Strauss Jean Luc

De: Jean-Luc STRAUSS [jeanluc@strausshiva.com]

Envoyé: lundi 13 avril 2009 12:54

À: Strauss Jean Luc

Objet: Envoi d'un message : L'émergence du double numérique - Version imprimable - Société de l'information - L'observatoire des Usages de l'Internet.htm

L'émergence du double numérique

Date 28/2/2006 18:30:00 | **Sujet :** Société de l'information

Sommaire :

Présentation
Le double numérique correspond à l'ensemble des données personnelles recueillies par tous les systèmes d'information aussi bien publics que privés.
Le double numérique est pour le moment constitué de fichiers publics distincts, administrés de manière à préserver les données personnelles, selon les directives de la CNIL. Mais il existe une double pression à la fois du secteur public (sous couvert de lutte contre le terrorisme) et du secteur privé (pour réduire les fraudes du commerce électronique) pour connecter l'ensemble des fichiers à données personnelles avec introduction de la biométrie. Cette évolution quasi irréversible conduit à " marquer " de façon sûre et quasi indélébile chacun des individus. Se trouve par conséquent à nouveau posé le problème de l'exercice de la liberté individuelle si rien n'est fait à l'encontre de cette tendance
Action demandée :
Mener une action concertée pour conscientiser les populations sur les dangers des usages du double numérique.

Interpeller les autorités pour rendre transparentes les données des individus : au lieu de chercher à conserver le caractère étanche des données personnelles en les tenant séparées et contrôlées de manière spécifique au niveau des usages qui en sont faits, il convient de donner accès à son double numérique à tout individu en lui procurant les moyens de faire effacer les aspects jugés non conformes à l'exercice de sa liberté.

Situation actuelle

La liberté que proclame l'article 2 de la Déclaration des droits de l'homme et du citoyen de 1789 implique le respect de la vie privée. La liberté individuelle est protégée par l'autorité judiciaire au titre de l'article 66 de la Constitution, l'article 34 donnant la compétence exclusive au législateur de fixer les règles concernant les garanties fondamentales accordées aux citoyens pour l'exercice des libertés publiques.

Les données personnelles sont stockées dans les bases de données conservées par les services qui les ont collectés (administration, éducation, santé, banques, services divers...) avec un droit de regard donné à l'usager par la CNIL (Commission nationale de l'informatique et des libertés). Le croisement de ces données est contrôlé par la loi informatique et libertés qui délimite strictement les conditions d'usage des données personnelles afin de protéger les droits de l'usager concerné. Il n'en reste pas moins que chaque ministère a son propre identifiant, par exemple : NUMEN à l'Education Nationale, projet Copernic aux Finances.

* La nouvelle loi Informatique et liberté, publiée au Journal officiel du 8 août 2004, transpose la directive communautaire 95/46/CE et modifie la loi du 6 janvier 1978 relative à l'informatique aux fichiers et aux libertés. Le nouveau texte simplifie les formalités de déclaration des fichiers de données personnelles (1). L'allégement de ces formalités trouve sa contrepartie dans l'augmentation des pouvoirs de la CNIL. La loi précise les modalités de cette action, maintient l'existence du délit d'entrave et renforce la coopération de la CNIL avec la justice. En cas d'urgence, la CNIL peut recourir au référé sous astreinte, ordonner le verrouillage de bases de données et l'interruption de traitements ou encore retirer une autorisation, enfin infliger une amende.

* La loi n° 2004-575 du 21 juin 2004 relative à la confiance dans l'économie numérique ne permet pas d'utiliser le contenu des communications par téléphones portables et sur Internet sans de bonnes raisons. Toutefois, les numéros appelés, la

localisation et la durée de l'appel sont des éléments que les fournisseurs d'accès doivent systématiquement stocker (2).

Le citoyen n'a pour le moment pas un droit de regard effectif sur les données stockées à son sujet, encore moins le pouvoir de les modifier. Ces données sont éparpillées dans toute sortes de services privés ou publics. Il n'a pas connaissance de leur nature et peut difficilement en contrôler l'usage. Il court aussi le risque de captation d'identité et de falsification de données sur lui. Il n'est pas maître de sa propre information ce qui nous paraît contraire à l'exercice de la liberté individuelle.

Tendances constatées

L'omniprésence des outils de surveillance dans l'espace public entraîne la multiplication des possibilités de traçage des individus dans leur vie quotidienne. Ainsi une personne peut apparaître 200 fois dans une seule journée sur les caméras de surveillance dans les rues d'une ville. Le résultat est l'accumulation de données à caractère personnel sur les fichiers de surveillance permettant de bâtir un double numérique complet en ce sens qu'il permettra d'éliminer toutes les zones d'ombre dans lesquelles la personne pouvait jusqu'à présent passer inaperçue. Si l'usage de l'identifiant personnel unique est protégé par la loi en France, il n'en reste pas moins qu'il est de plus en plus utilisé pour relier des fichiers à caractère personnel qui se multiplient au fur et à mesure du traçage généralisé des individus rendu possible par les développements des outils idoines. D'autre part, sous la double pression, à la fois des secteurs publics, et des secteurs privés marchands, nous constatons une tendance forte vers le croisement des données en France, en Europe et partout dans le monde.

Quelques exemples de cette tendance en France

* La carte vitale + identité personnelle
Cette tendance vers la centralisation des données personnelles s'observe avec le développement de la carte vitale qui regroupe les données personnelles concernant l'assuré social afin de mieux contrôler les dépenses de santé. La réduction de la fraude sous forme de captation d'identité est combattue par l'ajout sur la carte de la photographie de l'assuré social. Le choix d'un médecin traitant à même de juger de la pertinence des examens et traitements à engager, est proposé pour réduire les dépenses de la caisse maladies.

* La carte de vie quotidienne est une autre manière d'intégrer un ensemble de services publics à la personne sous forme d'un système de paiement électronique centralisé.

* La nouvelle carte d'identité
Le programme français de carte d'identité électronique INES propose d'architecturer les services d'identification policière, administrative et commerciale autour d'une procédure d'authentification unique de la personne, comme c'est déjà le cas en Belgique. Sur cette carte seront inscrits des droits tels que le permis de conduire, la carte d'électeur et la signature électronique à des fins d'authentification de documents et de commerce électronique.

* Le secteur marchand : Le développement des échanges électroniques dans l'univers marchand tend également à l'identification la plus fine et exacte des consommateurs afin d'éviter les impayés et les fraudes en repérant à l'avance ceux susceptibles d'en être passibles. Du point de vue de la sécurisation des échanges commerciaux électroniques, l'objectif est de s'assurer non seulement de l'identité du client mais de sa capacité à payer. La partie des données personnelles relatives à la définition des goûts et préférences qui débouchent sur les choix dans l'acte d'achat, est un autre aspect qui intéresse le secteur marchand. Les gestionnaires de cartes de crédit sont détenteurs de très nombreuses informations relatives à notre mode de consommation. Notre comportement de consommateur est ainsi suivi au plus près par les méthodes de traçage électroniques. La technique du traçage de chaque bien est rendue possible par l'utilisation de puces électroniques permettant de l'identifier tout au long de son cycle de production et d'usage. Les récents développements en radio fréquence font qu'il est possible de suivre géographiquement les biens, de l'entrepôt au magasin jusque chez le consommateur. Un rapide examen au scanner de ce dernier dans la rue et sans qu'il s'en rende compte, permettra de repérer la provenance de ses vêtements. De cette manière, la vérification des effets des campagnes de publicité peut être réalisée sous forme non seulement de chiffres de vente mais aussi de types d'usages en temps réel quasiment.

Le double numérique est donc en train de devenir une réalité : Les données personnelles recouvrent d'abord celles relatives à l'identité de la personne, telles qu'elles figurent sur sa carte d'identité, son passeport, son permis de conduire. Ces éléments ont vocation à être accessibles par l'identifiant unique personnel comme c'est le cas avec le numéro INSEE. Elles concernent aussi l'ensemble des informations relatives aux caractéristiques de la personne telles qu'elles peuvent être déduites de ses interactions sur les réseaux. Il s'agit de ses modes de consommation et de production mais aussi de ses préférences, de ses capacités avérées, de ses problèmes de santé, etc.. L'éventail de ce type de données s'élargit sans cesse avec les nouveaux usages qui se développent sur les réseaux de communication au fur et à mesure de l'intégration des outils et services qui y sont offerts.

Les données personnelles sont de plus en plus utilisées par le e-gouvernement, la e-santé, le e-commerce, avec l'utilisation de puces électroniques disposées sur les biens et bientôt sur les personnes aux fins d'authentification.

Exemples de pratiques à l'étranger

La Belgique a déjà mis en place la carte d'identité électronique, gérée par Microsoft, selon les principes d'interconnexion des données personnelles administratives et commerciales.

Le contenu des communications par téléphones portables et sur Internet ne peut pas être enregistré sans de bonnes raisons,

mais les numéros appelés, la localisation et la durée de l'appel sont des éléments que les fournisseurs d'accès doivent systématiquement stocker en Italie, Allemagne et Royaume-Uni.

Mise en place d'un projet de directive européenne sur les communications électroniques: données personnelles, protection de la vie privée et l'accès aux données relatives au trafic à des fins antiterroristes (modif. direct. 2002/58/EC).

L'Union européenne s'est dotée d'une législation sur la protection de la vie privée sur le modèle de la loi française Informatique et libertés, et notamment l'article 5 de la convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (directive 95/46 du Parlement européen et du Conseil du 24 octobre 1995). Mais la situation face au terrorisme international (et sous la pression du Royaume-Uni, de la France, de la Suède et de l'Irlande) a fait naître ce projet de directive selon lequel les États membres devraient veiller à ce que soient conservées les données nécessaires pour :
- retrouver et identifier la source d'une communication;
- retrouver et identifier la destination d'une communication,-;
- déterminer la date, l'heure et la durée d'une communication; déterminer le type de communication;
- déterminer le dispositif de communication utilisé ou ce qui est censé avoir été utilisé comme dispositif de communication;
- localiser le matériel de communication mobile.

Les technologies de reconnaissance biométrique sont en train d'être adoptées en Europe, après les Etats-Unis, avec les conséquences de divulgation de toutes les données personnelles à un ensemble de services qui ne sont pas redevables à l'individu de la manière dont ces informations rassemblées sur lui peuvent être utilisées, en l'absence d'organismes équivalent à la CNIL.

A la demande de la Commission européenne, les premiers passeports biométriques européens apparaissent. Malgré les réticences d'une partie de l'opinion, ce nouveau procédé devrait être généralisé de façon à éviter la falsification et l'usurpation d'identité.

L'Allemagne a introduit le passeport biométrique sécurisé (ePass) sur lequel est fixé un composant à lecture sans contact (RFDI-Chip) qui permet de comparer la photo d'identité du titulaire et de lire ses données personnelles. En mars prochain, ce composant enregistrera deux empreintes digitales. La Belgique dispose aussi du ePass et la Suède se prépare à le délivrer. En France, les ePass sont en cours de distribution.

La situation aux USA

La notion de zone de sécurité pour les données personnelles ("safe harbour") mise en avant par l'administration Clinton ainsi que la possibilité donnée au consommateur de choisir entre donner accès à ses données personnelles ou les garder confidentielles ("opt in opt out") de Ralph Nader ont été balayées par l'administration Bush au nom de la doctrine libérale tendant à ne pas entraver le libre exercice de la concurrence. Elle a décidé de ne pas pénaliser les compagnies américaines avec des systèmes de contrôle des données personnelles utilisées qui alourdiraient les coûts de gestion et par conséquent diminueraient la compétitivité de ces entreprises.

Des expériences concluantes de paiement biométrique ont actuellement cours aux USA. Il suffit aux individus enregistrés de se présenter aux caisses avec leur index ou la reconnaissance de leur iris pour procéder à toutes les transactions financières souhaitées. Données personnelles et bancaires sont reliées.

Dans le cadre du " Patriot Act ", l'ampleur du profilage personnalisé réalisé par les services de police américain peut être imaginé à partir des nombreuses données personnelles qui sont recueillies sur tous les passagers en partance pour les USA sans qu'ils puissent y avoir accès.

Ceci est l'occasion de faire le point sur les dangers que recèle le système Passport de Microsoft par exemple (contre lequel le projet Liberty Alliance avait été conçu), qui prétend avoir rassemblé des données personnelles sur 150 millions d'usagers de son service Web hotmail.com ou l'entreprise de ventes de livres en ligne, Amazon.com, capable de proposer des produits musicaux à ses clients acheteurs de livres, à partir de profilages permettant d'identifier des goûts communs entre même type de consommateurs. Ces deux approches peuvent devenir complémentaires et permettre la mise en place de doubles numériques très détaillés sans que les consommateurs en soient informés ou aient un droit de regard, avec la possibilité de centraliser les doubles numériques avec une clé unique sous forme d'un identifiant personnel ignoré de l'usager.

L'évolution plausible des bases de données personnelles maintenues par les pouvoirs publics et par les offreurs de biens et de services privés, est de les rendre interconnectables en utilisant l'identifiant personnel unique, permettant d'obtenir un double numérique regroupant l'ensemble des données personnelles concernant un individu donné, même si elles sont physiquement dispersées.

Que faire ?
Se pose donc la question de l'attitude à adopter face à de telles évolutions.

Trois scénarios possibles :

1 - maintenir la parcellisation des données
Le premier est la continuation de l'état de fait actuel où services publics et privés élaborent les doubles numériques de leurs

administrés et clients sans chercher à les réunifier autour d'un identifiant personnel unique. Les services concernés prennent sur eux de respecter chacun de leur côté la loi concernant la protection des données personnelles quand elle est appliquée comme c'est le cas en France avec le risque de pouvoir s'en dispenser depuis d'autres pays. Leur prolifération accroît les risques d'erreur et force à développer des procédures d'authentification pour chaque double numérique. Il n'autorise aucun contrôle de la personne sur les données qui sont détenues à son sujet par les diverses instances, publiques ou économiques qui les détiennent. Ce scénario semble le plus défendu actuellement par les consommateurs (ex CREIS)(3).

2 - donner le contrôle à l'individu
Le deuxième scénario consiste au contraire à faciliter l'interconnexion de toutes les traces laissées par la personne sur les réseaux et à permettre de créer des données personnelles, grâce à l'usage généralisé et encadré d'un identifiant personnel unique, lui-même utilisé pour les repérages de biométrie individuelle. Ceci permettrait de prévenir la multiplication des doubles numériques de la personne à son insu sans qu'elle puisse y avoir un droit de regard. Ceci impliquerait que les identifiants actuels soient connectés entre eux afin de les relier à l'identifiant unique personnel (4). Ceci est considéré comme source de tous les dangers pour les tenants de la liberté individuelle mais aussi , comme le meilleur moyen de contrôler tous les doubles numériques qui foisonnent. Le corollaire de cette mis en oeuvre concerne la mise à disposition du citoyen de procédures lui permettant à partir de son identifiant unique personnel, d'avoir accès à tous ses doubles numériques.

Mais cette approche adresse une partie seulement de l'enjeu de la protection des données personnelles du fait qu'elle laisse le dernier mot aux usagers : ceux-ci ont tendance à faire confiance aux services non seulement publics mais aussi privés et risquent de communiquer leurs identifiants sans coup férir en échange d'une promesse d'amélioration des produits et prestations offerts.

3 - Impliquer la société civile
Le troisième scénario est une hypothèse de travail qui consiste à impliquer la société civile en tant que représentante des usagers et de la rendre partie prenante d'instances conjointes régulant la création de l'identifiant personnel unique, sa généralisation systématique, son accès et d'une manière générale les usages du double numérique. S'il ne paraît pas souhaitable de laisser sous la seule responsabilité des pouvoirs publics la procédure de centralisation des doubles numériques par l'intermédiaire de la promotion de l'usage de l'identifiant unique personnel et encore moins qu'il soit révélé sans contrôle au secteur privé, les garanties correspondantes sont à mettre en œuvre par des institutions tierces, capables à la fois d'assurer l'inviolabilité de l'identifiant unique et de donner accès à chaque citoyen à toutes les informations personnelles le concernant.

La poursuite de tels objectifs implique des efforts tant au niveau de la législation, de la validation normalisée des outils de protection des données personnelles et de la mise en place des procédures adéquates dans les institutions publiques et privées utilisant ce type de données. Ceci suppose la montée en puissance de corps intermédiaires tripartites contrôlés à la fois par les représentants des pouvoirs publics, de la société civile et des acteurs privés, chargés de réguler le recueil des données personnelles et de vérifier à quels types d'usages elles peuvent être affectées.

Pistes de revendications :

* Vu la quantité considérable d'informations recueillies sur les échanges interpersonnels par les réseaux et exploitées par les consortiums financiers et industriels aussi bien que les pouvoirs publics, le meilleur pare-feu à envisager serait de déclarer bien privé, propriété de la personne, tout ce qui a été recueilli sur elle sous formes de données personnelles. De cette manière, celle-ci pourrait décider de rendre publiques ces informations la concernant avec un accès restreint et dans un contexte précis. Même si leur recueil coûte beaucoup d'argent, la mise à disposition gratuite de la personne des données personnelles la concernant est indispensable pour lui permettre de s'assurer de leur validité et de contrôler leurs usages.

* Une manière de réguler l'accumulation des données personnelles est de veiller à leur effacement périodique. C'est aussi le moyen donné à la personne de garder le contrôle sur des données qui lui appartiennent afin de les faire disparaître, même si elle accepte de les divulguer pour une période donnée. Pour ce faire, elle a besoin d'institutions tierces pour l'assister dans ses démarches et d'une manière générale la représenter et protéger ses intérêts. Les garanties concernent la défense de la personne qui se verrait indûment accusée de démarches répréhensibles dans le cas d'identité usurpée, ce qui suppose non seulement d'avoir accès aux données de son double numérique mais aussi d'avoir un pouvoir de recours.

Pour contrecarrer l'effet repéré par Marcuse qui critiquait l'homme unidimensionnel, réduit à des modèles de comportement parcellaires et fragmentés, des institutions tierces, interfaces s'interposant entre les individus et les systèmes de suivi informatique, pourraient les aider à mieux contrôler les usages de leurs données personnelles d'un point de vue à la fois de la personne concernée tout comme du demandeur de données personnelles. Le correspondant de la CNIL dans l'entreprise ou l'institution publique (" correspondant informatique et liberté " : CIL), chargé de surveiller les fichiers traitant de données personnelles, en tant que tiers de confiance, est un premier pas dans la bonne direction.

Premiers travaux vers cette direction :

La protection des données personnelles a été étudiée par un groupe de travail du Comité Européen de Normalisation, qui a produit le rapport Initiative pour la normalisation de la protection des données personnelles en Europe (" Initiative on Privacy Standardization in Europe " : IPSE). Ce rapport a débouché sur la création d'un atelier sur la protection des données personnelles (" Data Protection and Privacy Workshop ") qui fait des propositions concernant la normalisation des technologies de protection des données personnelles.

Il s'agit d'une part de protéger l'identifiant personnel unique pour le rendre si possible inviolable ou en tout cas travailler dans ce sens afin d'éviter les falsifications et les captations d'identité. D'autre part, il s'agit de faciliter l'accès individuel à toutes ses données personnelles où qu'elles se trouvent. Ces deux démarches ne sont pas triviales et nécessitent des développements informatiques pour répondre à cette double exigence. Enfin, l'utilisation de pseudos à la place des identifiants personnels uniques comme mesure de protection est à rendre possible par un accord réciproque entre les demandeurs de données personnelles, les individus concernés et le tiers de confiance, jouant le rôle d'infomédiaire entre les deux parties.

Bibliographie :

Belleil A., E-privacy. Le marché des données personnelles : protection de la vie privée à l'age d'Internet. Liaisons (Droit vivant), Paris : 2001

Marcuse H., L'homme unidimensionnel. Essai sur l'idéologie de la société industrielle avancée, Paris, Les éditions de Minuit, 1969
Perriault J., Arnaud M., Juanals B., Les identifiants numériques humains, éléments pour un débat public, Les cahiers du numérique, vol 3, no2-2002, p.169-182

Truche P., Faugère J.-P. et Flichy P., Administration électronique et protection des données personnelles, Rapport au ministre de la Fonction publique et de la Réforme de l'État, Paris, La documentation française, 2002.

Sur la biométrie :

(Ashbourn, 1999) J. Ashbourn, A biometric white paper.
http://www.avanti.1to1.org/whitepaper.html

(Ashcroft et al., 2004) John Ashcroft, Deborah J. Daniels, Sarah V. Hart. DNA forensics Research and Development, U.S. Department of Justice, Office of Justice Programs, Nov. 2004

(Bailly-Bailliére et al., 2003) E. Bailly-Bailliére, S. Bengio, F. Bimbot, M. Hamouz, Jo. Kittler, J. Mariéthoz, J. Matas, K. Messer, V. Popovici, F. Porée, B. Ruíz, and J.-P. Thiran. The BANCA Database and Evaluation Protocol. Audio- and Video-Based Biometric Person Authentication

(AVBPA), Guilford, 2003.

(Beslay & Punie, 2002) Beslay L. & Punie Y. 'The virtual residence: Identity, privacy and security', The IPTS Report, Special Issue on Identity and Privacy, No. 67, September 2002, 17-23.

(Betsch, 2004) David F. Betsch, DNA Fingerprinting in Human Health and Society Biotechnology Training Programs, Inc. Edited by Glenda D. Webber, Iowa State University Office of Biotechnology, 2004

(Bowyer, 2003) K. W. Bowyer, Face Recognition and the Security versus Privacy Tradeoff.
http://www.cse.nd.edu/~kwb/nsf-ufe/SecurityPrivacy.pdf, August 2003.

(Bromba, 2004) Dr. Manfred Bromba, Biometrics FAQ, last change November 2004
http://www.bromba.com/faq/biofaqe.htm

(Brown et al., 2002) C. C. Brown, X. Zhang, R.M. Mersereau & M. Clements Automatic Speech Reading with Application to Speaker Verification. ICASSP International Conference on Acoustics, Speech and Signal Processing (ICASSP) 2002

(Burgess, 2004) Richard Burgess. Defence challenges accuracy of DNA. Oct. 6, 2004.
http://www.acadiananow.com/searchforakiller/html/5922BC48-F441-4EA3-929A-5685BD070A51.shtml

(Butler, 2004) Dr. John M. Butler. Technology Developments in Forensic DNA Typing and Prospects for Non-Forensic. Use of DNA Identification. NIST Biotechnology Division May 12, 2004

(Daugman, 1993) John Daugman, High confidence visual recognition of persons by a test of statistical independence, IEEE Trans, Pattern Analysis and Machine Intelligence, Vol. 1, No. 11, 1993, pp 1148-1161.

(Daugman, 1994) John Daugman, Univ. Cambridge, protected by U.S. Patent No. 5291560 issued March, 1, 1994
Biometrics at the Frontiers: Assessing the impact on Society

EC-DG JRC-IPTS Page 160 of 166

(Daugman, 2003) John Daugman, How Iris Recognition works, Univ. Cambridge, 2003. http://www.cl.cam.ac.uk/users/jgd1000/

(Daugman, 2004) John Daugman, Univ. Cambridge, BIOSEC conference. Barcelona, June 2004.

(DTFC, 1992) DNA Technology in Forensic Science, Committee on DNA Technology in Forensic Science, Board on Biology, Commission on Life Sciences, National Research Council, NATIONAL ACADEMY PRESS, Washington, D.C., 1992

(Ducatel et al., 2000) Ducatel, K., Bogdanowicz, M., Scapolo, F., Leijten, J. & Burgelman, J-C. (eds.) (2000) Scenarios for Ambient Intelligence in 2010, IPTS-ISTAG, EC: Luxembourg. http://www.cordis.lu/ist/istag

1 Huit catégories génériques de traitements, considérés comme générateurs de risques pour les droits et libertés, sont désormais soumis à l'autorisation préalable de la CNIL du fait de la nature des données concernées et de leur finalité (segmentation de la clientèle, profilage, évaluation, lutte contre la fraude et listes noires, cybersurveillance des salariés, biométrie, géolocalisation

2 La loi d'orientation et de programmation sur la sécurité intérieure, adoptée le 31 juillet 2002 en France contient ainsi un volet relatif aux communications téléphoniques, à Internet et aux bases de données. Elle est revotée en ce moment avec des conditions de surveillance accrue

3 Le CREIS se bat contre le programme INES tout comme le projet de directive européenne sur la rétention des données personnelles

4 Dans le cas où l'identifiant personnel unique se généralise pour toutes les bases de données personnelles, l'idée d'un contrôle du citoyen sur ses données personnelles et la manière de les utiliser pourrait se concrétiser sous forme de clés logicielles d'accès à son coffre fort électronique où elles seraient entreposées et d'où il pourrait les extraire pour les communiquer à qui serait habilité par lui pour les lire (rapport Truche, 2002). Il ne s'agit pas de stocker toutes les données personnelles dans ce coffre fort virtuel mais les clés d'accès à l'identifiant personnel unique et aux autres identifiants utilisés et qui lui sont reliés, qui constituent le sésame ouvrant tous les fichiers contenant des données personnelles dispersées dans des banques de données diverses. Si les pouvoirs publics peuvent avoir un double de ces clés à des fins de contrôle policier et juridique, le citoyen pourrait mettre à jour lui-même ses données identitaires immédiatement reprises dans l'ensemble des identifiants à partir de l'identifiant personnel unique, en application du droit d'accès et de rectification prévu par la loi informatique et libertés. L'usage des logiciels libres pour la gestion de ce coffre fort électronique permettrait de réduire les possibilités d'immixtion intempestive rendues invisibles si des logiciels propriétaires étaient utilisés.