relation entre l'administration et le citoyen. Ainsi, couplée et subordonnée aux structures publiques locales, les fichiers visent à favoriser l'efficacité de l'action publique et collective par des mécanismes de quasi marché. A l'heure des réseaux, les outils numériques appréhendés comme des nouveaux espaces de stockage facilitent le traitement et la transmission des données. De plus, il semble être une variable indispensable dans la conduite du processus de qualité d'un service public. Au-delà de ces affirmations, qu'en est-il, en pratique pour les collectivités territoriales de ces systèmes d'information proclamés comme déterminants à l'accomplissement de l'action publique ? Quel est alors l'impact de l'information fournie par les fichiers sur la gestion des services publics ?

Mots clefs : performance, fichier, système d'information, archivage, traitement

La transparence de l'action administrative à l'épreuve du fichier

Jean-François Kerléo
Maître de conférences en droit public
Université Jean Moulin Lyon 3

La dialectique toujours contrariée entre la transparence et le secret prend une dimension toute particulière lorsqu'elle porte sur la question des fichiers de l'administration. Si la gestion par voie de fichiers déjoue les tentations d'instaurer une « administration de verre », elle fait également ressurgir brutalement la transparence comme en atteste l'adoption de la loi du 6 janvier 1978 après les révélations du fichier SAFARI. La transparence sera ici entendue *a minima* comme un ensemble de techniques juridiques fondées sur une réévaluation du rapport savoir/pouvoir, proche de la philosophie de Michel Foucault, en renvoyant à un processus d'accès à l'information dans un but de contrôle, d'efficacité ou de légitimation. Il y a transparence administrative lorsque le savoir et le pouvoir sur le fichage profitent également aux citoyens, et ne sont pas réservés à l'administration.

Être informé de la création d'un fichier administratif constitue un préalable indispensable à la réalisation des droits des administrés. Or, le droit ne contient pas de règles juridiques permettant, d'une part, de contenir la pratique du fichage et, d'autre part, d'en limiter l'usage par l'administration. Aucune autorité ne contrôle le bien-fondé du fichage en lui-même, seule sa conformité avec les obligations de la loi de 1978 sont contrôlées à partir du principe de finalité. En dépit des contrôles actifs de la CNIL, les pratiques occultes de l'administration continuent de se développer sans possibilité de les contenir.

Selon la loi du 6 janvier 1978, l'administration peut collecter et traiter les données à caractère personnel des administrés qui disposent en contrepartie d'un droit d'accès, de rectification et de suppression. Ces pouvoirs de l'administré sont conditionnés par la connaissance préalable de l'existence d'un fichier, ici dénommé savoir. Or, le consentement préalable de l'intéressé n'est pas toujours requis pour la création d'un fichier administratif ce qui, en anéantissant le savoir, écarte tout pouvoir d'action de l'administré sur le fichage. Si la plus grande transparence résulte de la liaison entre le savoir et le pouvoir, cette concordance reste aujourd'hui insuffisante, en dépit des nombreuses obligations légales.

Il apparaît, en conclusion de cette réflexion, que la reconnaissance et la protection d'un droit des lanceurs d'alerte renforceraient la transparence administrative en instaurant au sein de l'administration un système panoptique, et en érigeant les citoyens en véritable Tribunal de l'opinion publique.

Le fichier, moyen d'inclusion de l'administré et du gouverné au sein de la collectivité

Julien Thomas
Maître de conférences en droit public
Université de Rouen

Alors que leur développement est perçu comme un moyen d'exercer une emprise sur la société, il est intéressant de constater que les fichiers sont aussi des outils au service de l'individu. Considéré comme gouverné ou administré, son existence est reconnue par l'Administration, des prestations lui sont ouvertes du fait de l'inscription sur des fichiers. Il trouve la possibilité d'une implication dans la vie de la collectivité au moment de son inscription sur les listes électorales et peut accéder à des informations utiles au contrôle des gouvernants.

Cette analyse abordera les relations nouées entre l'individu et la collectivité, qu'elles relèvent de l'inclusion ou de la participation, qu'elles soient contraintes ou libres.

A qui appartiennent les fichiers ?

Valérie-Laure Benabou

Professeur de droit privé

Université de Versailles-Saint-Quentin-en-Yvelines

Après avoir tenté de définir le fichier, il s'avère qu'on peut dégager deux valeurs différentes ; celle du contenu et celle du contenant, lesquelles sont intimement mêlées mais sont toutefois dissociables.

Il convient de voir si ces deux valeurs sont le siège de possibles appropriations et si oui à quel titre et par qui ? En second lieu, au regard des difficultés à caractériser systématiquement les fichiers comme étant des sièges de propriété, il convient de réfléchir à la nécessité de s'interroger sur la nécessité d'utiliser la figure propriétaire pour accompagner les échanges de fichiers.

Le fichage de l'internaute : quels garde-fous ?

Nathalie Mallet-Poujol

Directrice de Recherche au CNRS

ERCIM - UMR 5815

Université Montpellier I

Les traces, visibles ou invisibles, laissées par l'internaute sur la toile, sont susceptibles d'alimenter de multiples fichiers. Comment garantir à l'individu que sa navigation sur l'internet respecte ses libertés individuelles ? Ce fichage est-il inéluctable ? Quels garde-fous peut-on y opposer ? Les réponses apportées, supposent, au delà de la pure technicité juridique, des choix de société. Elles ouvrent - ou alimentent - des débats fondamentaux et nécessitent des arbitrages, de plus en plus difficiles, entre les impératifs de protection de l'individu et certains impératifs d'intérêt général. La protection de l'internaute suppose, dans l'absolu, une maîtrise individuelle du fichage, à travers le recueil de son consentement et la reconnaissance d'une forme de droit à l'oubli numérique, droit à l'effacement ou au déréférencement. Elle suppose aussi une maîtrise institutionnelle du fichage, à travers une limitation de la durée de conservation des données, des restrictions à leur transmission et un contrôle opéré par des autorités administratives indépendantes.

Les fichiers de contrôle interne à l'entreprise : le cas des salariés

Damien Chenu
Maître de conférences en droit privé
Université d'Orléans

Le droit du travail ne possède pas une définition particulière du fichier, ni même une appréhension particulièrement originale.

La singularité du droit social s'illustre dans ces circonstances lorsque l'employeur ou le salarié entend consulter ou utiliser un fichier dont le contenu relève de la confidentialité professionnelle ou personnelle.

Dans ces circonstances, le droit du travail offre un riche panel de solutions dont le point d'équilibre est constamment réévalué au gré des nombreuses actualités jurisprudentielles.

Les fichiers de contrôle externe à l'entreprise: le cas des assurés

Matthieu Robineau
Maître de conférences à l'Université d'Orléans – EA 1212

L'activité d'assurance repose notamment sur la collecte et le traitement de données permettant d'évaluer les risques et de tarifer les garanties. En la matière, les fichiers sont donc omniprésents. Ils jouent également un rôle non négligeable dans la lutte contre la fraude à l'assurance.

La protection des données personnelles est dès lors une préoccupation majeure pour les entreprises d'assurance, au point qu'il est possible d'affirmer que celles-ci sont soumises à deux autorités de contrôle, l'ACPR (Autorité de contrôle prudentiel et de régulation) et la CNIL (Commission nationale de l'informatique et des libertés). En concertation avec les assureurs, la seconde a d'ailleurs élaboré un référentiel destiné à faciliter les pratiques et à fluidifier les procédures mises en œuvre par les assureurs lorsqu'ils traitent des données personnelles. Des autorisations uniques et des normes simplifiées ont ainsi été adoptées ces dernières années. Elles ont pour objectif de concilier l'impératif de protection de la vie privée des assurés et les nécessités de l'opération d'assurance, dans un environnement particulièrement concurrentiel.

La révolution du *big data* et l'explosion des objets connectés conduisent à s'interroger sur l'efficacité et la pertinence de la conciliation opérée. Les enjeux ne sont pas minces : si d'ores et déjà, les assureurs disposent de divers instruments de contrôle des assurés, leur accès élargi et simplifié aux données personnelles de ces derniers conduit à densifier le contrôle et, sans doute, à bouleverser l'activité d'assurance. Aussi comprend-on que si les fichiers sont un instrument de contrôle des assurés, il importe plus que jamais de contrôler les fichiers des assureurs.

I – Les fichiers de contrôle des assurés
II – Le contrôle des fichiers des assureurs

Les fichiers des indésirables

Stéphanie Mauclair
Maître de conférences à l'Université d'Orléans

Afin de protéger des données parfois sensibles, la loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés a été promulguée. Puis en 2004, le législateur a modifié cette loi par celle du 6 août 2004 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel. Les dispositions de cette législation concernent toutes les entreprises et tous les organismes dès lors qu'ils mettent en œuvre le traitement de données à caractère personnel (vidéosurveillance, fichiers clients, fichiers du personnel, accès par badge…). Parmi la multitude des fichiers qui existent, on peut relever celui des indésirables. L'indésirable dans le langage courant est celui que l'on souhaite éviter, celui auquel on ne préfèrerait ne pas avoir à faire, parce qu'il dérange… Il dérange par son comportement ou encore par ses opinions. Or, les particuliers ne sont pas les seuls à vouloir éviter les indésirables, les entreprises, les associations, les syndicats aussi, et ce, pour plusieurs raisons. Il peut s'agir de se prémunir contre un risque d'impayé (bannir les mauvais payeurs) ou bien prévenir les contentieux en excluant les clients trop « tatillons » ou enfin se préserver des incivilités en interdisant les supporters trop « démonstratifs ». Ces raisons et bien d'autres encore pousseront ces organismes à créer des fichiers pour identifier et éviter ceux qu'ils jugent indésirables. Or, au regard de la loi de 1978, tout ne saurait être permis, il existe ainsi des fichiers illégaux, des indésirables que l'on ne peut évincer et des fichiers autorisés, des indésirables qu'il est possible de ficher. Reste à déterminer la frontière entre le bon et le mauvais indésirable. Se dégage alors de la loi tout un arsenal de conditions permettant d'établir cette frontière et tentant d'assurer, autant qu'il est possible, aux individus une garantie efficace de la protection de leurs données personnelles.