Interconnexion et identités électroniques : le pouvoir d'enquête à l'heure des systèmes de fichiers répartis

Amar Lakel

Interconnexion et identités électroniques : le pouvoir d'enquête à l'heure des systèmes de fichiers répartis

Amar LAKEL, Janvier 2007

> « On entend souvent dire qu'il est temps de désenclaver les différents services de l'administration par la diffusion et l'échange des informations. (...) S'il est vrai qu'il faut abattre des barrières, il en est aussi d'utiles et de nécessaires. Le jour où, au sein de l'État, chaque fonctionnaire qui détient une parcelle de la puissance publique pourrait tout savoir de chaque homme, de chaque famille, de chaque entreprise, ne voit-on pas à quels risques l'administré serait exposé ?» (*Bernard Tricot, Rapport de la Commission informatique et libertés, 1975.*)

Si Pierre Piazza a su rappeler la pertinence d'une approche généalogique de la question de la carte d'identité dans le débat sur la CNIE (PIAZZA, 2004), il nous faut ajouter à ce recul sur le temps long la spécificité d'un contexte particulier lié au double phénomène de la mondialisation et de la démocratisation des échanges publics. Depuis 1997, l'insécurité électronique s'est installée comme une donnée majeure des débats permettant ainsi aux gouvernements successifs chargés d'établir une politique de régulation de l'Internet, dans le cadre de la souveraineté nationale, de problématiser la relation entre le pouvoir d'Etat et le réseau des réseaux, en terme de pouvoir d'identification.

Le pouvoir inquisitorial est le fondement essentiel du pouvoir régalien. L'œuvre de Michel Foucault (FOUCAULT, 1975, 1997), à travers son exploration de la gouvernementalité moderne, a depuis longtemps posé les bases heuristiques d'une analyse des technologies de gestion des identités. Consubstantielle au développement de l'Etat moderne, l'autorité judiciaire se fonde sur le passage d'une justice tribale, basée sur le flagrant délit et le duel, à une justice instituée, capable de réinvoquer l'acte par l'enquête (FOUCAULT, 1997). Une technologie informationnelle, du recueil de la trace à la réification de l'acte, en passant par la profilisation du sujet,

assiste le pouvoir de véridicité de l'instance tierce chargée de condamner les infractions. Cette *technologie d'attribution* de l'acte au sujet, désormais « responsable » devant le souverain (que ce soit le Roi ou la Loi), est le premier pilier fondateur de l'Etat de droit. Avec le développement de la police et du dispositif de normalisation des sujets de la nation, le dispositif d'enquête s'étendra de l'infraction à l'évaluation de la quotidienneté. Garant de la santé publique et des bonnes mœurs, l'Etat se dote des moyens d'appréhender les comportements des individus pour mieux mesurer les écarts par rapport aux comportements idéaux inscrits dans une économie globale de la puissance de la nation. Cette *technologie de traçabilité* du quotidien est le second pilier d'un Etat-Providence responsable de la bonne santé de chacun et de l'efficience globale de l'économie nationale. Sa politique d'éducation et de conduite du changement social l'amène à développer cette profilisation des individus, qui se voient désormais refléter en de nombreux dossiers administratif plus ou moins publics. C'est l'ère du développement bureaucratique des fichiers. Dans une logique nosographique, une *technologie de stigmatisation* assurera la qualification des individus selon des critères qui varieront au gré des impératifs et des besoins de politique publique. Selon la logique d'un pouvoir pastoral, l'individu fait partie d'un groupe qualifié selon son espèce et sa position sur le territoire (âge, sexe, origine, adresse territoriale, numéro d'immatriculation, « ethnie »[1]…).

La question de la carte nationale d'identité *électronique* peut être éclairée alors comme le point nodal de rencontre entre la longue évolution d'un dispositif de gouvernementalité de la population (et des individus), le pouvoir inquisitorial et l'émergence d'une nouvelle forme d'espace public médiatisé : Internet. Dans le cadre d'une recherche en sciences de l'information et de la communication, nous avons tenté de suivre la construction des politiques publiques des NTIC en France sur ces dix dernières années (entre 1994 et 2004) au regard d'une rationalité de l'Etat moderne en butte aux nouvelles opportunités d'une mise en réseau des groupes sociaux (LAKEL, 2007). Plus de deux décennies après la loi Safari, enterrée par la loi informatique et libertés de 1978, après la première tentative de la carte d'identité électronique abandonnée à l'arrivée des socialistes au pouvoir en 1981, la CNIE semble réactiver les projets de perfectionnement de la fonction d'identification du sujet sur le territoire national. S'il nous faut saisir la spécificité du débat actuel et des enjeux qu'il soulève, nous ne pouvons que revenir sur les modes de problématisation qui ont présidé à la question de la régulation de l'Internet par le contrôle de l'identité (archives du débat). Face à ce qui s'est élaboré comme un nouveau contrôle de légalité des actes publics, l'Etat s'est engagé dans un renforcement de ses dispositifs de pouvoir actualisés par

les nouvelles technologies. Pour autant, ce renforcement n'est pas un simple accroissement de moyens ou de degrés mais une remise en cause radicale du « compromis de 78 ».

La virtualisation de l'espace public : l'enjeu de la (géo)localisation.

Dans un premier temps, l'interconnexion généralisée apparaît aux acteurs publics comme la condition même du développement des infractions. Ces dernières seraient transnationales dans leur essence même. En un mot, la nature du réseau mondial interconnecté fait de l'Internet un espace de communication qui ne respecte ni les frontières de l'Etat-Nation, ni les lois, ni les règles qui régissent l'ordre de l'échange. Le « *zonage* », qui permettait de qualifier un sujet et ses actes, par son identité nationale, semblait avoir volé en éclats sur Internet. En effet, bien plus qu'une facilitation des échanges transfrontaliers, c'est l'émergence d'un champ d'action sans territoire (virtuel disait-on à l'époque), véritablement globalisé, qui rend préoccupant l'avenir des régimes politiques. La globalisation, enfin réalisée par la technique, fut la première épreuve que les organisations de l'Etat durent affronter pour assurer l'effectivité de leur pouvoir. Vient ensuite *la fugacité des actes* qui pose problème aux pouvoirs inquisitoriaux de la police. Le régime de la preuve repose sur les techniques de traçabilité que mettent en branle les agents de la force publique. Sans trace, on ne peut que constater les dégâts sans pouvoir établir les infractions. Or, Internet semble avoir instauré une course poursuite avec le temps. L'enquête serait le fruit d'une course entre deux régimes de temporalité : celui de la technologie d'enquête, qui tente de reconstituer la scène du crime et celui de l'empreinte, qui a enregistré pour un temps les conséquences de l'acte. Temps de l'enquête et temps de l'acte entreraient en compétition avec le risque d'obsolescence qui pèserait sur le premier. Ainsi, s'ajoutent à la dispersion et à l'internationalisation de l'acte, son extrême rapidité, sa volatilité, voire son instantanéité (FALQUE-PIERROTIN, 1998). Enfin, derrière la question du temps et de l'espace de l'acte, émerge l'enjeu primordial pour le pouvoir inquisitorial : la possibilité de l'identification des auteurs afin de résoudre les contraintes de l'*anonymat. « Le vrai problème actuel est la lutte contre l'anonymat, qui est la base de tous les dérapages, car sans auteur du délit, pas d'application de la loi. »* (CSA, 1999) La dimension virtuelle du réseau (permettant la dichotomie des sujets virtuels, des sujets réels et en particulier du sujet légal, le citoyen), et les *techniques d'anonymisation* défient le droit, qui repose son pouvoir sur l'attribution de la responsabilité.

Ainsi, les contraintes infrastructurelles jouent également contre le pouvoir inquisitorial. Si l'espace a connu une extension dans la globalisation des échanges, le temps s'est, quant à lui, contracté. ***Accélérer les dispositifs d'investigation et rallonger la conservation des traces apparaissent très logiquement comme les fondements d'une restauration du pouvoir de l'enquêteur. La question de l'archivage est donc juridico-politique, la mémoire des actions est la base de la responsabilité.*** *Le pouvoir régalien disparaît dans une société de l'information où il deviendrait difficile de traduire l'identité virtuelle en identité réelle, de conserver les traces des actes, d'en géolocaliser les auteurs.*

Le contrôle d'identité comme fondement du pouvoir d'Etat

Entre remise en cause radicale et extension infinie, les défenseurs du droit ont pris appui sur la notion d'identité numérique, qui a le grand avantage d'être à la fois une propriété en tant que réification informationnelle de la personne et la base de la liberté du sujet. La puissance publique n'aura donc de cesse d'assurer sa présence dans la société de l'information. Elle s'appuiera pour cela sur une triple extension de sa capacité inquisitoriale, censée résoudre les défis du réseau des réseaux :

maîtriser un système de certification électroniques tierces , capables d'assurer le contrôle d'identité dans les transactions contre l'anonymat et la fugacité (1) ;

favoriser le pouvoir d'enquête absolu dans les systèmes d'information informatisés totalement ouvert afin de poursuivre la cybercriminalité dans un monde en réseau (2) ;

mettre en place un système global d'information informatisé qui adapterait les forces de police aux nouveaux modes de criminalité (3).

Pouvoir connaître le sujet en acte est devenu un enjeu stratégique et un objet primordial pour le pouvoir institutionnel. Avec le spam ou la sécurité des transactions, l'identité numérique fait partie de ce type de problématisation paradigmatique qui permet de légitimer la mise en place d'un dispositif de régulation étatique. On peut affirmer que l'ensemble des problématiques politiques sur la question de l'Internet repose sur la question de l'identité comme objet même du pouvoir inquisitorial. L'identité est cet ensemble de données rassemblées, puis unifiées et attribuées à un sujet. L'identité est en quelque sorte le fruit d'un processus de réification du sujet de la loi que les agents de l'Etat, de l'inspecteur des

finances au sociologue de l'INSEE, tentent depuis plus de trois siècles de constituer[2]. **Cette possibilité de modélisation d'une identité est donc bien consubstantielle à la notion de mise en réseau** (**et de recoupement**) **des données.** La défense de la protection de la vie privée vise à empêcher et à limiter l'enquête comme connaissance illégitime du sujet. On distingue deux catégories de données à la source de ce type de traitements : les *données relatives au trafic*, qui permettent d'enregistrer les comportements des individus bien souvent à leur insu, et les *données de transaction*, du même ordre, plus souvent échangées avec le consentement de l'interlocuteur (même si les traitements postérieurs en vue d'une profilisation ne sont pas toujours clairement perçus, *l'archive dans les mémoires en ligne* est à ce titre un enjeu essentiel).

Dans la question de cette identité, une information particulière, si menue soit-elle[3], joue un rôle stratégique, voire systémique : l'**identifiant**. L'identifiant est une méta-information qui s'ajoute à une grappe de données reliées entre elles de façon définitive. Cet identifiant permet de rassembler toutes ces grappes en un tout unique (et ce indépendamment de leur éparpillement temporel ou spatial). Sans identifiant, la grappe de données est fermée sur elle-même et donc très limitée dans son usage. Sans identifiant, pas d'identité digne de ce nom, capable de constituer un sujet. Par contre, plus le même identifiant sera utilisé, plus l'interconnexion permettra une pertinence d'analyse, plus elle sera capable d'individualiser le sujet. Au premier rang des identifiants numériques viennent ces numéros que les institutions attribuent à leurs assujettis, usagers, clients, membres. Ces « *identifiants de gestion » permettent aux organisations de regrouper, sans ambiguïté, toute une série d'informations sur une même personne. Certains identifiants sont stables* » (TRUCHE *et alii*, 2002)[4]. La signature manuscrite a joué ce rôle de signe métonymique arbitraire individualisant. Elle joue encore de nos jours un rôle d'authentification de la personne et du consentement en acte. Son équivalent numérique assure une reconnaissance du sujet au fur et à mesure des transactions. **Le développement d'une signature électronique unique est la base de l'identification globale et donc du contrôle de l'identité du sujet.** (Les cartes de crédit, de consommation, de client, et leur couple numéro/code, appartiennent à cette catégorie).

Une identité particulière possède une valeur sans égal dans la relation de pouvoir que l'on peut établir avec un individu : l'identité personnelle. **Un processus d'identification qui relie une somme d'informations à une vie biologique unique, et ce de façon indiscutable.** Cette identité personnelle fonde la relation de pouvoir entre le souverain et ses sujets par la connaissance des corps. Cette identité se fonde sur la présence d'une

trace valide du corps du sujet comme identifiant infalsifiable (présence réifiée par une donnée biométrique : empreinte, photo et tout autre procédé comme l'ADN). L'identité personnelle révèle clairement la base du pouvoir de l'Etat : la vie de l'espèce territorialisée. **Voilà la plus grande problématique de la gouvernance de l'internet depuis 2001.** Chaque ministère a en réalité développé son identifiant personnel unique (NUMEN pour l'éducation nationale ; SPI pour l'administration fiscale), qui est devenu un véritable identifiant sectoriel pour une utilisation globale chez tous les acteurs professionnels publics ou privés. En 1983, la jeune CNIL, dans sa délibération n°83–058, avait constaté avec impuissance la logique d'utilisation extensive du NIR comme identifiant sectoriel global du secteur de la sécurité sociale. Si elle a dû accepter l'état de fait, elle a, dans le même temps, donné naissance à son principe de « cantonnement » sectoriel des identifiants. Or, ces identifiants ne peuvent devenir certains que par recoupement via le NIR. Dans nos sociétés, l'Etat civil et ses différents supports (dont la carte d'identité est la base) jouent ce rôle. Dans le cadre d'une procédure formalisée, le sujet habitant en France devient citoyen ou résident étranger (ou réfugié politique, etc.) par la reconnaissance de son identité, manifestée par la possession d'un titre d'identité. Pour que ce titre d'identité soit valable, la procédure met en relation un ou plusieurs agents accrédités par l'Etat, en présence de la personne à identifier. L'agent assermenté relèvera une série d'informations biométriques pertinentes pour l'identification physique de la personne (taille, sexe, âge, lieu de naissance, signature, photo et surtout empreintes). A cette présence physique, il associera les informations propres à l'Etat civil (prénom, nom, adresse et ID). Il ajoutera, à des fins de contrôle, l'identification de l'autorité de certification (la préfecture et signature de l'autorité). Afin de s'assurer de l'unicité du titre, il rendra cette carte infalsifiable et renouvelable périodiquement. Cependant, cette *procédure d'authentification*, si elle est déjà assurée par la possession de ce titre matériel, n'est absolue que dans la relation triangulaire qui relie un agent identificateur et un sujet identifié par le recours à la base de données de l'autorité d'authentification.

Les technologies de l'information et de la communication comme mode absolu d'identification.

L'identité a une double nature, à la fois objet informationnel et réification d'un sujet, qui peut être par extension un être humain. Le pouvoir inquisitorial n'est donc pas un outil de savoir neutre. L'appropriation d'objets informationnels, quand elle autorise la connaissance de sujets actants, est le préalable à une connaissance des conditions de la liberté

humaine. La base d'une technologie permet donc de déterminer une stratégie dans le cadre d'une relation de pouvoir. Internet semble, à ce titre, permettre une extension quasi-infinie du pouvoir inquisitorial, de l'enregistrement généralisé, de la mémorisation infinie au service de puissants outils de recherche. Mais au service de qui ? Ainsi, que ce soit par la description d'un Internet comme barrage au pouvoir inquisitorial ou celle d'un Internet comme extension infinie de ce pouvoir, la problématisation juridique de l'Internet s'attache à souligner une question essentielle : l'émergence des intermédiaires techniques dans cette relation de pouvoir (et celle de leur légitimité).

On peut dire que sur Internet, il ne peut y avoir de communication sans signature électronique, c'est-à-dire sans processus d'authentification. La première des signatures est inscrite au cœur même du protocole TCP/IP et vise à identifier les machines. D'une part, l'adresse IP fait office d'identité temporaire de la machine car elle est fournie par le fournisseur d'accès durant un délai limité et, d'autre part, l'adresse MAC du module de connexion permet de connaître son identité définitive (l'adresse IP permet toutefois de connaître l'identité fixe du fournisseur d'accès)[5]. Mais l'identité d'une machine n'est pas celle d'un sujet de droit. Même si aujourd'hui les fournisseurs d'accès sont tenus de conserver des journaux de connexion associant leurs clients à des adresses IP et MAC, la responsabilité individuelle est toujours sujette à caution. Cette adresse peut toujours être usurpée ou « spoofée » (particulièrement avec l'explosion du Wi-Fi), la connexion Internet peut être collective (cas d'un cybercafé ou d'une entreprise avec un serveur proxy ou un routeur NAT, d'un réseau familial, etc.), la responsabilisation d'un acteur identifié est précaire (même si elle n'est pas impossible). Dans le système Internet, la signature électronique, basée notamment sur une infrastructure à clé publique (type PKI), est la seule capable d'assurer l'authentification des interlocuteurs d'une transaction spécifique par l'intervention d'un tiers. Ce dernier permet non seulement l'intégrité de l'échange, en assurant le traçage et l'enregistrement des informations, mais aussi l'identification réelle des auteurs en fonction des règles en vigueur. En imposant, comme condition a priori, la signature électronique à l'ensemble des échanges (par l'usage d'un login/mot de passe, par le téléphone via SMS, par les cartes à puce, CVQ, CNIE, CB...), on s'assure en amont la réintégration de la communication à un espace traçable au niveau du sujet de la loi. L'authentification électronique est la règle qui fait disparaître « l'anonymat » du sujet dans la communication électronique. Le modèle le plus abouti s'appuie sur une architecture à « fédération d'identités » qui centralise un unique « Espace de Confiance Primaire », ECP (comprendre Espace de Contrôle Central), gérant un méta-identifiant relié par des

vecteurs d'identification à des « Espaces de Confiance Secondaire », ECS (où Espace de Contrôle Sectoriel) gouvernant les identifiants sectoriels. Mais le rôle central du « service de propagation » dans l'interconnexion des données réside dans ce pouvoir de mémorisation et de traçabilité. **C'est l'objectif d'une centralisation de l'identification, qu'elle soit privée ou publique, comme condition a priori des transactions sur Internet.**

C'est dans le cadre d'abord contractuel du commerce électronique, puis dans les relations entre administration électronique et usager, que la signature électronique a pu devenir le laboratoire d'une relation entre droit et technologie. Dès son origine, le PAGSI avait donné la priorité aux « *conditions de reconnaissance de la signature électronique dans les relations entre les administrations et le public* » en s'attaquant en priorité aux « *problèmes d'authentification, de sécurité et de confidentialité des transactions* » (PAGSI, 1997). La question de la signature électronique assure, à condition que le tiers de confiance soit sous le contrôle de l'Etat, la non révocabilité des actes. Contre la fugacité des échanges, un espace de séquestre des actes légaux rend possible la constitution d'actes authentiques. « *Le problème de la preuve reste l'une des difficultés à résoudre pour généraliser les échanges électroniques avec les administrations dont le droit est imprégné des pratiques traditionnelles en matière d'échanges sur support papier.* » (PRADA, 1997) Mais l'émergence d'un tiers comme condition de possibilité d'une communication électronique authentifiable révèle un dispositif qui se constituera comme le modèle d'un droit assuré par une technique, administrée par un opérateur. La question de la signature électronique est manifestement apparue comme un laboratoire testant, dans un champ restreint, les possibilités de régulation de la communication.

Pourtant, le tiers n'avait jusque-là que très peu de moyens pour s'assurer de la véracité des déclarations préalables des auteurs. Numéro de carte de crédit et photocopies de documents identifiants sont encore sujets à falsification. Seul un pouvoir de contrôle avancé permettrait de résoudre définitivement cette incertitude. Seul l'Etat, dans sa volonté de récupérer la gouvernance de l'information sur Internet, peut réaffirmer son droit au contrôle absolu de l'identité. Parallèlement aux modes de régulation traditionnels, la régulation par le code devait aboutir à de nouveaux types d'instances de régulation. Importées directement des transactions entre entreprises privées et clients, les transactions entre l'Etat et la société civile seraient assurées par un dispositif électronique de gestion d'identité électronique : la carte nationale d'identité électronique, couplée au dispositif d'interconnexion des identifiants sectoriels « mon.service-public.fr ». Fruit d'une série de projets en technologies de l'information et de la communication, autour d'une infrastructure de gestion de clés pour

ses services administratifs en ligne, le ministère des finances, en tant que ministère le plus avancé en matière de NTIC[6], et le ministère de l'intérieur, seul légitime à contrôler l'identité des citoyens, souhaitent désormais mettre en place une véritable « citoyenneté numérique » chargée de restaurer la base de l'Etat de droit sur Internet par l'authentification et la responsabilité du citoyen. « *En sécurisant cette procédure, l'État se donnerait les moyens de mieux garantir l'identité des citoyens français.* » (TRUCHE *et alii*, 2002) Tout d'abord, les acteurs publics de l'Internet souhaitent constituer une identité numérique publique pour chaque résident français. Cette identité serait conservée par l'Etat dans un coffre fort et permettrait d'interconnecter toutes les informations issues de tous les services publics. Ainsi, la problématique de l'interconnexion des bases de données des administrations serait dépassée par l'émergence d'un espace tiers, ayant seul le pouvoir de recevoir ou d'émettre les données. Cet espace conserverait en son sein l'ensemble des données pertinentes pour les transactions administratives ou privées. Ces dernières seraient ainsi mises en relation sans que les bases de données des administrations aient à l'être. De plus, cet espace pourrait archiver les transactions administratives et conserver les documents produits dans la période de leur validité. Il s'agit directement d'une récupération des projets de compte universel des consommateurs, comme le projet « passeport » de Microsoft, proposé dès 1998[7].

La métaphore du coffre-fort suggère que les données personnelles sont « enfermées » (sous clé) et que seule la personne concernée (son détenteur ou son « propriétaire ») est habilitée à y accéder ou à les transmettre. Pour puiser ces données dans le coffre-fort, les interlocuteurs (entreprises ou administrations) doivent obtenir son autorisation et, éventuellement, la clé. Cette notion de coffre-fort renvoie à une grande diversité de dispositifs et d'architectures. Pourtant, l'idée d'une nouvelle génération de carte d'identité apparaît à tous comme le meilleur compromis entre fiabilité et facilité. Cette carte deviendrait, outre une carte comportant une série d'informations sur l'usager, un trousseau de clés d'accès au compte personnel public. Le rapport TRUCHE, après consultation des intéressés, nous a annoncé officiellement que le ministère de l'intérieur, sous la direction de son ministre de l'époque, Nicolas Sarkozy, conduisait sérieusement un projet en ce sens. Le ministère de l'intérieur a réaffirmé son angoisse permanente de rendre plus sûre la procédure de délivrance des titres d'identité. Le projet unifierait l'identité du sujet sous un « titre fondateur » dans la mesure où il permettrait la délivrance, dans un premier temps, de la carte nationale d'identité et du passeport et autoriserait ensuite, l'ajout d'autres titres publics ou privés : la carte nationale d'identité électronique (CNIE+ passeport) ; la carte du citoyen (CNIE +

carte électorale) ; la carte du conducteur (CNIE + permis de conduire).[8]

Conclusion : l'actualité de la question de l'interconnexion comme limite au pouvoir d'Etat.

Aujourd'hui, Internet comme système d'information, constitué de l'interconnexion a priori des réseaux (le réseau des réseaux), rend possible l'interconnexion globale des systèmes de fichiers. Dans cette Société de l'Information, le droit distingue un système de cercles concentriques qui, de la périphérie au centre, autorise toujours plus de pouvoir sur la gestion des données personnelles. La zone du secteur privé (1), une zone tabou fortement contrôlée par la CNIL, la zone des services publics ou privés liés aux transactions (2) et enfin celle des institutions de police et de justice (3), aux pouvoirs largement étendus par les réformes législatives depuis le 11 septembre 2001, sont autant de lieux d'enregistrement possible, plus ou moins absolu, des données personnelles.

Les données sont elles-mêmes hiérarchisées. Données relatives au trafic, données de transaction (3), données personnelles (2), données personnelles sensibles (1) (Article 8 de la loi informatique et libertés rénovée), données d'identification (0) sont éparpillées en une multitude de fichiers, qui forme une mosaïque complexe réifiant l'identité du sujet et l'histoire de ses transactions avec son environnement. **Cependant, pour que cette mosaïque forme une unité liée à un individu, il faudrait un identifiant unique à tous ces fichiers** (**fusse-t-il une simple combinaison alphanumérique**) **enregistré selon une procédure d'authentification biométrique certaine, archivant chaque transaction.**

Un fichier central de l'identité numérique ne serait autre qu'une méta-base de données relationnelle, dont l'une des tables principales fonderait la carte nationale d'identité électronique (les autres servant principalement à l'archivage des transactions certifiées[9]). Chaque individu présent sur le territoire obtiendrait donc une occurrence dans ce fichier à travers l'obtention de sa CNIE. Dans une infrastructure interconnectée a priori, la société de l'information deviendrait un unique fichier contenant une base de données relationnelle répartie en une pyramide de pouvoirs, dont le sommet serait tenu par les instances inquisitoriales régaliennes (ministère de l'intérieur et ministère des finances), le cœur, par les secteurs d'administration publique et affiliés (Sécurité sociale, santé, éducation…), et la base, par les grands services de consommation (Carte Bleue, Carte de Vie Quotidienne, Carte de

consommation), dont la cohérence reposerait sur l'utilisation de l'identifiant numérique unique (un simple numéro unique et infalsifiable).

Le ministère de l'intérieur souhaite que cet identifiant unique (matérialisé par la CNIE) serve à l'ensemble des transactions individuelles (qu'elles soient publiques ou privées), que ce soit sur le territoire national ou en dehors (d'où l'intérêt d'unifier les cartes d'identité et les passeports). Ainsi, l'ensemble des données individuelles serait mis en cohérence par cet identifiant. A chaque usage d'une identification certifiée par l'utilisation de la CNIE, les données recueillies nourriront le fichier unique virtuel du sujet actant. Pour apporter une certitude à l'authentification de l'interlocuteur, la carte a enrichi sa batterie d'identifications personnelles, en y ajoutant de nouvelles données biométriques (photo et empreinte digitale numérique, et pourquoi pas Iris et code ADN ?) et en les numérisant. Le législateur a modifié la loi informatique et libertés pour autoriser l'ensemble du service public à procéder à des identifications biométriques : les services privés étant autorisés à relever les identifiants généraux et à les vérifier par une authentification moins sûre (type carte de crédit, qui combine le numéro de la carte, son code PIN et une validation interne ou externe).

Ce « fichier unique virtuel et réparti », qui recouperait l'ensemble des données individuelles, réside d'une métaphore. Celle d'une base de données virtuelle nécessitant une actualisation par une procédure d'interconnexion, car en effet, dans un système de données relationnelles réparties et basées sur une infrastructure de communication interconnectée a priori, il n'est nul besoin d'une interconnexion permanente des fichiers ou que les identifiants soit signifiants (cette propriété n'ayant que peu d'importance dans ce système, le débat de la CNIL sur ce sujet est tout simplement obsolète). Le traitement des données, à partir de la mise en relation par l'identification unique ou d'un système unique d'identifiants pluriels, actualise l'occurrence d'un fichier unique. Ainsi, la fonction d'authentification et d'identification joue un rôle systémique primordial, non seulement dans l'enregistrement des données, mais dans l'actualisation par l'enquête de ce fichier virtuel unique. Il suffit à un agent d'obtenir un ensemble de grappes de données réparties possédant la même *"grappe d'identifiant"*, pour actualiser l'occurrence d'un fichier global pertinent. Les fichiers ne sont donc pas interconnectés, mais c'est la requête de l'agent qui interconnecte les identifiants et les tables de données réparties qui lui sont liées. Il suffit juste alors de donner tous les pouvoir a cet agent...

Or, les réformes récentes ont donné au pouvoir inquisitorial d'Etat, dans l'océan numérique, une extension de ses prérogatives depuis

l'année 2004. Elle s'est opérée de façon éparse et parcimonieuse, au fil d'une multitude de lois sur la sécurité intérieure (LSQ, LSI, Loi Perben II, LCEN, Loi dite « Paquet télécom », Réforme de la loi informatique et libertés, etc.)[10]. **La volonté de rendre transparente une société de l'information, qui recoupe toute la communication sociale, est très claire. Nulle barrière ne doit exister entre l'autorité judiciaire et le cyber-citoyen.** D'une part, le droit de la police à accéder à toutes les communications est réaffirmé avec force. D'autre part, son droit à garder secret ses démarches d'enquête lui assure une invisibilité dont la logique fut largement explicitée par Michel Foucault dans son modèle du panoptique. Nous avons pu dégager un processus permanent d'extension de ce pouvoir d'enquête à travers la mosaïque, toujours plus complexe, des réformes législatives. Du délinquant sexuel au militant syndical, jusqu'à bientôt l'usager des services publics, le système unique d'identification s'offre comme accélération de l'efficacité de l'administration publique. Une politique d'intégration progressive de l'innovation techno-politique prend en compte l'acceptabilité sociale du contrôle. Aujourd'hui, l'administration électronique apparaît comme le dernier contrat pour une extension généralisée de ce dispositif : transparence contre facilité, contrôle contre efficacité.

Les débats actuels révèlent la persévérance et la pugnacité du corps administratif à vouloir imposer, depuis plus de 40 ans, un fichier central unique autour du NIR. Après le coup de flibustier, au début des années 70, du projet SAFARI, après le coup de force, au début des années 80, du secteur des services sociaux à utiliser le NIR, après le développement des années 90, des grands identifiants sectoriels nationaux (le dernier en date étant l'identifiant national de santé, voir supra note 9), la CNIL doit de nouveau faire face au retour d'une tentative de projet central d'identifiant. La délibération de la CNIL du 8 décembre 2005 (n°2005–304) portant sur le projet « mon service public » et le débat national sur la Carte Nationale d'Identité Electronique, tous deux présentés par Madame Falque-Pierrotin, à la fois commissaire à la CNIL et présidente du Forum des Droits de l'Internet, promeuvent une nouvelle architecture de fédération d'identités autour d'un identifiant unique. Les nombreuses réserves de la CNIL et la levée de boucliers des usagers, lors des débats publics, montrent qu'aujourd'hui le terme de « confiance » tant usité dans les projets d'identité numérique publique est devenu un signal pour les autorités de régulation et les défenseurs des libertés civiles qui exigent « un bilan précis des expérimentations » (CNIL, 2005)

Les NTIC ont révélé, par leur potentialité technologique, l'étendue des capacités d'un nouveau dispositif de savoir au service du pouvoir. **En 2004,**

depuis la révision de la loi « informatique et libertés », sur décret du Conseil d'Etat, l'Etat est autorisé, toujours après avis de la CNIL, à collecter les données sur « ***les origines raciales ou ethniques, les opinions politiques, philosophiques ou religieuses ou l'appartenance syndicale des personnes, ou qui sont relatives à la santé ou à la vie sexuelle de celles-ci*** » (**art. 8 I**)**. La tension entre pouvoir inquisitorial, droit de l'homme et libertés individuelles fondamentales est à la base de la légitimité de l'Etat de droit.** La convention sur la cybercriminalité du Conseil de l'Europe avait pris toute la mesure des risques d'un droit international qui en appelle au développement du pouvoir d'enquête. Tiraillé entre l'impératif de protéger le capital informationnel et celui d'assurer les droits de l'homme, l'article 15 rappelle en préambule de la section 2, sur le droit procédural :

> « Chaque partie veille à ce que l'instauration, la mise en œuvre et l'application des pouvoirs et procédures prévus dans la présente section soient soumises aux conditions et sauvegardes prévues par son droit interne, qui doit assurer une protection adéquate des droits de l'homme et des libertés (…) ces conditions et sauvegardes incluent, entre autres, une supervision judiciaire ou d'autres formes de supervision indépendante, des motifs justifiant l'application ainsi que la limitation du champ d'application et de la durée du pouvoir ou de la procédure en question.. »

Et dans le même article, la convention invite les Etats à « *examiner l'effet des pouvoirs et procédures dans cette Section sur les droits, responsabilités et intérêts légitimes des tiers.* » Dans le même esprit, en France, la loi du 6 janvier 1978, relative à l'informatique, aux fichiers et aux libertés avait voulu établir un cadre légal aux menaces du pouvoir inquisitorial, assisté par les technologies de l'information. Elle rappelait, dans son article premier, que l'informatique « *ne doit porter atteinte ni à l'identité humaine, ni aux droits de l'homme, ni à la vie privée, ni aux libertés individuelles ou publiques.* » Ainsi, face aux déséquilibres instaurés entre les technologies de savoir et la liberté des individus à connaître une vie paisible, la notion de données personnelles (ou nominatives en 78) avait permis d'instituer une frontière entre libertés personnelles et responsabilité publique dans l'espace public médiatisé. Comment s'assurer d'un nouveau compromis sans remettre en cause la mise en satellite de la CNIL par rapport aux prérogatives d'Etat ?

BIBLIOGRAPHIE :

ALCAUD David, LAKEL Amar (2004), « Electronic Government and the French State: a negotiated and gradual reform", in *Information polity*,

London, IOS Press, 2004.

Conseil Supérieur de l'Audiovisuel, *Communication audiovisuelle et Internet : journée d'étude du 14 octobre 1999*, Paris, CSA.

FALQUE-PIERROTIN Isabelle, THERY Jean-François, *Internet et les réseaux numériques*, Paris, La Documentation française, 1998.

FAUGERE Jean-Paul, FLICHY Patrice, TRUCHE Pierre, *Administration électronique et protection des données personnelles : Livre blanc*, Paris, La Documentation française, 2002.

FOUCAULT Michel, Surveiller et punir, Paris, Gallimard, Bibliothèque des histoires, 1975.

FOUCAULT Michel, *« Il faut défendre la société » : cours au Collège de France (1975–1976)*, Paris, Seuil, 1997, pp.283

LAKEL Amar, « La CNIE et le pouvoir d'enquête en France : l'interconnexion au défi des technologies de l'information et de la communication. », in *Débat national sur la carte d'identité électronique*, Paris, Forum des Droits de l'Internet, mars 2005.

LAKEL Amar, *L'administration électronique : laboratoire de la gouvernance sur internet*, Rennes, Editions Apogée, 2007.

LESSIG Lawrence (1999), *Code and other laws of cyberspace*, New York, Basik Book, 1999.

PIAZZA Pierre, *Histoire de la carte nationale d'identité*, Paris, Odile Jacob, 2004.

PREMIER MINISTRE, *Préparer l'entrée de la France dans la société de l'information : programme d'action gouvernemental*, Paris, La Documentation française, 1998.

ROBERT Pascal, *Logique politique des technologies de l'information et de la communication*, P.U. de Bordeaux, Bordeaux, 2005.

[1] Même si en France, cette référence est devenue indirecte en raison du passé de l'administration française sous Vichy. En effet, contrairement à de nombreux pays (les ex-pays du bloc soviétique en sont l'exemple le plus

notable), en France l'ethnie ne se déclare pas mais peut se déduire par recoupement du nom et du prénom, du lieu de naissance et de la photo. En cas de recherche, les ascendants peuvent permettre de retrouver avec une quasi-certitude « l'appartenance ethnique » d'un individu.

[2]Erik Neveu (NEVEU, 2001) a réintroduit cette réflexion dans la problématisation de la société de l'information.

[3] Souvent une simple combinaison alphanumérique.

[4] En France, la loi sous le contrôle de la CNIL, surveille l'usage des identifiants pour qu'il ne soit pas signifiant. Mais la bataille la plus importante autour d'un identifiant fut sans nul doute celle du NIR. Sous le régime de Vichy, l'INSEE a créé le NIR, numéro d'inscription au RNIPP, afin de renforcer l'identification des sujets vivant sur le territoire d'une façon permanente, fiable et stable. Cet identifiant est totalement signifiant au point d'être une véritable carte d'identité numérique qui renseigne le lecteur de ce numéro sur le sexe, l'âge et le lieu de naissance (particulièrement, par le 99, si ce lieu est étranger au territoire français).

[5] Il faut se rappeler que depuis son origine jusqu'à la création de l'ICANN, le réseau des réseaux, qui partout promeut le mode organisationnel complexe d'unités autonomes interconnectées (sur le paradigme du P2P), a fait preuve d'un conservatisme anachronique en ce qui concerne les questions d'identité. Si de nombreux experts ont manifesté leur étonnement devant cette « anomalie » technique, l'infrastructure hiérarchique et centralisée des adressages (IP et Noms de domaine), nous voudrions soutenir l'hypothèse qu'à l'origine du projet, la question de l'identification et de son architecture technique était inscrite dans le code.

[6] Ministère qui a récupéré, à ce titre, l'ensemble du projet d'administration électronique par la dissolution, en 2005, de l'Agence de Développement de l'Administration Electronique (ADAE), rattachée au Service du Premier ministre, et la création, le 1er janvier 2006, au sein du MINEFI, de la Direction Générale de la Modernisation de l'Etat (DGME), avec en son sein le Service du développement de l'administration électronique (SDAE). (ALCAUD et LAKEL, 2004)

[7] Le projet, abandonné sous la pression des associations d'usagers, relayées par les gouvernements, a donné naissance à une norme proposée par le projet Liberty Alliance (http://www.projectliberty.org/)

[8] Pour une discussion plus poussée sur la CNIE, voir (LAKEL, 2005)

[9] La conservation des données personnelles mutualisées dans cette base de données est une option qui n'a que peu d'importance dans le système, car peu importe le lieu ou sont conservées ces données (sur la carte, dans un fichier central, dans des fichiers non interconnectés, etc.), l'enjeu politique réside avant tout dans les modalités d'accès.

[10] Pour le suivi et les archives de cette tumultueuse tactique juridique, se reporter au site de Meriem Marzouki, présidente de l'IRIS (http://www.iris.sgdg.org)

PUBLISHED IN

Internet Governance

My Papers between 2002 and 2007 about Internet Governance

WRITTEN ON DEC 28, 2014 BY

Amar Lakel

Expert in Digital Marketing research, i drive, since 15 years, data analysis on web consummers behavior for optimising digital marketing strategies.