Tous fichés, tous fliqués.

Les précaires en première ligne et à la croisée des contrôles.

Prémisses.

David Lannoy ▪ Mars 2016

Au nom du progrès, de la facilité, du bon sens, de la lutte contre la fraude ou le terrorisme, nos données personnelles sont de plus en plus collectées, échangées, décortiquées, croisées… Qu'elle soit d'ordre commercial ou le fait des pouvoirs publics, l'analyse de nos données personnelles semble ne plus connaître aucune limite.

Consommation énergétique, défauts de payements, informations relatives à leur état de santé… Les citoyens les plus précaires sont souvent les premiers cobayes des nouvelles méthodes de fichage et de flicage. Ce document tente de dresser l'état des lieux de ce qui se fait actuellement mais aussi d'analyser « l'avenir radieux » que certains nous préparent.

CENTRE D'ÉDUCATION POPULAIRE
ANDRÉ GENOT
rue de Namur 47 • 5000 Beez
T. 081/26 51 52 • F. 081/26 51 51
cepag@cepag.be • www.cepag.be

Introduction

C'est lorsque le cocktail des difficultés économiques, sociales et politiques rend l'Etat peureux que le contrôle des citoyens et, plus singulièrement, des allocataires sociaux et des étrangers se renforce au nom de l'efficience des politiques sociales, de la lutte contre la fraude sociale, de la mise en sécurité des citoyens et de la nation.

De tout temps, gouvernements et puissants ont tenté de ficher les citoyens qu'ils craignaient. Le fichage officiel, en France, date du XIX^{ème} siècle pour les criminels récidivistes et les anarchistes.

Aujourd'hui, les gouvernements possèdent des outils des plus efficaces : les puces, l'informatique, facebook, la téléphonie, l'ADN, les caméras de surveillance… Mais aussi les services sociaux, leurs banques de données, les outils de croisement de celles-ci, les services privés de consommation… De plus en plus fréquemment, ces différents organismes collaborent pour répertorier, s'échanger, croiser des données privée.

La confidentialité de nos vies et de nos relations s'étiole. La vie privée se rétrécit.

Des informations sensibles et hautement personnelles sont amassées et accessibles par plusieurs personnes et/ou organismes sans le moindre contrôle réel.

Que ce soient les dossiers médicaux, sociaux, les crédits, les difficultés de payement, les comportements de consommation, les appartenances idéologiques… ces données sont récoltées et croisées. Elles peuvent être consultées par un nombre croissant d'intervenants et utilisées contre les citoyens, plus particulièrement pour retirer certains droits aux plus précaires et fragiles d'entre eux. Un contrôle et des sanctions qui s'exercent d'une manière de plus en plus arbitraire, insidieuse, inégalitaire et excessive.
Nos vies sont de plus en plus tracées et déprivatisées.

Il est urgent de se pencher sur ce phénomène et ses graves dérives. Afin, dans un premier temps et dans les prochaines analyses, de dresser l'état des lieux de ce qui se fait déjà dans plusieurs domaines. Mais aussi et surtout de se prémunir à moyen et long terme contre « l'avenir radieux » que certains veulent nous imposer. Pour que les générations futures n'aient pas à vivre un 1984 du troisième millénaire.

Le fichage des citoyens : latitudes injustifiées [1]

Avant de se pencher sur le phénomène du fichage et ses dérives, Manuel Lambert, juriste à la Ligue des Droits de l'Homme, insiste sur l'esprit du temps, le contexte culturel et le climat intellectuel très particuliers.

- D'une part, on a vu se développer une propension des citoyens à dévoiler volontairement des parties de plus en plus vaste de leur intimité. Ce phénomène est relativement surprenant et s'observe aussi bien sur Facebook ou d'autres réseaux sociaux que, par exemple, dans des émissions de téléréalité. Cela a évidemment des conséquences politiques : ce contexte socioculturel rend moins scandaleuses des mesures d'atteinte à la vie privée comme l'installation de caméras de surveillance ou la proposition d'intégrer les empreintes digitales sur les cartes d'identité.

- D'autre part, les pouvoirs publics et privés (les grandes entreprises, les réseaux sociaux, les agences publicité, les sociétés de télémarketing…) ont développé leur appétit de données à caractère personnel au point d'en devenir littéralement boulimiques, voraces ! La collecte de ces données semble maintenant sans limite : le privé le fait à des fins commerciales, le public à des fins de contrôle.

La combinaison de ces deux phénomènes conduit à ce que des pans de plus en plus larges de notre vie privée soient collectés, triés, analysés et traités tout à fait légalement.

Qui et responsable ?

Il est tout d'abord légitime de s'interroger sur la responsabilité des citoyens eux-mêmes. Ont-ils en effet réellement conscience des conséquences de leurs actes ? On assiste souvent à une attitude nonchalante de la part de certains, à une sorte d'« exhibitionnisme » inconscient. La prise de conscience éventuelle ne survient souvent qu'en cas de problème : contrôle fiscal, poursuites judiciaires, sanction professionnelle...
La responsabilité du secteur privé est toutefois énorme : le marché nous pousse dans cette direction. L'ambivalence n'est qu'apparente : si les gens révèlent leur intimité, ils veulent néanmoins garder le contrôle sur ce qu'ils révèlent. Le citoyen ne renonce pas au contrôle de son image : il met en évidence ce qu'il a envie de mettre et contrôle ce qu'il diffuse sur internet.

D'autre part, on peut se demander si les pouvoirs publics ont un réel besoin d'amasser des quantités démesurées de données pour exercer leurs missions.
Pas moins de vingt données à caractère personnel sont exigées pour établir le passeport – outre la biométrie ! En quoi l'autorité communale a-t-elle besoin de notre numéro de GSM ou notre adresse électronique pour nous délivrer un passeport ?

[1] Cette partie de l'analyse est très largement inspirée des arguments développés par Manuel Lambert, juriste à la Ligue des Droits de l'Homme, à l'occasion d'un colloque organisé par le CEPAG le 18 mars 2016.

De cette situation, et pour amorcer une réflexion sur la question, on peut partir du principe suivant : ce qui n'est pas nécessaire est abusif.

Sécurité/liberté.

S'il y a bien un secteur où la collecte de données est massive c'est dans le cadre dit des politiques de sécurité : la lutte contre la criminalité en général, celle contre le terrorisme en particulier. Depuis une vingtaine d'années, on assiste en effet à une collecte aussi massive que systématique de données à caractère personnel.

Si l'objectif affiché est d'améliorer la lutte contre la criminalité, il faut reconnaître un problème : ça ne fonctionne pas ! Voyons ce qui se passe en matière de lutte contre le terrorisme : l'échec est flagrant. Cela n'a pas empêché les attentats de Madrid, Londres, Boston ou Paris (pour ne parler que de l'Occident).

Pae contre, cette collecte massive et systématique de données à permis d'accentuer la répression contre les opposants politiques, de renforcer l'espionnage industriel et l'espionnage politique[2].

Cette lutte, menée au nom de la liberté et de la sécurité est donc totalement déséquilibrée. Les restrictions et les limitations au respect de notre vie privée sont de plus en plus nombreuses… Mais nous ne vivons pas plus en sécurité !

La principale cause de ce déséquilibre et de cette inefficacité tient dans un mythe : celui de l'infaillibilité technologique et du contrôle total.
Cette légende est erronée car trop d'information tue l'information. La récolte massive de données ne permet pas de lutter efficacement contre le terrorisme ou la criminalité. L'abondance de données inintéressantes et/ou non pertinentes, conjuguée au manque de personnes disponibles pour analyser les informations sont ici en cause.

Rappelons une évidence : l'anonymat, le respect de la vie privée, la liberté d'expression sont des valeurs et des conditions indispensables de notre démocratie.
Le contrôle a un coût social. On constate en effet que le développement du contrôle social touche l'ensemble des citoyens mais cible plus prioritairement les plus faibles : sans emploi, étrangers…
On remarque d'ailleurs que les personnes chargées de gérer et visionner des caméras de surveillance reproduisent les mêmes types de stéréotypes en braquant les objectifs sur une certaine « catégorie » de citoyens plutôt qu'une autre : jeunes, étrangers…

Le fichage

Délimitation du champ d'analyse

[2] Rappelons par exemple que la NSA - la National Security Agency, organisme du renseignement étasunien - a, avec la complicité de tous les acteurs privés des nouvelles technologies de l'information – Google, Microsoft, Facebook, etc… - placé des responsables politiques de différents Etats sur écoute.

Le fichage est une réalité protéiforme et de plus en plus prégnante dans notre société, notamment en raison du développement continu des technologies informatiques.

Historiquement, le fichage remonte loin dans le temps. Il s'est cependant généralisé avec le développement de l'Etat providence. La nécessité pour l'Etat de connaître sa population afin de déterminer qui est en droit, ou non, de bénéficier de mesures de protection sociale a entraîné la constitution de fichiers contenant des données personnelles sensibles.

Avant de se pencher sur le « fichage », il est nécessaire de le définir strictement. Il est en effet organisé pour des objectifs divers et variés : à des fins de surveillance (fichiers policiers), à des fins commerciales (fichiers publicitaires), à des fins politiques/publiques (état civil), à des fins privées (fichiers des membres du CEPAG). On se limitera ici au fichage à des fins de surveillance, celui organisé par les pouvoirs publics, les services de police et de renseignement.

En partant de cette définition, on peut considérer le fichage comme étant l'indexation de personnes comportant des renseignements, confidentiels ou non, à des fins de contrôle et de surveillance.

Formes de surveillance.

L'évolution technologique et l'information croissante de la société ont ouvert la voir à une nouvelle dimension de la surveillance. On peut citer en autres :

- La méthode d'identification biométrique : l'identification automatisée d'un individu à partir de ses propriétés physiologiques[3] ou de ses modes de comportements
- La surveillance par caméra : la gamme d'appareils est très vaste (des caméras statiques à faible résolution et facilement repérables aux caméras zoom miniaturisées et à vision nocturne, souvent dotées de systèmes de reconnaissance du visage ou de la démarche)
- Le monitoring : plus le travail est informatisé et numérisé, plus la surveillance sera aisée et étendue, plus les prestations des travailleurs pourront être contrôlées (citons, par exemple le rythme de travail, la productivité, la ponctualité, le comportement en ligne, la durée et la fréquences des pauses, les entretiens téléphoniques…).
- Les puces RFID (Radio Frequency Identification) : le recours à la technologie RFID ouvre des possibilités inédites de collecte de données et de contrôle, la technologie RFID permettant la lecture de données sans contact et à distance (comme dans le cas de la carte MOBIB de la STIB à Bruxelles)[4].
- La géolocalisation, la téléphonie mobile, les écoutes téléphoniques…

[3] Voyons par exemple la proposition du ministre de l'Intérieur, Jan Jambon, d'insérer les empreintes digitales sur la carte d'identité.

[4] Lire à ce sujet, *La révolution numérique : En route pour un e-avenir radieux ? Sur base des réflexions de Bruno Poncelet*, in « *Objectif « Plein Emploi » : Comment sortir enfin et durablement du chômage de masse ?* », page 3.

Base juridique.

Tout fichage constitue une ingérence dans la vie privée des individus. Dès lors, afin de répondre aux exigences de l'article 8§2 de la Convention européenne des Droits de l'Homme[5], celui-ci doit répondre à trois conditions, à savoir être prévu par la loi, être nécessaire dans une société démocratique et être proportionné à l'objectif poursuivi.

Pour cette dernière exigence, prenons un exemple concret : la consultation des bases de données des fournisseurs d'énergie dans le cadre de la lutte contre la fraude sociale. Est-ce une mesure proportionnelle à l'objectif poursuivi ? Alors que la fraude aux allocations représente seulement 41% de la fraude sociale (contre 47,5% pour les fraudes patronales), on va toucher une large population, déjà très fragilisée, pour récolter quelques millions d'euros…

Pour la suite…

Ce bref état des lieux de la situation actuelle en matière de fichage va nous permettre d'avancer dans cette thématique.

En quoi les mesures actuelles et les projets futurs dans les domaines de la consommation énergétique ou de la Sécurité sociale et des données de santé respectent-ils les cadres légaux ? Quelles sont les dérives déjà observées et à craindre dans le futur ? Quelles questions éthiques l'utilisation de ces données posent-elles ? Que peut-on faire, en tant que citoyen actif, pour limiter ces abus dans le cadre de sa vie privée mais aussi pour s'opposer à leur développement afin de faire respecter les valeurs de notre démocratie ?

Autant de thématiques qui seront développées et qui mèneront nos réflexions dans les analyses à venir. _____

[5] L'article 8, qui traite du Droit au respect de la vie privée et familiale est libellé comme suit :
« 1. Toute personne a droit au respect de sa vie privée et familiale, de son domicile et de sa correspondance. 2. Il ne peut y avoir ingérence d'une autorité publique dans l'exercice de ce droit que pour autant que cette ingérence est prévue par la loi et qu'elle constitue une mesure qui, dans une société démocratique, est nécessaire à la sécurité nationale, à la sûreté publique, au bien-être économique du pays, à la défense de l'ordre et à la prévention des infractions pénales, à la protection de la santé ou de la morale, ou à la protection des droits et libertés d'autrui. »