Le fichage et le respect du droit à la vie privée

Dumortier, Franck

Published in:
L'état des droits de l'homme en Belgique : rapport 2008

Publication date:
2009

Document Version
le PDF de l'éditeur

2. Le fichage et le respect du droit à la vie privée

Par **Franck Dumortier**
Membre de la Commission Justice de la Ligue des droits de l'Homme
Assistant en droit et chercheur au CRID (Centre de recherches informatique et droit) – FUNDP (Namur)

Le déploiement de nouvelles technologies de l'information et de la communication lié à certains développements sociopolitiques contemporains défient la liberté individuelle en ce qu'ils induisent un type de contrôle particulier communément appelé «fichage». Ce phénomène, qui s'est considérablement amplifié ces dernières années, menace tout particulièrement le droit au respect à la vie privée en raison de plusieurs de ses tendances récentes *a priori* hétérogènes les unes aux autres mais qui pourtant se renforcent entre elles : l'utilisation de technologies d'identification réputées plus précises et plus fiables, un recours accru à la technologie RFID (identification par radiofréquences) permettant la lecture à

distance d'informations personnelles parfois à l'insu des personnes concernées, une conservation toujours plus vaste et plus durable des données collectées, l'émergence d'un nouveau «partenariat public-privé» dans lequel s'efface progressivement la frontière entre les rôles de l'autorité publique et de la société en général, et enfin une conception politique réductrice du rôle du droit fondamental à la vie privée dans une société démocratique.

Des technologies d'identification réputées plus fiables

Il va de soi que plus une personne peut être identifiée avec précision, plus les considérations relatives à la protection de sa vie privée prennent de l'importance. Or on assiste ces dernières années à l'introduction accrue de «technologies d'identification» réputées plus précises et plus fiables des individus. Rappelons tout d'abord que l'État belge vise la généralisation de la «carte d'identité électronique» d'ici à 2009. Par rapport à son ancêtre en carton plastifié, l'une des particularités de la nouvelle carte est de permettre, en sus de l'«identification» en tant que telle de son porteur, l'«authentification» de l'identité de celui-ci lors de l'utilisation d'une application de l'administration en ligne, comme une demande de documents officiels ou de formulaires. Pour s'«authentifier» à l'application en ligne, le détenteur de la carte met celle-ci dans un lecteur et tape un code secret (le code PIN) afin de déverrouiller une clé électronique. En cas de piratage de la carte, peut donc se poser un problème de confiance excessive dans le système informatique, dans la mesure où pour l'administration il peut paraître évident que celui qui aura entré le «code juste» est «la

personne identifiée», inversant par là même la charge de la preuve de l'authentification. Les craintes liées à une confiance accrue ou exagérée accordée aux identifiants réputés «fiables» est d'autant plus importante dans le cadre des passeports dans lesquels ont été introduits, depuis 2006, des éléments biométriques, c'est-à-dire liés au corps des individus. Dans un premier temps, c'est l'image faciale numérisée du titulaire qui est ainsi utilisée comme moyen d'authentification, mais à partir de juin 2009, les passeports contiendront également les empreintes digitales. Il importe toutefois de souligner que l'identification biométrique est, par définition, un processus statistique, et qu'il serait donc exagéré de considérer qu'elle assure une «identification exacte» des personnes. L'authentification de personnes, par empreinte digitale, est ainsi affectée d'un taux d'erreur normal de 0,5 à 1%. Un risque accru de décisions arbitraires prises sur base d'informations considérées comme infaillibles mais pourtant fausses peut donc découler de l'utilisation de telles technologies.

Le recours aux technologies de lecture à distance

Une seconde tendance récente consiste en l'utilisation croissante de technologies d'identification par radiofréquences (RFID) associant des puces électroniques stockant des données à des lecteurs capables de capter celles-ci à distance. Si ces dispositifs sont au carrefour d'enjeux importants pour le respect du droit à la vie privée, c'est parce que ceux-ci ont pour caractéristique de pouvoir «parler pour nous» sans requérir forcément d'action volontaire de leurs porteurs. Or une condition essentielle au développement de nos relations sociales, que protège

le droit à la protection de la vie privée, est la possibilité que nous avons, en tant qu'individus, de choisir quelle information à propos de nous-mêmes nous voulons communiquer, à qui, et en quelles circonstances. Le risque de voir se développer des traitements de données invisibles et illégitimes est encore accru en cas de défaut de sécurisation des systèmes : dans ce cas, les « données RFID » que nous transportons peuvent être interceptées, sans même que nous nous en apercevions, par des tiers équipés d'un lecteur. Conçues au départ pour faciliter la gestion des stocks dans le secteur de la distribution, et donc pour suivre un produit en ne révélant qu'indirectement les comportements des consommateurs, les applications de la technologie RFID tendent pourtant à se diversifier tant dans le secteur public que dans le secteur privé.

C'est tout d'abord dans les passeports, équipés depuis 2006 de ces fameuses puces, que l'introduction de la technologie RFID doit inciter à la prudence. En effet, selon plusieurs études européennes, les passeports européens « peuvent être lus et interceptés jusqu'à une distance de 10 mètres du porteur, de façon transparente et sans contrôle interactif ; cette faiblesse est encore aggravée par un contrôle d'accès susceptible d'être contourné ou attaqué, de sorte qu'un tiers, autorisé ou non, peut y avoir accès pour identifier le porteur et le ficher afin de, par exemple, suivre à la trace les touristes dans un pays étranger. »

Ces mises en garde en matière de sécurité ont depuis lors été actualisées par plusieurs chercheurs démontrant, par exemple, que les passeports belges de première génération – c'est-à-dire ceux émis jusqu'en juillet 2006 – ne sont munis d'aucun mécanisme de sécurité et ont pu être lus à distance en quelques secondes à l'insu de leur porteur. Quant aux passeports seconde génération, émis depuis juillet 2006 et équipés de mesures de sécurité

– le Basic Access Control (BAC) –, les chercheurs ont également démontré qu'ils ont pu accéder au contenu de ceux-ci après seulement une heure.

La même tendance est perceptible dans le secteur privé. Ainsi, depuis juillet 2008, la STIB, la Société des Transports Intercommunaux de Bruxelles, remplace ses traditionnels titres de transport en papier par des « pass MoBIB » contenant des puces lisibles à distance. S'il semble que la puce en elle-même ne contienne que le numéro de la carte, le nom, le prénom, l'âge et les informations de facturation du titulaire, aucune information quant à la sécurisation cryptographique de la puce n'a été publiée par la STIB à ce jour. De plus, une base de données externe conserve, quant à elle, pour chaque voyageur, l'ensemble des lieux et des dates de pointage reliées au numéro unique de la carte. Il en découle de sérieuses craintes quant à une surveillance possible des déplacements de chacun en cas d'accès illégitime à la banque de données. En cas de faille de sécurité ou d'accès illégitime, il serait ainsi possible de croiser les trajets de tous les voyageurs pour découvrir qui va où et en même temps pour établir, par exemple, la liste des participants à une manifestation en comparant les noms de ceux qui sont arrivés à De Brouckère avec ceux qui, un peu plus tard, sont partis de la gare du Midi.

Outre les passeports et les tickets de transports, les écoles menacent elles aussi d'être infestées par les puces RFID. Ainsi, la commune de La Bruyère, dans la province de Namur, a décidé d'en accrocher aux cartables des enfants dans le but d'enregistrer leurs entrées et sorties de la garderie et de facturer le service. Si la finalité du traitement mis en place par la commune de La Bruyère semble être justifiable, encore fallait-il choisir les moyens les moins attentatoires à la vie privée pour

l'atteindre. C'est ce que l'on appelle, dans le jargon juridique, le principe de proportionnalité qui a été maintes fois rappelé par la Cour européenne des droits de l'Homme et repris dans la loi dite « vie privée » (loi du 08 décembre 1992). À cet égard, le groupe consultatif européen en matière de vie privée a précisé que « la pertinence d'un tel système [surveillance par badge RFID] doit être justifiée au regard des risques spécifiques en jeu, particulièrement lorsque d'autres méthodes de surveillance existent ». Il a également estimé que, « en évaluant la situation, il faut particulièrement prendre en compte le statut de l'enfant dont les données font l'objet d'un traitement, en gardant à l'esprit son intérêt supérieur ». Or, « *a priori*, ce principe exige que la vie privée de l'enfant soit protégée le mieux possible, en donnant le plus large effet possible au droit à la protection des données de l'enfant ». Au vu des risques de sécurité inhérents à technologie RFID, on peut légitimement se demander si cette analyse de proportionnalité a été réalisée de manière adéquate. L'utilisation de cette technologie est d'autant plus critiquable que les enfants s'habitueront à être contrôlés de manière automatique en perdant ainsi leur sens critique. L'enjeu est là et il est inquiétant que ce soit le lieu de l'apprentissage par excellence – l'école – qui leur enlève ainsi le sens critique fondamental à leur épanouissement. De plus, le projet de la commune consistant à vouloir faire payer davantage les parents qui sont soucieux de prémunir leurs enfants de l'effet liberticide des puces porte atteinte à leur liberté de choix, pourtant protégée par leur droit au respect de la vie privée.

Une conservation plus longue et plus vaste des données collectées

Une troisième tendance consiste en une conservation de plus en plus vaste et durable des données collectées tant dans le secteur public que dans le secteur privé.

En ce qui concerne le secteur public, il semblerait que, depuis 1998, les polices locales et la police fédérale procèdent à des fichages de citoyens, via la Banque générale de données. Cette mesure concernerait 1,6 million de citoyens, qui seraient aujourd'hui fichés pour l'une ou l'autre raison. La police semble pourtant considérer comme insuffisante l'étendue des enregistrements dans cette base de données puisque, tout récemment, un avant-projet d'arrêté royal concernant le fichage des citoyens belges prévoyait d'étendre les données pouvant être collectées par les forces de l'ordre à des données extrêmement sensibles comme celles relatives à la race ou à l'ethnie, aux opinions politiques, à la santé physique ou psychique, aux situations et comportements à risques, aux données relatives à la vie sexuelle, ou encore aux données de localisation électroniques (GSM, GPS...), d'identification électroniques (IP, cookies...) et biométriques. Ces données extrêmement sensibles pourraient être collectées et conservées en cas d'« intérêt concret » pour la mission de police administrative ou de police judiciaire poursuivie. La notion d'« intérêt concret » est cependant tellement vague qu'il n'est pas requis qu'une personne soit soupçonnée ou ait commis une infraction pour que ses données « psychiques » ou « sexuelles » soient reprises dans la banque de données : faire partie d'un « groupe de pression » tels certaines associations, certains syndicats ou certains partis politiques suffit. Vu les points sensibles auxquels touche la mesure,

il est plus que regrettable que l'extension du fichage des citoyens belges par les forces de l'ordre soit réglée par voie d'un arrêté royal, évitant ainsi un débat démocratique fondamental au sein du Parlement.

La tendance à la conservation accrue des données par les autorités publiques est encore renforcée par un nouveau paradigme de « partenariat public-privé » imposant, par exemple, aux opérateurs de télécommunications de conserver un grand nombre de données afin de « faciliter » le travail de la police.

L'émergence d'un nouveau paradigme de « partenariat public-privé »

Traditionnellement existait une frontière claire entre les missions d'intérêt public de l'État et les intérêts des particuliers. Ainsi, les contrôles d'identité tout comme la prévention et la répression des infractions pénales relevaient normalement de la compétence exclusive des autorités publiques. Petit à petit cette frontière tend cependant à s'estomper. Deux exemples permettent d'illustrer ce propos : d'une part des opérateurs privés sont soumis à une obligation de conservation de données dans le but de faciliter le travail des forces de l'ordre, de l'autre la nouvelle carte d'identité électronique permet certaines utilisations par des organismes privés.

En ce qui concerne notre premier exemple, rappelons que, le 15 mars 2006, le Parlement et le Conseil de l'Union européenne ont adopté la directive 2006/24/CE relative à « la conservation de données générées ou traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public ou de réseaux publics de communications ». Cette directive

a été adoptée dans le but d'obliger les opérateurs de télécommunications et les fournisseurs d'accès à Internet à conserver entre 6 et 24 mois les données relatives au moment, au lieu, à la durée, à l'ampleur et à la modalité d'une conversation téléphonique, d'un SMS ou d'un e-mail. De cette façon, les institutions européennes veulent garantir que ce genre de données soient disponibles pour examiner, rechercher et poursuivre la criminalité grave. Dans ce dossier, outre que l'obligation de collaboration du secteur privé est étendue dans une mesure sans précédent, c'est la proportionnalité de la mesure qui pose question. En effet, dans la pratique, le stockage du trafic des télécommunications paraît être non seulement une mesure inadaptée, mais il entraîne également, pour toutes les parties concernées, une charge financière et pratique déraisonnable. De plus, à l'heure du GSM et d'Internet, le fichage de l'ensemble des communications des individus peut porter une sérieuse atteinte au droit de « nouer des relations sociales avec un minimum d'ingérence » tel qu'il a été consacré par la Cour européenne des droits de l'Homme. Enfin, ces mesures risquent de renverser le principe démocratique selon lequel chacun est présumé innocent jusqu'à la preuve du contraire. Le dossier de la rétention des données en Belgique est d'autant plus sensible que le gouvernement pourrait être tenté de régler nombre de questions importantes – telles la durée de conservation ou les données exactes à conserver – par voie d'arrêté royal, évitant à nouveau un débat démocratique fondamental au sein du Parlement.

Le second exemple de confusion entre les rôles respectifs de l'autorité publique et du secteur privé découle de la nouvelle carte d'identité électronique. Outre ses fonctions d'identification et d'authentification, celle-ci

aurait également pour mission, notamment, de nous identifier, *via* la signature électronique, lors de transactions électroniques auprès d'entreprises privées. Si la question prête peut-être à sourire, les risques de troubles et de confusions dans le rôle d'une part d'un service public, d'autre part d'une entreprise privée contribueront à confirmer que l'État s'assimile progressivement à un prestataire de service et que de moins en moins de critères distinctifs (qui passent notamment par la symbolique de la Maison communale ou les rapports entretenus avec des fonctionnaires identifiés) ne permettent de le distinguer d'un opérateur lucratif.

Une conception politique réductrice du rôle du droit fondamental à la vie privée

L'ensemble des tendances évoquées en matière de fichage tendent à confirmer l'émergence d'une conception politique réductrice du rôle du droit fondamental à la vie privée dans une société démocratique. Ainsi les intérêts sécuritaires et de facilité d'utilisation (*usability*) tendent à devenir des arguments permettant de justifier des ingérences de plus en plus importantes dans ce droit fondamental. Tout d'abord, depuis les attentats du 11 septembre 2001, les conceptions relatives au respect du droit à la vie privée ont été bouleversées. Un climat particulier s'est instauré, dans lequel le droit à la protection de la vie privée est minimisé par rapport à l'aspiration à la sécurité. D'autre part, une certaine banalisation des atteintes au droit à la vie privée au sein de l'opinion publique – beaucoup se dévoilant, par exemple, de leur propre chef dans des réseaux sociaux, tel Facebook – permet tant au secteur public qu'au secteur privé de généraliser l'introduction de technologies liberticides dans un nombre de secteurs croissants sans opposition audible. Cet état de fait est rendu possible par la persistance de la croyance selon laquelle si l'on n'a rien à cacher, on n'a rien à craindre.

Rappelons toutefois que le droit à la protection n'est pas un droit fondamental comme les autres. En effet, il conditionne l'effectivité de bon nombre d'autres droits et libertés telles la liberté d'association et d'expression, à tel point que certains ont pu voir dans le droit à la vie privée l'expression d'un « droit fondamental fondamental ». Le droit à la protection de la vie privée a ainsi pour but de protéger des comportements, attitudes et modes de vie qui, sans être illégaux ni sans causer dommage à autrui, sont néanmoins impopulaires et exposeraient ceux qui s'y adonnent à l'animosité ou à des réactions discriminatoires ou stigmatisantes de la part de tiers s'ils en avaient connaissance. L'on voit ici que le droit à la protection de la vie privée et l'interdiction des discriminations fondées sur des motifs non pertinents s'inscrivent dans la même optique. Il s'agit de préserver un certain « droit à la différence », essentiel à la fois pour l'individu comme condition nécessaire à son épanouissement personnel, mais également pour l'évolution et la vitalité de la société dans la mesure où ce « droit à la différence » autorise l'expression de modes de vie et de pensée innovants, source d'expérimentations individuelles et collectives.

En cela, un enjeu essentiel du droit à la protection de la vie privée est la représentation de l'humain, et la restitution des logiques absolues de sécurité et d'efficacité économique à leurs cadres relatifs. Alors que le dogme sécuritaire fait de tout individu un suspect par défaut et que la logique économique en fait un être essentiellement rationnel et égoïste, rendre possible la contestation de ces

logiques absolues est d'autant plus urgent qu'à force de déployer, à travers notamment les dispositifs technologiques de la société de l'information, des représentations aussi négatives de l'individu, on risque effectivement de susciter des comportements qui justifieront *in fine* ces logiques sécuritaire et économique absolues, mais au prix de la plus précieuse de nos aptitudes : la liberté.

Pour aller plus loin

Profiling the European Citizen, M. Hildebrandt & S. Gutwirth (Eds), Springer, 2008

« The right to informational self-determination and the value of self-development. Reassessing the importance of privacy for democracy », A. Rouvroy and Y. Poullet, dans *Reinventing Data Protection*, Springer, 2009 (à paraître), disponible à l'adresse suivante : http://works.bepress.com/antoinette_rouvroy/7

« Privacy, Data Protection, and the Unprecedented Challenges of Ambient Intelligence », A. Rouvroy, dans *Studies in Ethics, Law, and Technology*, Berkeley Electronic Press, 2008, disponible à l'adresse suivante : http://works.bepress.com/antoinette_rouvroy/2

L'utilisation de la biométrie et des RFIDs dans le cadre de l'espace européen de liberté, de sécurité et de justice : une affaire de balance ou une question de dignité ?, F. Dumortier, ERA-Forum, 2009 (à paraître)

RFID : la police totale, collectif Pièces et main d'œuvre, L'Échappée, 2008