Société de surveillance, vie privée et libertés

Rapport rédigé par Jean-Claude Vitran et Alain Weber

De nombreux sociologues affirment que le citoyen était plus libre pendant le septennat de Georges Pompidou dans les années 1970 et que depuis une dizaine d'années la surveillance des personnes s'est particulièrement intensifiée.

Il est vrai que depuis 1997, la sécurité est devenue la « première des libertés ».

A partir de cette date, la délinquance qui était auparavant considérée comme la conséquence des inégalités sociales devient l'une de ces causes.

Jamais les révolutionnaires de 1789 ne mentionnent la sécurité dans la déclaration universelle des droits de l'Homme et du citoyen du 26 août 1789 ; l'article II affirme seulement que la sûreté est un droit naturel et imprescriptible.

Comme le dit Robert Badinter[1] « *la sûreté est précisément l'assurance pour le citoyen, que le pouvoir de l'Etat ne s'exercera pas sur lui de façon arbitraire et excessive* ».

La convention européenne des droits de l'homme reprend cette notion en donnant le droit au citoyen d'attaquer son propre Etat quand il porte atteinte à ses libertés fondamentales.

Une autre cause fait le lit de la surveillance généralisée et globale, plus insidieusement, c'est l'idéologie du risque zéro.
Dans notre société moderne, l'angoisse existentielle exacerbe le besoin de sécurité. Nous ne voulons pas que nous-mêmes et nos proches courent des risques ; de notre conception jusqu'à notre dernier souffle, nous demandons à l'Etat de nous garantir notre intégrité, voire de nous garantir l'immortalité.
Ce risque zéro n'existe pas, bien entendu.
L'apprentissage du métier d'homme, l'éducation, vivre tout simplement obligent à des prises de risque permanentes.

L'Etat instrumentalise la demande sécuritaire au point d'en faire un outil politique, et pour entretenir le besoin de sécurité, développe des systèmes de surveillance de plus en plus sophistiqués et généralisés.

Pour s'en convaincre, il suffit de noter le glissement de langage qui fait que l'on nomme maintenant avec un aplomb ahurissant la vidéo surveillance : vidéo-protection voire vidéo tranquillité.

Chacun sait que, preuves à l'appui, ces caméras n'ont jamais protégé personne, ni empêché les délits ; elles permettent d'interpeller éventuellement plus rapidement les coupables.

Plus prosaïquement, elles soignent les angoisses de beaucoup de nos concitoyens.

Avant d'aller plus loin, un peu d'histoire.

Que désigne-t-on sous l'expression « contrôle social »[2].

A l'origine, elle est utilisée dans le sens de maîtrise, les Anglo-saxons ne parlent-ils pas de *self-control* ?

C'est la manière de vivre ensemble et de se supporter. C'est ce qui permet à une société de « vivre en harmonie ».

[1] Le Monde – jeudi 5 février 2009

[2] De la politique de sécurité au contrôle social - Dominique Guibert - H&L N°145

Depuis toujours, les hommes ont cherché des codes, qu'ils soient philosophiques, religieux ou politiques.
Les écrits des philosophes grecs, comme Platon, de ceux du siècle des lumières, Rousseau, Voltaire, et les livres sacrés des religions révélées comportent des codes du respect des consignes pour bien vivre ensemble.

Plus près de nous, la déclaration des droits de l'Homme et du Citoyen est une des normes du contrôle social.

Bien plus tôt en 1215, un texte, la *Magna Carta,* fut rédigé par les barons anglais pour réduire les pouvoirs royaux de Jean sans terre.

Ensuite le 26 mai 1679 les Anglais, encore eux, proclamaient le *Bill d'Habeas Corpus* qui réglait avec précision le droit de l'inculpé et du détenu, et en 1688, les Anglais, toujours eux, mettaient à la porte Jacques II et proclamaient le *Bill of right* qui marquait le passage d'une monarchie de droit divin à une monarchie constitutionnelle basée sur un contrat.

Le 4 juillet 1776, les « Américains » ont par une déclaration, écrite par Thomas Jefferson, proclamé leur indépendance.

Enfin, le 26 août 1789, les députés de l'Assemblée nationale constituante établissent la synthèse des textes anglo-saxons et des idéaux politiques et philosophiques du Siècle des Lumières et rédigent la Déclaration des Droits de l'Homme et du Citoyen.

Tout cela procède du contrôle social, du code du bien vivre ensemble ; de la recherche d'une harmonie qui oscille entre la satisfaction psychologique de l'appartenance à un groupe structuré, d'occuper une position et d'être valorisé dans ce groupe et la mise à l'écart, la punition pour avoir transgressé le code.

Aujourd'hui, le mot « Contrôle » est employé dans son seul sens punitif[3].

Celui de « CONTROLER, VERIFIER, SURVEILLER, TRACER pour SANCTIONNER ».

Et comme l'a dit Michel Foucault[4] « *surveiller, c'est aliéner la pensée et c'est punir* »

Surveiller, ficher les individus n'est pas une envie nouvelle, depuis longtemps, les monarchies et les gouvernements rêvent de tout savoir sur leurs concitoyens pour faire régner la paix sociale.

Depuis Hobbes et les philosophes utilitaristes qui ont suivi, l'Etat est supposé assurer un rôle de protecteur des citoyens.

Les premiers fichiers datent de la fin du règne de Louis XIV, ceux des galériens, puis les fichiers des prostituées, des mendiants, des nomades et des mal-pensants du règne de Louis XV et entre 1800/1810 Joseph Fouché, ministre de l'intérieur de Napoléon 1er, voulait réduire en fiches l'ensemble de ses concitoyens.
Vers 1860, la création des fichiers des Renseignements Généraux, et vers 1900 la capture des empreintes digitales et les débuts de la police « scientifique » ; depuis le nombre des fichiers papier n'a cessé d'augmenter.

Mais c'est l'après-guerre, et surtout la guerre froide, qui ont accentué la référence à la sécurité nationale et au mythe du bien et du mal. « *Tout ce qui n'est pas dans mon camp est contre mon camp* ».

Cette approche a amené les démocraties occidentales à multiplier les moyens de surveillance ; les attentats du 11 septembre 2001 n'ont fait qu'accentuer les dérives appréhendant le citoyen en délinquant potentiel, voire en terroriste en puissance. Chacun d'entre nous est suspect d'une possible atteinte à la sûreté de l'Etat et fait l'objet d'une surveillance, d'un fichage et d'un profilage destinés à permettre sa neutralisation.

[3] Politique sécuritaire et contrôle social, deux faces d'un même danger – Jean Danet
[4] Michel Foucault – Surveiller et punir – Editions Gallimard

La première révolution dans la surveillance du citoyen remonte à novembre 1971 lorsque fut commercialisé le premier micro-processeur qui permit de multiplier de façon exponentielle dans l'espace (capacité de stockage), dans le temps (rapidité de travail), et de diminuer par le prix (abaissement des coûts de fabrication) les possibilités des machines informatiques et du traitement numérique des données.

La seconde révolution, en gestation, c'est la technologie « nano ». Cette hyper miniaturisation, qui tend vers l'invisibilité et l'indétectabilité posera à l'humanité d'énormes problèmes en matière d'éthique et de droits de l'Homme.

C'est le développement anarchique des technologies, sans réflexion citoyenne, et axées essentiellement sur le profit qui pose problème, pas les technologies elles-mêmes.
Cette surveillance, ce fichage, que l'on peut sans exagérer penser qu'il sera, à terme, généralisé, est la conséquence d'une inversion de valeurs : on substitue la présomption d'innocence par la présomption de culpabilité.

Sa matrice purement policière est claire : tous suspects donc tous fichés.

Ses promoteurs poussent même la logique jusqu'à expliquer qu'il est donc un progrès puisque accusés à tort nous pourrions ainsi plus facilement être disculpés.

Compte tenu de l'inversion des valeurs, de la dictature du risque zéro, et de la folie sécuritaire du monde occidental, comment s'étonner que la surveillance globale et généralisée des citoyens soit élevée au rang d'un dogme ?

A cela, il y a lieu d'ajouter la vigueur du secteur marchand qui a fait du domaine de la sécurité un axe de croissance et de développement économique important – et affiche plus de 20 % de croissance annuelle.

Ces acteurs sont si puissants qu'ils influencent les prises de décisions des Etats, et sous couvert de confort, de commodité, créent et développent des systèmes de surveillance de plus en plus sophistiqués et intrusifs.

Les grandes typologies de la surveillance sont :

Surveiller :

La surveillance vidéo.
Il existe deux types de surveillance vidéo.

L'une où les images ne sont pas enregistrées, ni conservées dans des traitements informatisés ou des fichiers structurés qui permettent d'identifier des personnes physiques. C'est le cas des caméras de circulation automobile ou de sécurité sur les quais du métro.
L'autre enregistre et traite les images collectées par les techniques numériques en vue de constitution de bases de données.

Le Royaume Uni et ses 4 millions de caméras constituent le terrain d'expérimentation privilégié des chercheurs qui s'acharnent à démontrer, preuves en main, l'inefficacité patente de la vidéo-surveillance pour lutter contre la criminalité. Un rapport du ministère de l'Intérieur britannique pointe trois faiblesses des dispositifs : la mise en œuvre technique, la disproportion des objectifs assignés à la technologie et le facteur humain.

Le visionnage des images est fonction des préjugés sur le caractère à priori délictueux de certaines attitudes, mais surtout de certaines populations. Une étude révèle que 86 % des individus surveillés ont moins de 30 ans, que 93 % sont de sexe masculin, et que les individus noirs ont deux fois plus de chance de faire l'objet

d'une attention particulière[5], ce qui constitue une discrimination complémentaire d'une population déjà en situation précaire et une atteinte caractérisée aux droits fondamentaux.

En conclusion, la vidéo-surveillance, qui rate son objectif avoué, dissuader et détecter les délits, est surtout un marché lucratif.

Ficher :

C'est collecter des informations et les stocker dans d'énormes bases de données informatiques en vue :
- de gérer (exemple : les fichiers de la sécurité sociale ou des caisses de retraites, etc.) ;
- de renseigner (les fichiers des renseignements généraux, EDVIRPS, SIS, etc.) ;
- d'enquêter et de sanctionner (les fichiers STIC, FNAEG, etc.) ;
- de profiler des citoyens (les fichiers d'Etat : EDVIRPS, ELOI[6], Base Elèves, etc.) ou des individus (fichiers marchands).

Les fichiers de police sont au nombre de 45, bientôt 57 d'après le rapport du groupe de surveillance sur les fichiers[7].
D'autres fichiers administratifs collectent des données tant privées que personnelles. Le fichier des impôts, il connaît tout du citoyen, son identité, son patrimoine, sa situation personnelle, ses revenus, etc.
Les fichiers des banques qui connaissent, comme les impôts, tout de nous, et même des éléments de notre santé pour l'octroi d'un prêt. Bizarrement, ces fichiers bancaires privés sont interconnectés avec le fichier central de la Banque de France qui est un fichier institutionnel.

Les fichiers marchands, au nombre d'environ 2 millions à fin 2008 selon Alex Türck, le président de la CNIL[8].
Ils sont le noyau dur du fichage. Ils sont alimentés par les traces que nous laissons volontairement à l'occasion de transactions avec les commerçants (cartes de chaînes de supermarchés, cartes de fidélité) ou involontairement lors de nos connections sur le Web (signature de pétition, connexions à des sites spécialisés).
Au contraire des fichiers institutionnels où il est, quelquefois difficilement, possible de connaître et de rectifier ses propres informations, les fichiers du secteur marchand sont opaques, peuvent être copiés, et changer de mains. Ces fichiers sont créés dans un but purement commercial et sont source de profits très fructueux.

Fichiers de police :

L'exemple le plus caricatural des dérives du fichage institutionnel est celui du FNAEG.

Ce fichier était à l'origine en 1998 destiné aux fichages des délinquants sexuels et concernait environ 1500 individus, alors qu'aujourd'hui 1 million de personnes sont fichées.
De modifications en 2001 en modifications en 2003 puis 2004, présentées comme essentielles au contrôle et à la protection de la sécurité nationale, presque tous les crimes et délits ont été intégrés, justiciables comme suspects, et les données conservées pendant une période allant de 25 à 40 ans.
Ainsi, aujourd'hui tout citoyen peut se faire prélever son ADN lors d'une garde à vue, pour un simple chapardage comme pour de simples soupçons.

Bizarrement, les délits financiers et politiques ne sont pas concernés par ce fichage.

---

[5] idid

[6] EDIVRPS : Exploitation Documentaire et Valorisation Relative à la Sécurité Publique.
SIS : Fichier d'Information Schengen.
STIC : Système de Traitement des Infractions Constatées.
FNAEG : Fichier National Automatisé des Empreintes Génétiques.
ELOI : Comme ELOIgnement –fichier de contrôle des étrangers.

[7] Rapport Bauer : http://www.ladocumentationfrancaise.fr/rapports-publics/064000885/index.shtml

[8] CNIL : Commission Nationale Informatique et Libertés – www.cnil.fr

L'autre exemple est le Fichier EDVIGE.

Jusqu'au 28 juin 2008, deux organismes de renseignements étaient à la disposition de nos gouvernants, la DST - Direction de la surveillance du territoire – office de contre-espionnage - et les RG – Renseignements généraux. Pour des raisons de compression budgétaires, mais aussi politiques, ces deux officines ont été réunies[9] en une Direction centrale du renseignement intérieur.

A cette occasion furent créés, par arrêté le 1er juillet 2008, deux nouveaux fichiers, EDVIGE[10] et CRISTINA[11].

Le fichier EDVIGE portait atteinte au principe de finalité[12] car il mélangeait les personnes considérées comme « susceptibles de porter atteinte à l'ordre public » avec les militants associatifs, syndicaux ou politiques et en général tout citoyen sur lequel le pouvoir souhaite en savoir davantage. L'enregistrement des données à caractère personnel n'avait aucune limite, ni dans le temps, ni dans son contenu puisque pouvaient être répertoriés toutes les informations relatives aux fréquentations, au comportement, aux déplacements, à l'appartenance ethnique, à la vie sexuelle, aux opinions politiques, philosophiques et religieuses, au patrimoine, au véhicule …

Un mouvement citoyen s'est constitué et fédéré au sein du collectif « NON A EDVIGE[13] » ; sa pétition a en l'espace de deux mois recueilli près de 250 000 signatures. Le 2 septembre 2008, un recours au Conseil d'Etat contre le décret promulguant le fichier a été déposé. Devant cette mobilisation, et son fort retentissement dans la presse, le pouvoir a reculé et a retiré son projet initial, l'a remplacé par un projet de décret EDVIRSP, nom imprononçable, vite dénommé EDVIGE 2.0.

A part le retrait des informations concernant la santé et les particularismes sexuels, il y a peu de modifications : les origines « raciales » et ethniques, les opinions politiques, philosophiques et religieuses ou l'appartenance syndicale sont toujours collectées.
Le mélange de deux finalités, l'une administrative[14], l'autre clairement sécuritaire, persiste, comme le fichage des enfants à partir de 13 ans sur de simples présomptions, au mépris de l'article 9 de la Déclaration des droits de l'Homme et du citoyen et de l'article 16 de la Convention internationale des droits de l'enfant.

Fin mars 2009, le nouveau décret EDVIGE 2.0. n'était toujours pas promulgué.

CRISTINA, classifié secret défense, est complètement opaque.

Ces trois exemples montrent les mécanismes qui président à la création et au développement des fichiers.

Le FNAEG, fichier tout à fait légitime, correspondant à une problématique grave et ponctuelle, l'identification de tueurs en série, est, de décrets en arrêtés, sans le vote du parlement dénaturé par les gouvernements successifs. La Cnil, qui depuis 2004 ne donne plus qu'un avis consultatif[15], n'a pas eu les moyens d'enrayer cette dérive.

---

[9] Une partie des RG a été réunie avec la DST dans la DCRI, l'autre devenant une sous-direction de la Direction générale de la police nationale.
[10] EDVIGE : Exploitation Documentaire et Valorisation de l'Information GEnérale
[11] CRISTINA : Centralisation du Renseignement Intérieur pour la Sécurité du Territoires et Intérêts NAtionaux
[12] Voir définition ci-après
[13] Le collectif « NON à EDVIGE » a reçu le prix Voltaire des Big Brother Awards
[14] Destinée au recrutement des personnels devant être accrédités – personnels des aéroports – cela concerne environ 1 000 000 de personnes.
[15] La loi Informatique et Libertés de 1978 avait donné des pouvoirs de blocage à la Cnil, les avis conformes, ce pouvoir lui a été enlevé en 2004.

Le gouvernement a aussi promulgué le fichier EDVIGE par arrêté, à la hussarde. C'est la réaction citoyenne qui a obligé le gouvernement à reculer et à revoir sa copie.

Fichiers administratifs :

Un troisième fichier continue à faire beaucoup parler de lui, le fichier de l'école primaire BASE ELEVES.

Base Elèves[16] a fait l'objet d'une importante mobilisation de parents, enseignants, citoyens, syndicats et associations, qui a conduit à des modifications de son contenu. Base élèves, qui concerne 6,5 millions d'élèves, leurs parents et leurs proches, est introduit en décembre 2004, en catimini, sans débat démocratique ni concertation de la profession. Le ministère n'attend ni les remarques de la CNIL, ni son récépissé. Justifiant du principe de finalité, il décide de regrouper dans une base de données des renseignements nominatifs portant sur 59 champs (comme la nationalité, les compétences, les besoins éducatifs particuliers…) et conservés pour la plupart pendant 15 ans. Les données sont partagées avec les inspections départementales et académiques et en partie avec les mairies. Alors que jusque là les informations nominatives ne sortaient pas du cadre de l'école, un pas important est ainsi franchi sans loi, ni décret, ni arrêté.
Une absence totale de sécurisation de Base Elèves, qui contient pourtant des données sensibles, est mise en évidence dès juin 2007.
La mise en place de Base Elèves s'est également caractérisée par une absence totale d'information des parents de la part du Ministère de l'Education Nationale (MEN). Comment exercer son droit d'accès aux données personnelles quand on ignore l'existence même d'un fichier ?
Cependant la proximité entre enseignants et parents dans les écoles maternelles et élémentaires a favorisé la diffusion de l'information et une importante mobilisation s'en est suivie.

Quelle est la situation de « Base élèves » aujourd'hui ?

En réponse à la mobilisation importante, un arrêté a été publié le 1er novembre 2008, 4 ans après le début de l'« expérimentation ». Certes certaines données ont été supprimées, mais **le traitement automatisé d'informations à caractère personnel garde toutes ses caractéristiques**. Il est obligatoire dès l'inscription à l'école à 2 ou 3 ans *« enseignement public, privé, établissements spécialisés, hôpital »* et dès 6 ans pour la scolarisation par le « *CNED »* ou dans la « *famille ».* Les modifications successives sont mémorisées. Le traitement comporte 25 champs dont le numéro d'identification national élève (INE), les domiciliations et les coordonnées des familles et des proches, les écoles et classes fréquentées, le nom des enseignants (depuis le 3 décembre 2008), les activités périscolaires. Rappelons que classes et écoles, dans notre système éducatif, peuvent renseigner sur une appartenance religieuse ou un handicap. Base élèves reste partagé avec les mairies, soit une administration différente, ce qui constitue une interconnexion déguisée, le fait d'avoir des données communes ne pouvant justifier de partager un fichier sans autorisation.

De plus, la notion de secret professionnel partagé introduite par la Loi relative à la prévention de la délinquance rend les renseignements accessibles, à des degrés divers, à de nombreuses administrations.

Les problèmes liés à la mise en place de fichiers administratifs ne sont pas nouveaux et la LDH a souvent eu l'occasion de s'exprimer sur ce sujet.

Les interconnexions annoncées

Il y a autour de l'utilisation du NIR notamment un enjeu particulièrement important. Certains d'entre nous se souviennent encore de la mobilisation suscitée en 1973 par le projet Safari, lequel prévoyait l'utilisation du NIR pour interconnecter un grand nombre de fichiers. Le gouvernement de l'époque avait du faire machine arrière mais les tentatives pour accroître l'utilisation de ce numéro qui permet l'accès à des données sensibles sont récurrentes.
Si certaines d'entre elles sont battues en brèche (exemple le dossier médical) d'autres aboutissent. Ainsi, depuis l'amendement Brard adopté en 1998 l'administration fiscale est autorisée à utiliser le NIR.

[16] Texte repris de la contribution de la section de Grenoble – voir annexe 2

Avec le RNCPS qui vient d'être institué, l'offensive se poursuit. Par l'intermédiaire du NIR, ce répertoire inter-branches et inter-régimes recense l'ensemble des bénéficiaires des prestations et avantages de toute nature servis par les divers régimes de protection sociale. Selon la direction de la Sécurité sociale, une soixantaine d'organismes sont concernés par l'alimentation du RNCPS et un nombre bien plus important encore de structures y aura accès, notamment les collectivités locales et territoriales pour les procédures d'attribution de toute forme d'aide sociale. Dans un communiqué en date du 2 mars 2009, les administrateurs et conseillers CGT des caisses nationales de Sécurité Sociale viennent de dénoncer très violemment les dangers de ce répertoire.

La dernière période a vu la mise en place d'autres interconnexions.
Parmi elles, citons par exemple l'information due aux maires par la CAF, permettant le recensement des enfants soumis à l'obligation scolaire et qui est de fait juxtaposable avec le fichier de l'Education nationale sur l'absentéisme scolaire.

On peut citer aussi la convention nationale qui vient d'être conclue entre la direction générale des impôts, la direction de la sécurité sociale et les organismes nationaux de protection sociale. Celle-ci a pour objet de mettre en commun les informations disponibles et de faciliter les échanges de données. En ce qui concerne la Caisse nationale des allocations familiales, cette convention s'est traduite par un acte réglementaire afin d'intégrer de nouvelles données dans son système informatique. Le conseil d'administration de la Cnaf a émis un avis défavorable le 3 février 2009.

Quels sont les arguments mis en avant pour justifier ces interconnexions ?

Souvent ces interconnexions sont censées faciliter le travail des salariés des administrations concernées ou faire gagner du temps.
Le plus souvent il s'agit de faire **la chasse aux fraudeurs**, cet exercice étant devenu dans la bouche même de certains de nos ministres « grande cause nationale ». C'est d'une part exagérer un phénomène qui reste marginal et d'autre part désigner **un certain nombre de boucs émissaires**, souvent les plus fragiles parmi les allocataires. Cette chasse aux fraudeurs a parfois des conséquences dramatiques : exemple le bug qui vient de priver des milliers d'allocataires des aides au logement qu'ils percevaient.

Les nouveaux fichiers

Il est sans doute difficile de faire un point exhaustif sur ce sujet. Exemple de 2 domaines :

Celui de la santé : avec la mise en place du fichier RIM-psy du ministère de la santé. Ce fichier nominatif n'est pas anonymisé à la source et risque donc de devenir un outil de contrôle rêvé pour un gouvernement engagé dans un traitement répressif de la santé mentale. L'USP vient d'appeler ses adhérents à ne pas le remplir.

L'Education Nationale avec Base-Elèves (voir ci-dessus) qui vient s'ajouter à Sconet **:** Plus récemment encore, un fichier national consacré au « retard scolaire » vient d'être créé. De manière totalement discriminante, il concerne exclusivement les élèves résidant dans les quartiers de la politique de la ville et dans les quartiers Iris 2000.
L'INSEE devra procéder à la géolocalisation des données individuelles transmises.

Face à ces fichiers, il convient de dénoncer les pressions exercées sur les personnels qui s'opposent à leur mise en place, qu'il s'agisse d'enseignants, de travailleurs sociaux, de personnels médicaux On peut aussi évoquer les personnels de Pôle emploi qui refusent toujours de transmettre à la préfecture la photocopie de toutes les cartes de séjour des étrangers venant s'inscrire. Pour contourner l'opposition des salariés qui refusent de se transformer en auxiliaires de police, le gouvernement entend maintenant imposer la validation d'un dispositif entièrement automatisé.

Tracer :

Les technologies de traçabilité se développent rapidement : RFID[17], géolocalisation, téléphone mobile, vidéosurveillance, lecture automatique plaque d'immatriculation, etc.

Sans réaction de la classe politique ou du contre pouvoir citoyen, les RFID auront, dans les toutes prochaines années, les conséquences les plus contraignantes en terme de droits fondamentaux.

Que sont les RFID ?

Voilà un exemple actuel : Au pré avec sa mère, un poulain de trois jours tangue sur ses pattes. La seringue pénètre sous la peau du cou. Le vétérinaire vérifie son lecteur portable : le numéro d'identification X0723A s'inscrit à l'écran, la puce est opérationnelle. Grâce à l'interface sans fil, le lecteur transmet directement à l'ordinateur les données concernant X0723A : date de naissance, sexe, numéro des géniteurs, vaccinations, allaitement, etc. Il sera désormais simple, en consultant les bases de données, d'assurer un suivi sanitaire rigoureux, de vérifier qui est le propriétaire.

La puce injectée à l'animal est une RFID.

Sans bruit, les RFID envahissent nos vies. Non seulement par implant dans les animaux, mais aussi en placage sur chaque chose, comme un mini-mouchard électronique.

La chose ressemble à une mini-étiquette (d'où son nom d'étiquette « intelligente » ou « smart tag ») et se compose d'une puce et d'une antenne. Chaque étiquette est unique, donc distingue l'objet ou la personne qui la porte parmi tous les autres, et est lisible à distance.
« Sans contact », elle offre la possibilité de suivre, pister, détecter, contrôler, surveiller électroniquement l'être ou l'objet qui la porte.

Ç'est le système du Pass Navigo, le nouveau billet de métro parisien que vous ne sortez plus de votre sac pour valider, ou le télépéage des autoroutes qui débite votre compte, ou encore le forfait de ski, validé lui aussi à distance dans la queue du télésiège. Très commode, à condition d'admettre que chacun de nos déplacements puisse être enregistré - date, heure, trajet, temps de parcours, etc.

C'est l'intérêt principal des RFID pour leurs utilisateurs : recueillir et stocker des millions de données - une richesse dans la société de l'information mais aussi une source de pouvoir dans une société de domination.

Les utilisations sont vastes et variées :
Le portable de Nokia avec lecteur RFID pour inventorier les objets autour de soi et transmettre les données à distance.
Le dispositif « Person Tracking Unit » d'IBM permettant de scanner les étiquettes sur les éléments d'une foule pour suivre les mouvements dans les lieux publics.
Les billets de la Coupe du Monde 2006 avec mouchard pour faciliter le suivi des supporters.
Les bibliothèques : l'enregistrement de l'emprunt des livres se fait au passage du portique de sortie.
Les collèges américains où l'on contrôle la présence et le comportement des élèves par leur carte électronique.

Mais encore : le suivi des bagages dans les aéroports ; l'identification des véhicules, des produits de luxe et des médicaments (contre la contrefaçon) ; l'ouverture contrôlée des portes électroniques ; le remplacement des badges ; les passeports, les visas et les cartes d'identité électroniques ; la traçabilité alimentaire ; l'identification des animaux et des humains, pourquoi pas.

Pour généraliser, d'ici à 2010, chacun des environ 50 000 milliards d'objets de la vie quotidienne vendus quotidiennement seront munis d'une puce RFID.

La Commission nationale informatique et libertés (Cnil) estime que ces technologies de radio-identification permettent potentiellement le « profilage » des individus et font par conséquent peser un risque particulier. Selon la CNIL, la solution consisterait à neutraliser la puce RFID une fois l'objet acheté.

[17] RFID : Radio Frequency Identification – identification par radio fréquence, dites aussi étiquettes « intelligentes », « smart tags », puces à radiofréquence, transpondeurs.

A l'évidence, cette révolution technologique, croisée avec les nanotechnologies[18] dont les scientifiques disent qu'elles seront la prochaine révolution industrielle et qu'elles vont bouleverser tout notre environnement, pose la question du respect de la vie privée.

Car ces avancées ont un revers. D'abord, elles sont surtout un puissant moteur de développement industriel et engendrent des profits importants. Ce pactole ne manque pas d'attirer les grands groupes agroalimentaires, les entreprises militaro-industrielles, les laboratoires médicaux qui sont prompts à faire miroiter les bienfaits en omettant, jusqu'au mensonge, d'évoquer des risques notamment en matière de santé publique, pour l'instant mal cernés.

Dans le domaine du contrôle social, les applications multiples liées à la miniaturisation nanométrique – des RFID de la taille de la poussière, par exemple – couplées à l'informatique, peuvent faire redouter une société de surveillance totale où les moindres faits et gestes d'un individu sont épiés et enregistrés à son insu.

Les étiquettes électroniques posent la question du stockage et de l'usage des informations personnelles. Il est bien prévu une neutralisation de chaque RFID, mais comment procéder si elles sont à la taille nanométrique[19], et donc invisibles ?

A défaut d'un encadrement contraignant et de garanties effectives de limitation de leur emploi et de contrôle sur leur utilisation, les nanotechnologies permettraient, par leur hyper miniaturisation et par leur invisibilité, une surveillance indétectable des citoyens : mini-caméras de vidéosurveillance, microdromes, RFID invisibles, etc.

La situation est d'autant plus préoccupante que cette nouvelle technologie représente, on l'a vu, des enjeux économiques considérables, sur des marchés qui ne sont encore qu'en émergence. On peut donc s'attendre à des pressions industrielles et financières importantes : prendront-elles en considération le respect des libertés individuelles et collectives ?

Cette technologie RFID est aussi en service dans le nouveau passeport biométrique qui est en cours de développement en France.

Il est, d'ailleurs, impossible de parler du traçage des individus sans évoquer la biométrie et l'ADN.

La biométrie est une technique globale visant à établir l'identité d'une personne en mesurant une de ses caractéristiques physiques.

Les techniques :
- Les empreintes digitales : la donnée de base dans le cas des empreintes digitales est le dessin représenté par les crêtes et sillons de l'épiderme. Ce dessin est unique et différent pour chaque individu.
- La géométrie de la main / du doigt : ce type de mesure biométrique est l'un des plus répandus, notamment aux Etats-Unis.
- L'étude de l'iris de l'œil.
- L'étude de la rétine : cette mesure biométrique est plus ancienne que celle utilisant l'iris, mais elle a été moins bien acceptée par le public et les utilisateurs, sans doute à cause de son caractère trop contraignant.
- L'étude du système et de la configuration des veines : cette technique est habituellement combinée à une autre, comme l'étude de la géométrie de la main.
- La dynamique des frappes au clavier d'ordinateur.
- La reconnaissance vocale.
- La dynamique de la signature.

Par ailleurs, il existe d'autres techniques en cours de développement à l'heure actuelle : parmi celles-ci, citons la biométrie basée sur la géométrie de l'oreille, les odeurs, les pores de la peau et les tests ADN.

[18] Nanotechnologies : développement de nanomatériaux ou de nanosystèmes de la taille du milliardième de mètre. - http://www.cnrs.fr/fr/organisme/ethique/comets/docs/ethique_nanos_061013.pdf
[19] Du danger des nanotechnologies – Jean Claude Vitran - Hommes et Libertés N° 144

Tous ces éléments sont susceptibles de nourrir une méga base de données biométriques.

Le Journal Officiel le 4 mai 2008 a validé le principe du passeport biométrique. Les premiers exemplaires seront disponibles à partir de juin 2009 dans 2000 mairies.
Ils intègreront une image du visage ainsi que les empreintes digitales de 8 doigts (à l'exception de celles des enfants de moins de 6 ans) stockées dans une puce RFID.

Profiler :

C'est la conséquence des agissements que nous venons d'énumérer ci-dessus : SURVEILLER, FICHER, TRACER.

Le sens de ce verbe, qui nous vient de l'Anglais, est « le fait d'établir à partir d'indices liés à un acte criminel le profil psychologique de son auteur. »

Aujourd'hui par un glissement paranoïaque, la société considère tout individu comme potentiellement dangereux ; cet axiome amène les gouvernements à tenter d'établir le profil psychologique de tous les citoyens. En corollaire à cette frénésie, le secteur marchand « profile » le consommateur dans le but de lui vendre un maximum de produits, mais aussi de le manipuler aux travers des médias et de la publicité.

La caricature du profilage est le PNR « Passenger Name Record ».

Ce système fait obligation aux compagnies aériennes opérant des vols à destination ou transitant par les Etats-Unis de transmettre aux douanes américaines les données personnelles des passagers et membres d'équipage.

Les données sont au nombre de 34[20] et certaines informations sont personnelles et d'ordre privé :
Modes de paiement - Adresse de facturation - Numéros de téléphone - Adresse électronique - Observations générales - Données SSI/SSR : il s'agit des demandes relatives à des services spécifiques, ce point fait beaucoup débat car il fait référence à des demandes particulières (repas sans sel, ou sans porc, par exemple).

La collecte de ces données et leur moulinage informatique permettent de « profiler » les futurs passagers et de dresser la « No fly list » et la « Selectee list » qui empêchent certains passagers de voyager via ou à destination des Etats-Unis et qui en soumettent d'autres à des contrôles intensifs.

Fait inquiétant, les noms sont approuvés sur la base de critères secrets. Il n'existe par ailleurs aucune référence au « Privacy Act » de 1974, ni aucune mention du droit des individus fichés, notamment pour ce qui concerne le droit d'accès et de rectification.

Par ailleurs, un autre type de profilage pratiqué directement ou indirectement par les services internet type réseaux sociaux ou moteurs de recherche suscite de plus en plus d'inquiétude de la part des citoyens. En permettant d'améliorer les services publicitaires proposés aux annonceurs, les traitements de données à caractère personnel de l'internaute, le profilage et leur exploitation commerciale sont en effet au cœur de l'économie de ces services[21].

[20] La liste est disponible sur : http://www.cnil.fr/index.php?id=1016

[21] Sur ce sujet, voir notamment « Impunité de Google en matière de vie privée sur le territoire français » - Lieu *d'archivage des données personnelles et loi applicable*, Eric A. Caprioli, Communication Commerce électronique n°10, Octobre 2008, comm. 199.

Les services web font partie de la vie quotidienne[22]. A n'en pas douter les possibilités offertes par les nouveaux services de communication en ligne en terme d'accès à l'information, d'accès à la culture, de communication ou encore de liberté d'expression apparaissent comme des acquis incontournables. Pourtant, au revers de la médaille figure une traçabilité accrue des citoyens internautes. E-commerce, e-administration, jeux en ligne, réseaux sociaux, moteurs de recherche, boîte email… toute interaction dans le monde numérique requiert aujourd'hui son lot d'identification, de vérification ou encore d'authentification. Nom d'utilisateur, pseudo, mot de passe, adresse IP, cookie, numéro de carte bancaire sont autant d'identifiants qui viennent composer l' « *identité numérique* » des citoyens internautes.

Parallèlement à l'adoption massive de ces outils de communication, on observe l'émergence d'une vive défiance de la part des internautes vis-à-vis du peu de garanties offertes par les services web à l'égard du traitement de leurs données personnelles et de leur vie privée. Par ailleurs, si par opposition aux traitements de fichiers opérés par la force publique la traçabilité résultant des services web résulte au moins théoriquement de données communiquées de manière volontaire par les individus concernés, il serait faux de penser que ces deux domaines sont imperméables. Il faut en effet garder à l'esprit que toute donnée conservée par un acteur privé est susceptible d'être communiquée, conformément au cadre légal en vigueur[23], aux forces publiques.

- S'agissant des **réseaux sociaux**, au moins deux problématiques peuvent être distinguées. La première, liée à la collecte de données à caractère personnel sans information complète, préalable et explicite de l'internaute rejoint celle des moteurs de recherche. La seconde est tout à fait spécifique et tient à la divulgation volontaire d'informations relatives à sa vie privée (opinions politiques, croyances religieuses, cercle de connaissances) par l'internaute lui-même. Sans dégager les sociétés proposant ces services de toute responsabilité, il convient de rappeler que la maîtrise des informations relève en premier lieu de celui qui souhaite révéler une part de son intimité. A ce titre, il apparaît particulièrement nécessaire d'**attirer l'attention des jeunes publics** sur les risques d'une divulgation inconsidérée d'information à caractère personnel[24]. Opérer ces divulgations de manière consciente et mesurée apparaît comme un premier élément de solution. Les opérateurs de réseaux sociaux n'en sont pas quittes pour autant. Des progrès sont nécessaires quant à la transparence des traitements opérés. Il leur appartient notamment d'assurer une information explicite quant au **périmètre de diffusion** des informations mises en ligne. A cet égard les configurations « *par défaut* »[25] à un cercle de diffusion élargi sont à proscrire[26]. Par ailleurs, les garanties nécessaires à la **maîtrise de l'information** divulguée doivent être respectées[27]. Ainsi, l'internaute doit avoir la possibilité de rectifier ou encore de supprimer de manière effective tout élément personnel le concernant.

- De leur côté, pour chaque requête formulée les **moteurs de recherche** collectent de nombreuses données à même d'alimenter le profil comportemental de l'internaute à la recherche d'une information : mot ou expression recherché, date et heure de la requête, sites web visités, etc… Cette masse de données, consolidée en « *profil* », est associée à un internaute déterminé par l'intermédiaire de son adresse IP et de son

[22] 67 % des Français de plus de 18 ans disposent d'un ordinateur à domicile contre 64 % en 2007. Parmi eux, quasiment tous sont connectés à Internet, puisque 58 % (contre 53 % en 2007) des personnes interrogées déclarent disposer d'une connexion. CREDOC, La diffusion des technologies de l'information et de la communication dans la société française (2008) - **http://www.arcep.fr/uploads/tx_gspublication/etude-credoc-2008-101208.pdf**

[23] Voir notamment le dispositif de réquisition judiciaire organisé par les articles 60-1 et 99-3 du Code de procédure pénale et par l'article L 34-1 du Code des postes et des communications électroniques.

[24] Voir en ce sens **Internet et vie privée** LeMonde, 03.11.07

[25] Voir Une plainte déposée contre Facebook pour atteinte à la vie privée LeMonde, 03.06.08

[26] Protéger la vie privée dans un monde sans frontières - http://www.cnil.fr/index.php?id=2534

[27] Internautes : le droit à l'oubli aux abonnés absents - http://www.lesechos.fr/info/innovation/4794388.htm

numéro d'identification unique attaché au témoin de connexion (cookie) stocké sur son ordinateur. Au moins trois difficultés en rapport avec ces pratiques doivent être relevées :

i. le plus souvent, la **collecte de ces données est réalisée de manière indue** sans information explicite de l'internaute[28] qui ne soupçonne pas les implications sous-jacentes ;

ii. par exemple, ces **informations peuvent être recoupées et combinées** avec les données collectées par le bais d'autres services[29] pour constituer un profil de chaque internaute susceptible d'être commercialisé directement ou indirectement, le plus souvent dans le cadre d'activités publicitaires ;

iii. le **traitement sécurisé de ces données** n'est pas toujours assuré : en août 2006, une société américaine a divulgué accidentellement un fichier contenant les logs de 658 000 utilisateurs[30].

Face à ces menaces, au moins trois paradoxes doivent être relevés. Le premier tient au rapport qu'entretiennent les citoyens internautes avec ces technologies tandis que les deux autres relèvent davantage de l'approche déconcertante des pouvoirs publics.

Signe encourageant, le premier paradoxe permet de constater que pour une grande partie de la population, l'usage fréquent et même quotidien des outils offerts par Internet ne fait qu'entretenir leur réserve quand à la confiance qu'ils portent dans ces technologies, tout particulièrement quant au respect de leur vie privée[31]. Comme en témoigne l'étude du Centre de recherche pour l'étude et l'observation des conditions de vie (CRéDOC) en décembre 2007, le principal frein à la diffusion d'internet auprès du grand public est, pour 23 % des Français, l'insuffisance de la protection des données personnelles.

Le second paradoxe révèle la nécessité de rappeler que les données personnelles ne sont pas des données comme les autres et d'initier une réflexion autour de l'avènement d'un concept d' « identité numérique » qui pourrait réclamer le renforcement ou l'adaptation des garanties légales et des gardes fous techniques. Dans tous les cas, comme l'a souligné au niveau européen le Groupe de l'article 29[32], à « cet élargissement [des usages] ne peut correspondre un resserrement de la définition des données à caractère personnel »[33].

---

[28] Notamment à ce sujet, voir plainte déposée par l'Electronic Privay Information Center (EPIC) contre la société DoubleClick disponible ici http://epic.org/privacy/internet/ftc/DCLK_complaint.pdf

[29] Voir notamment Charte de confidentialité, Dernière modification : 27 janvier 2009 - http://www.google.fr/privacypolicy.html

[30] Peut-on tout confier à Google ? LeMonde 14.11.08

[31] La CNIL diffusait récemment les résultats d'une étude qui souligne que 71% des Français jugent la protection de la vie privée sur Internet insuffisante. Pour l'autorité en charge de la protection des données, « *les jeunes de 18-24 ans, « gros consommateurs d'Internet », se révèlent un peu plus soucieux que les autres. En effet, 78 % jugent la vie privée insuffisamment protégée sur Internet. Pour autant, cette défiance ne semble pas les détourner d'Internet* ». - 71% des Français jugent la protection de la vie privée sur Internet insuffisante, CNIL – Communiqué 13/10/2008 – http://www.cnil.fr/index.php?id=2532&news%5Buid%5D=587&cHash=3199e1a65b

[32] Avis 02/08 sur révision de la directive 2002/58/CE

[33] A contre courant de cette logique, au moins deux exemples permettent d'affirmer qu'une tendance visant à la réduction du périmètre des éléments d'identification protégés se développe. Le dangereux débat autour de l'adresse IP et la remise en cause de sa nature de données à caractère personnel est une première illustration. Par ailleurs, a contrario du principe d'effacement des données, le projet de décret d'application de l'article 6-II de la LCEN qui viendra fixer les conditions dans lesquelles hébergeurs et fournisseurs d'accès conservent les « *données de nature à permettre l'identification* » des internautes exigerait quant à lui la conservation de davantage de données que nécessaires au seul fonctionnement des services : nom, prénom, numéro de téléphone, heure de connexion, etc…

Le troisième paradoxe met en exergue l'absence de recours et de garanties effectives à même de faire respecter la vie privée des internautes. D'un côté, la CNIL garante de la bonne application de la loi "Informatique et Libertés"[34] se voit en pratique dépouillée de ses moyens d'action[35]. De l'autre, l'individu désireux de défendre ses droits en justice se voit refuser l'application des lois françaises ou européenne et des garanties qu'elles devraient lui apporter[36].

A travers ces trois paradoxes se profile un risque lourd de conséquence pour l'individu : la dépossession de son *identité numérique*.

<u>Quelques conclusions</u> :

Sur le versant juridique : ce glissement vers une société de surveillance généralisée des citoyens serait impossible si l'ensemble des textes fondamentaux[37] était scrupuleusement respecté.

C'est d'abord la finalité :
Dans quel but un système, un fichier est-il constitué ? Quelle est sa destination ?

C'est ensuite le principe de proportionnalité :
Les données collectées doivent être strictement nécessaires au but recherché.
L'article 8 de la Déclaration des droits de l'Homme et du Citoyen de 1789 est clair à ce sujet :
« La loi ne doit établir que des peines strictement et évidemment nécessaires » Cela veut dire que ce principe de proportionnalité doit être *« fondée sur un besoin impérieux et notamment proportionnée au but légitime recherché ».*

Ensuite, la liberté de conscience :
Ce point est clairement défini par les articles 10 et 11 de la Déclaration de 1789.
C'est qu'il y a des domaines qui sont exclusivement de la sphère privée : les orientations sexuelles, la santé, les opinions religieuses qui n'intéressent pas autrui et n'ont pas à figurer dans une base de donnée quelconque.

L'article 12 « protection de la vie privée » de la Déclaration Universelle des Droits de l'Homme[38] du 10 décembre 1948 précise :
Nul ne sera l'objet d'immixtions arbitraires dans sa vie privée, sa famille, son domicile ou sa correspondance, ni d'atteintes à son honneur et sa réputation. Toute personne a droit à la protection de la loi contre de telles immixtions ou de telles atteintes.

Tous les textes postérieurs, ceux de la Convention européenne des droits de l'Homme de 1950, de la Constitution française de 1958 et de la Charte des droits fondamentaux de l'Union Européenne de 1999 reprennent ces proclamations sur la protection de la vie privée.

Pourtant tous ces droits sont en permanence bafoués et toutes les associations de défense des libertés publiques et privées sont contraintes d'intervenir dans les débats pour dénoncer les dérives liberticides, voire demander l'annulation des textes par le Conseil d'Etat, c'est le cas actuellement pour les fichiers ELOI et EDVIRPS et pour la mise en place du passeport biométrique.

---

[34] Voir site de la CNIL, « Mission » http://www.cnil.fr/index.php?id=67

[35] Pour éviter toute équivoque, quelques chiffres doivent être cités : (i) lorsque ses homologues allemande et anglaise disposent respectivement de 400 et 270 personnes, la CNIL comptera 100 employés à la fin de l'année 2008 ; (ii) en 2006, la Commission a effectué 127 contrôles, contre près de 700 pour son homologue espagnol. (iii) le budget de communication de la Commission ne dépasse pas les 150 000 euros, quand son homologue anglaise lui consacre l'équivalent de 3 millions d'euros.

[36] Notamment, **l'exercice du droit à l'oubli se heurte à de nombreux obstacles**. Récemment une décision de justice écartait l'application de la loi « *Informatique et Libertés* » pour décider que le droit à l'oubli ne contraint pas un moteur de recherche qui stocke ses archives aux Etats-Unis. Voir à ce sujet « Impunité de Google en matière de vie privée sur le territoire français » - Lieu *d'archivage des données personnelles et loi applicable*, Eric A. Caprioli, Communication Commerce électronique n°10, Octobre 2008, comm. 199.

[37] Les textes fondamentaux sont disponibles sur www.ldh-france.org

[38] DUDH : http://www.assemblee-nationale.fr/histoire/dudh/declara.asp

Sur le versant technique : aucune technologie de surveillance n'est fiable à 100 %.

La fiabilité de la vidéo-surveillance est dépendante de la compétence des opérateurs, les fichiers sont remplis d'informations erronées – le STIC comporterait 60 % d'erreurs[39] – les puces RFID sont facilement piratables[40], les caractéristiques biométriques sont loin d'être parfaites et précises, et l'on atteint très vite des limites pour ces diverses techniques et la biométrie n'est nullement une « solution miracle et universelle » !

L'idée de recueillir des traces à l'insu de la personne, sans même qu'elle en ait conscience, est un risque tout à fait nouveau. Un individu peut se trouver à un endroit, où il ne fallait pas. Et sur cette base on peut le soupçonner. Le problème, c'est la confiance totale que l'on va accorder à tous ces procédés de surveillance et de reconnaissance. A ce moment là, on n'aura plus à prouver la culpabilité de l'individu mais c'est lui qui aura à prouver son innocence. Même si on n'a rien à se reprocher, on peut vouloir cacher des choses sur soi, c'est tout à fait légitime.

Ce qui est le plus angoissant c'est la banalisation de ces technologies. C'est ludique de mettre son index sur un scanner pour la reconnaissance des empreintes. On habitue d'ailleurs les jeunes enfants à ce type de démarches, qui deviennent des réflexes – cantines scolaires, bibliothèques – et lorsqu'on tend sa carte d'identité à un contrôle de police on sait qu'on est contrôlé. Et après, on n'aura aucun mal à accepter de le faire au supermarché, à la banque, à l'entrée d'une cantine scolaire...

Nous venons de brosser ci-dessus un tableau incomplet des différents moyens de surveillance et de contraintes des individus.
La synthèse de cette communication fait l'objet d'une résolution que nous vous proposons à la discussion.

Annexe N° 1

Politique sécuritaire et contrôle social, deux faces d'un même danger

par Jean Danet, membre du Comité central de la LDH

Un aperçu des politiques pénales sur le long cours montre que très souvent leur évolution coïncide avec celle des politiques publiques de contrôle social. Preuve en est encore aujourd'hui, où le durcissement en matière pénale et l'apparition de nouveaux modes de surveillance, fondés sur les nouvelles technologies, vont de pair.

La notion de contrôle social peut être comprise en deux sens, et elle a en tout cas deux emplois selon A. Ogien (1). Le premier est individualiste et neutre. Il renvoie « *à l'existence inhérente à toute société de mécanismes de régulation qui conduisent chacun de ses membres à intérioriser les prescriptions d'un système de normes et de valeurs unique et stable* ». Le second est collectif et critique : il nomme alors « *l'ensemble des dispositifs de surveillance et de répression mis en œuvre par des instances spécialisées (police, justice, armée, école, etc.) afin d'asseoir le pouvoir d'un groupe dominant, en reconduisant les conditions de l'asservissement des dominés* ».
Encore faut-il distinguer ici entre ce qui relève de la délinquance, de la norme pénale, de la distinction entre le « permis-prescrit » et l'interdit pénal, et ce qui relève de la déviance, d'une norme sociale qui veut organiser le normal et le pathologique, le conforme et le non-conforme.
Dès 1981, souligne A. Ogien, Robert Castel avait mis en exergue l'importance de l'institution dans l'analyse du contrôle social. Chaque modalité de contrôle s'exerce dans le cadre d'un organisme dont le mandat et les missions sont définies par une instance politique qui assigne une place à chaque pratique de correction ou de réparation. Un rapport de domination, analysé sous la notion de tutelle, se noue entre les individus qu'il faut éduquer ou réhabiliter, et les professionnels.

1975-1995, les années bascules ?

Du côté de la politique criminelle et des prisons, la période qui s'ouvre en 1975 (et ce jusqu'en 1995) semble complexe au plan des politiques publiques. Elle témoigne en tout cas d'un double mouvement.

[39] Le STIC : Système de Traitement des Infractions constatées - http://www.cnil.fr/index.php?id=2538&tx_ttnews[tt_news]=423&tx_ttnews[backPid]=1&cHash=ffd675465
[40] Voir le site BUG BROTHER : http://bugbrother.blog.lemonde.fr/

Les actions de prisonniers – le GIP (2) –, associées en même temps aux premières rafales d'un vent sécuritaire qui souffle d'outre-atlantique produisent une oscillation législative autour de la prison et de la pénalité. S'intercalent des textes qui manifestent le souci d'humaniser la prison tandis que d'autres relèvent d'une volonté de renforcer l'effectivité de la sanction. Le second mouvement témoigne d'une recherche de diversification des peines et se présente comme une volonté de développer les alternatives à la prison (peines de substitution, créations des travaux d'intérêt général). Mais en réalité, la population carcérale commence une remontée qui ne s'arrêtera plus vraiment jusqu'à aujourd'hui (elle augmentera de 26 000 à 66 000 personnes de 1975 à 2008).
Le nouveau Code Pénal, voté en 1992, entré en vigueur en 1994, marque aussi le début d'une profonde évolution avec l'irruption de la notion de risque, au cœur de nouvelles incriminations telles le délit de « risque causé à autrui ». De plus en plus d'infractions « formelles » surgissent, c'est-à-dire en amont de tout dommage, destinées à dissuader si possible de la prise de risque, mais qui peuvent conduire en prison (par exemple la conduite en état d'ivresse).
Ainsi, ce n'est plus la notion de « sujet dangereux » qui est désormais centrale mais celle des « facteurs de risque ». Cette mutation a aussi touché la pénalisation, qui n'est plus liée à un état de tel type de personnes mais à des comportements jugés menaçants. En 1995, la loi Pasqua va encore aller plus loin en posant le droit à la sécurité comme un droit fondamental. Le droit à la sécurité, bientôt « la tolérance zéro », le « risque zéro », deviennent les boussoles de toute politique criminelle. Le léger fléchissement des incarcérations autour des années 2000 ne retournera pas longtemps la tendance.
Depuis quelques années, et malgré la diversification des peines, la population carcérale augmente de nouveau. Le nombre des personnes incarcérées chaque année augmente depuis 2001 et, sur 85 500 personnes incarcérées en 2005, 72 000 l'étaient pour une peine de moins d'un an. Pour 300 000 condamnations à une peine de prison ferme ou assorties du sursis, on compte seulement 12 830 peines de travail d'intérêt général. La prison est plus que jamais la peine centrale de notre dispositif pénal. Et on doit s'attendre à ce que les peines minimales allongent de nouveau la durée moyenne des peines tandis que le nombre d'entrées en prison continue d'augmenter.

Un nouveau contrôle social des « populations problématiques »

Dans le même temps, exactement à l'envers de ce qui s'est passé entre 1945 et 1975, un nouveau mode de contrôle social s'affirme, fondé pour une grande part sur de nouvelles technologies. L'inflation carcérale et le développement de nouveaux modes de contrôle social vont donc de pair.
En premier lieu, des politiques publiques spécifiques appréhendent toujours plus de « populations problématiques » (3), avec un point commun : elles concernent des populations qui sont sans exception pensées aujourd'hui comme à la fois vulnérables et menaçantes (4). Regardons d'un peu plus près les points communs des politiques publiques dont elles relèvent. Les « populations problématiques », ce sont les populations envisagées comme sujets collectifs, non plus comme des collections d'individus, mais comme un ensemble, défini et caractérisé. En tel cas, elles reprennent une « population cible » ancienne (5), qui depuis longtemps a fait, continûment ou non, l'objet des attentions de l'Etat. En tel autre cas, elles agrègent autour d'une notion jusque là inusitée à de tels fins (le décrochage scolaire) un ensemble d'individus qui acquiert ainsi une visibilité pour des dispositifs à venir (6).
Mais si ce n'était que cela, la fabrique en question serait bien peu de choses et l'économie du pouvoir encore très rustique. Car ce dont il est question ici, c'est de l'objectif que les politiques publiques se donnent quant au devenir de chacune de ces populations en tant que sujet collectif. C'est ici que le contrôle social s'exerce. Et ici, on peut constater une vraie diversité de la fabrique. On peut relever des types d' « usinage » bien distincts. Il peut s'agir d'isoler cette population, de la constituer en catégorie là où elle ne l'était pas. Il peut s'agir de la mesurer, de la ficher, de « l'intégrer » ou de l'exclure, de la dissocier, la fragmenter, de la distinguer d'une autre catégorie, d'en assurer la visibilité ou au contraire de la rendre socialement invisible, de lui assigner des espaces, ou, au contraire, de l'exclure des espaces qu'elle a conquis, de lui dessiner des parcours sociaux vers plus de droits ou d'allonger ces parcours, etc.
Les fondements avancés pour justifier ces politiques sont eux aussi assez divers : moraux, médicaux, économiques, politiques ou géopolitiques.
Ces politiques vont travailler ces populations en séquences successives ou continues, au plan local ou au plan général. Ces politiques communiquent parfois, alors qu'elles visent initialement des populations distinctes, organisant ainsi des fongibilités (on était ceci, on devient cela) ou au contraire des alternatives (on est l'un ou l'autre).
Des technologies qu'ils utilisent, on retiendra bien sûr les fichiers ou la biométrie en certains cas, c'est-à-dire les technologies propres à une société de contrôle, mais on relève que les vieilles techniques dont Foucault retraça naguère la genèse, à savoir l'examen (examen du dossier), l'interrogatoire (pour sonder la sincérité, détecter la fraude), ou l'enquête sont ici toujours à l'œuvre. Du point de vue des outils juridiques convoqués à l'appui de ces dispositifs, il a pu être relevé un faible support normatif, des lois imprécises souvent très proclamatrices, des décrets par conséquent insuffisamment précis qui laissent trop de place à l'arbitraire des circulaires de l'administration et donc aussi des guichets, des agents.

Les technologies au service de nouveaux contrôles sociaux

Ces nouveaux modes de contrôle social se sont « branchés » depuis dix ou quinze ans environ sur les nouvelles technologies. Il en résulte un contrôle social qui peut être beaucoup plus général encore que celui qui vise des « populations problématiques », et qui passe par le recueil de toutes sortes de données et informations à caractère personnel. La logique repose sur l'idée que des risques de toute nature existent, qu'il faut déceler, mesurer. La prévention situationnelle installe des dispositifs de contrôle social dans les espaces publics classiques (la rue, les gares, les stades, etc.), à l'instar de la « vidéo-surveillance », appelée aussi « vidéo-protection ».
Dans le même temps, des infractions incriminent toutes sortes de « comportements menaçants » qui dépassent de beaucoup les frontières classiques des « populations à risque » et concernent tout un chacun. Se dessine un nouvel ordre public des espaces publics, de la collaboration à la sécurité, contraignant chacun à participer un peu plus à cette nouvelle croisade, et un nouvel ordre corporel qui se substitue à l'antique notion de « bonnes mœurs ».
Si ce surarmement pénal demeure impossible à mobiliser dans son intégralité, c'est le contrôle social qui va, lui, permettre d'évaluer les risques et de cibler une politique pénale sur un phénomène jugé ou présenté comme ayant atteint un niveau insupportable. Répression pénale donc quand un phénomène est jugé avoir atteint un niveau insupportable et puis, derrière, une politique publique prendra le relai en poursuivant des objectifs de contrôle social.
Ces nouvelles politiques sont aussi marquées par de multiples hybridations et notamment celles du public et du privé, y compris dans les prisons. Les articulations multiples entre les politiques criminelles et les politiques publiques de contrôle social sont source permanente de brouillage. Entre les objectifs d'éducation, de surveillance, de punition, tout un *continuum* nouveau de mesures et de peines émerge.
Mais le contrôle social peut encore aller beaucoup plus loin. Car l'espace informationnel – dans lequel chacun s'inscrit pour chaque acte de la vie quotidienne –, permet le recueil d'une multitude de données à caractère personnel, disponibles pour de multiples traitements, à des fins de sécurité, mais aussi de « prévention », « d'orientation », de « sélection ». La notion de vie privée disparaît, et ce n'est plus la sureté de la personne physique qui est ici menacée, mais celle de la personnalité et de l'intimité de chacun.

Discrétion et invisibilité de la surveillance

Comment expliquer que toutes ces techniques inhérentes au nouveau contrôle social soient si facilement acceptées ? D'abord, on doit remarquer que les dispositifs techniques sont le plus souvent peu perçus ou peu contraignants. Une simple « lecture » suffit, d'une carte, d'un badge, d'un mot de passe, d'une puce RFID demain. En apparence, la liberté d'aller et venir est sauve, l'anonymat aussi, le contrôle se fait invisible, la surveillance discrète. « Pourquoi m'y opposer puisque cela ne me gêne pas et que je n'ai rien à me reprocher ? » entend-on le plus souvent.
L'argument de la nécessité (il faut lutter contre l'insécurité, le terrorisme etc.) et de la fiabilité font encore recette car la société n'a que peu de recul sur ces dispositifs, leur efficacité et les risques de dérapages. Qui sait que le Système de traitement des infractions constatées (STIC) est bourré d'erreurs, que les passeports biométriques ou des cartes à multiples usages de demain pourraient bien être lus à distance et le contenu de leurs puces « volés » ?
Au fond, le bénéfice de la nouveauté est double : on prête à ces nouvelles technologies du contrôle social l'efficacité, et ils ne présentent pas les inconvénients des modes de contrôles sociaux précédents. L'agacement devant le portique de sécurité est en passe de disparaître. Dépersonnalisés côté contrôleur, les contrôles paraissent moins intrusifs. Ils apparaissent même comme une suite de sésames alors qu'ils instaurent des zones d'accès restreint. Recueillant les données personnelles du contrôlé, ils ne pèsent plus comme les disciplines sur les corps, mais sur les données et informations à caractère personnel.
Gérés par l'Etat, mais pensés à un niveau de plus en plus international, les nouveaux dispositifs techniques de contrôle social, articulés sur des politiques sécuritaires de plus en plus répressives, nous appréhendent, ensemble ou séparément, comme des fauteurs de risque potentiels. Pénalisation et contrôle social sont les deux faces d'un même danger pour les libertés.

(1) A. Ogien, « Contrôle social » in *Le Dictionnaire des sciences humaines*, PUF, 2006.
(2) Groupement d'information sur les prisons.
(3) Sont ici repris en synthèse les éléments d'un rapport final du colloque « La fabrique des 'populations problématiques par les politiques publiques' », Nantes, 13-15 juin 2007, consultable sur le site de Maison des sciences de l'Homme.
(4) Menace de toute nature y compris pour les finances publiques, menace de fraude, de parasitage du « système ».
(5) Prostituées, mendiants, gens du voyage, sortants de prison.
(6) RMIstes, jeunes en échec scolaire, toxicomanes, sans-abri, etc.

Annexe N° 2

Société de surveillance, vie privée et libertés - Les fichiers scolaires

proposée par la section de Grenoble

Depuis quelques années, nos autorités administratives développent de façon inquiétante un usage de plus en plus invasif et intrusif d'outils technologiques par la collecte, le traitement, le stockage et les échanges d'informations sur les biens, les personnes et sur leurs faits et gestes. Les lois et règlements se modifient pour ouvrir la voie à ces pratiques et au commerce qui les entoure.

L'Education Nationale n'échappe pas à ce développement effréné.

Ainsi, dans le secondaire, **la biométrie** est de plus en plus fréquemment utilisée pour l'accès à des cantines scolaires par le contrôle de l'empreinte palmaire des élèves, banalisant ainsi auprès des jeunes l'utilisation de techniques d'identification particulièrement intrusives.
Les caméras de vidéo-surveillance se multiplient dans les collèges et lycées, se substituant à des postes de surveillants ou de conseillers d'éducation. Cette réponse au sentiment d'insécurité entretenu par la diminution de la présence humaine malmène dangereusement les valeurs que l'école a pour mission de transmettre et notamment les libertés individuelles et collectives.

Les fichiers de l'Education Nationale sont une bonne illustration de la problématique du fichage. Ils nous interpellent tout particulièrement car sont concernés des enfants et des jeunes, personnes en devenir. Leur parcours se retrouve figé dans des bases de données, or un jeune, plus encore qu'un adulte, doit pouvoir bénéficier d'un droit à l'oubli.
A travers les élèves, nous assistons à la mise en place d'un fichage en « temps réel » de la jeunesse qui ne peut que conduire à terme à un fichage généralisé de la population.

Parmi les fichiers de l'Education Nationale, **« Base Elèves 1er dégré »** (BE) est le plus connu pour avoir fait l'objet d'une importante mobilisation de parents, enseignants, citoyens, syndicats et associations, qui a conduit à des modifications de son contenu. L'historique de sa mise en place met en évidence la légèreté avec laquelle les fichiers sont souvent créés, au mépris de la Loi Informatique et Libertés et de la CNIL mise devant le fait accompli.
Base Elèves, qui concerne 6,5 millions d'élèves, leurs parents et leurs proches, est introduit en décembre 2004, en catimini, sans débat démocratique ni concertation de la profession. Le ministère n'attend ni les remarques de la CNIL, ni son récépissé. Justifiant du principe de finalité, il décide de regrouper dans une base de données des renseignements nominatifs portant sur 59 champs (comme la nationalité, les compétences, les besoins éducatifs particuliers…) et conservés pour la plupart pendant 15 ans. Les données sont partagées avec les inspections départementales et académiques et en partie avec les mairies. Alors que jusque là les informations nominatives ne sortaient pas du cadre de l'école, un pas important est ainsi franchi sans loi, ni décret, ni arrêté.
Une absence totale de sécurisation de BE, qui contient pourtant des données sensibles, est mise en évidence dès juin 2007.
La mise en place de BE s'est également caractérisée par une absence totale d'information des parents de la part du Ministère de l'Education Nationale (MEN). Comment exercer son droit d'accès aux données personnelles quand on ignore l'existence même d'un fichier ?
Cependant la proximité entre enseignants et parents dans les écoles maternelles et élémentaires a favorisé la diffusion de l'information et une importante mobilisation s'en est suivie.

<u>Quelle est la situation de « Base élèves 1er degré » aujourd'hui ?</u>

En réponse à la mobilisation importante, un arrêté a été publié le 1er novembre 2008, 4 ans après le début de l'« expérimentation ». Certes certaines données ont été supprimées, mais **le traitement automatisé d'informations à caractère personnel garde toutes ses caractéristiques**. Il est obligatoire dès l'inscription à l'école à 2 ou 3 ans *« enseignement public, privé, établissements spécialisés, hôpital »* et dès 6 ans pour la scolarisation par le « *CNED »* ou dans la « *famille »*. Les modifications successives sont mémorisées. Le traitement comporte 25 champs dont le numéro d'identification national élève (INE), les domiciliations et les coordonnées des familles et des proches, les écoles et classes fréquentées, le nom des enseignants (depuis le 3 décembre 2008), les activités périscolaires. Rappelons que classes et écoles, dans notre système éducatif, peuvent renseigner sur une appartenance religieuse ou un handicap. Base élèves reste partagé avec les mairies, soit une administration différente, ce qui constitue une interconnexion déguisée, le fait d'avoir des données communes ne pouvant justifier de partager un fichier sans autorisation.

De plus, **la notion de secret professionnel partagé introduite par la Loi relative à la prévention de la délinquance rend les renseignements accessibles, à des degrés divers, à de nombreuses administrations.**

L'arrêté entérine, de fait, la diffusion de données nominatives hors des établissements scolaires (mairie, inspection départementale, inspection académique) mettant en péril l'indispensable relation de confiance entre enseignants et familles.

« Base élèves » se met en place, département après département, par la contrainte : des menaces et des sanctions, pouvant aller jusqu'au retrait d'emploi de direction, sont utilisées pour exiger des enseignants qu'ils entrent des données personnelles qui ne leur appartiennent pas, rompant ainsi le pacte implicite de confiance qui les liait aux parents.

Il est intéressant de noter que les modifications apportées à Base élèves ne concernent pas **le fichier Sconet - équivalent de BE dans les collèges et lycées -** qui rassemble encore aujourd'hui la plupart des données que contenait BE à sa création, comme par exemple la nationalité. La moindre proximité entre le personnel administratif et les familles a permis d'entretenir une opacité totale. Sur le site de l'Académie de Créteil, on peut mesurer l'ampleur du fichage permis par un tel dispositif : *« Le projet SCONET s'inscrit dans le cadre général de l'élargissement des possibilités d'accès et d'échanges des informations utiles aux acteurs locaux, de l'ouverture des systèmes d'information vers les collectivités territoriales et du déploiement des environnements numériques de travail (ENT).*
Il couvre les fonctionnalités relatives à la base élèves de l'établissement, à la gestion financière de l'élève, aux bourses des collèges, à la gestion des absences des élèves, à l'intégration des nomenclatures, aux paramètres généraux de l'établissement, aux échanges de données avec les bases académiques et aux interfaces avec les autres logiciels de gestion (emploi du temps, notes, …)»

Toujours en l'absence de débat et d'information, l'évolution des bases de données BE ou Sconet est d'ores et déjà annoncée dans le : *"Schéma stratégique des systèmes d'information et des télécommunications 2008" du MEN – « Enrichir les bases élèves d'informations relatives aux parcours des élèves et à leurs acquis certifiés, pour répondre aux besoins de suivi individualisé et de pilotage pédagogique. »*
*« **Le dossier de l'élève se verra progressivement enrichi de données nouvelles ou de données actuellement dispersées dans différents systèmes d'information**. Besoins éducatifs particuliers (loi du 11 février 2005 et décret d'application du 30 décembre 2005 sur le parcours de formation des élèves présentant un handicap), nouvelles modalités d'accompagnement éducatif (loi de cohésion sociale, dite loi Borloo), vœux et décisions d'orientation, participation à la vie scolaire, insertion professionnelle sont des informations indispensables pour le pilotage pédagogique au même titre que les acquis certifiés : résultats aux examens, diplômes et mentions obtenus, attestations telles que B2i… » ainsi que « les compétences validées en langues étrangères* » l'objectif étant d'enregistrer le suivi des acquis et des compétences « du socle commun ».
Un dispositif de traçage des citoyens est ainsi mis en place, avec conservation des mises à jour successives, sur des données sensibles, sans évaluation des conséquences, sans débat.

Parallèlement au développement de BE, sans débat ni public ni parlementaire, sans aucune autorisation ni déclaration à la CNIL, sans information des familles ni des enseignants, **le ministère a mis en place dès décembre 2004 un système centralisé d'attribution d'un numéro identifiant national élève (INE) à chaque enfant pour 35 ans (déclaration à la CNIL le 15 février 2006 pour 13,5 millions d'élèves, récépissé de la CNIL le 27 février 2007).**
Cet INE doit permettre, pour chaque enfant, le recoupement de données conservées dans différents systèmes informatiques, traçant ainsi son parcours de formation dans sa totalité.
A supposer que la création d'un tel identifiant soit justifiée, il est alors essentiel que l'accès à la BNIE, base de données nationale qui renferme des informations nominatives actualisées ainsi que les correspondances identité-INE, soit strictement limité et contrôlé. Or les documents de déclaration de la BNIE à la CNIL font état de 400 gestionnaires/utilisateurs habilités à la consulter.
Ici aussi apparaît, de manière flagrante, la légèreté avec laquelle ces dispositifs sont mis en place.

La généralisation de l'INE soulève différents problèmes, parmi lesquels celui de l'accueil d'enfants de familles sans papiers. Le 17 septembre 2007, l'Inspection académique du Haut-Rhin adresse un courriel à toutes les écoles du département : *« Avez-vous connaissance de la scolarisation d'élèves "sans papier" dans votre établissement ? Dans l'affirmative, veuillez nous le faire savoir dans la journée par e-mel ou par téléphone au… ou … ».* Avec l'INE, il sera désormais aisé de repérer les enfants de plus de 6 ans non encore immatriculés, et d'en transférer automatiquement la liste à la Préfecture, grâce aux bases élèves. Après vérification de la régularité de leur présence sur le territoire à partir de ses propres bases de données, la Préfecture peut aisément localiser le domicile, grâce au précieux fichier de l'Inspection d'Académie qui comporte les coordonnées actualisées des familles (et de leurs proches) et transmettre l'information à la police qui n'a plus qu'à procéder à l'interpellation.
Ainsi, la veille citoyenne devient impossible et l'école n'est plus un lieu d'accueil et de protection de tous les enfants.

Un meilleur contrôle des effectifs des établissements scolaires, la possibilité de réaliser des études statistiques plus complètes, une simplification des procédures administratives sont autant d'arguments avancés par le Ministère pour justifier la mise en place des bases élèves, du dossier de l'élève ou la création de l'INE.

En ce qui concerne **les effectifs**, on ne peut que noter une disproportion entre le but et les moyens mis en œuvre, à savoir un fichage généralisé de tous les enfants.
(Cet argument n'a d'ailleurs aucune réalité sur le terrain : les effectifs sur les Base élèves ne peuvent prendre en compte les mouvements de population pendant les grandes vacances scolaires ; les projections d'effectifs par le directeur restent donc plus fiables).

La tendance actuelle est d'attendre beaucoup d'**études statistiques** anonymisées mais s'appuyant sur des listes nominatives exhaustives par opposition aux échantillons traditionnellement utilisés et de remplacer les enquêtes par questionnaires par des exploitations de bases de données. Au besoin, celles-ci sont enrichies de variables qui n'ont pas d'utilité pour la gestion mais qui serviront à l'exploitation statistique. Si le prix à payer est le fichage du parcours de chaque jeune, le jeu en vaut-il la chandelle ? De plus, et c'est une grande inquiétude que nous avons, ce type d'études conduit, de fait, à la création de fichiers discriminatoires, comme celui du 18 février 2009 *« Arrêté du 28 janvier 2009 portant sur la mise en œuvre d'un traitement automatisé d'informations nominatives visant à produire et diffuser des indicateurs statistiques locaux sur le retard scolaire des élèves résidant dans les quartiers de la politique de la ville et dans les quartiers Iris 2000 ».*

Les aspects pratiques de l'automatisation des traitements de données sont souvent mis en avant. C'est le cas pour le dossier de l'élève, ou également pour **le système d'admission post bac** (APB) généralisé en 2009. Ce dispositif sur Internet centralise les demandes d'admission des élèves de terminale dans différents établissements (universités, IUT, grandes écoles…). Les élèves, outre leur INE et leurs données d'état civil, doivent entrer eux-mêmes leurs notes. Ce système introduit vraisemblablement une simplification dans les démarches, mais il **contribue également à banaliser auprès des jeunes la diffusion de données personnelles sans maîtrise de leur utilisation ultérieure. Alors que l'on doit attendre du système éducatif qu'il sensibilise les élèves aux risques liés à Internet et au fichage.**