

RÉSUMÉS – *Abstracts*

Jacques PERRIAULT, *Traces numériques personnelles, incertitude et lien social*

Cet article explore une problématique de l'identité personnelle alternative à celle du contrôle policier pour étudier les traces numériques que créent ou laissent les usagers sur Internet et sur les dispositifs informatiques en général. Cette problématique embrasse toutes les traces, numériques et non numériques. Le constat de départ est celui d'une évolution récente de la présentation de soi dans l'espace public qui expose désormais des données jadis réservées à l'intimité. L'hypothèse conséquente est qu'existe un lien entre l'affichage d'une identité plus détaillée et la conscience de vivre dans une société incertaine. Dans cette perspective, les motivations qui président à cet affichage sont la recherche de l'estime de soi et de la considération par autrui, deux composantes du lien social, ébranlées dans les sociétés incertaines. Une attention particulière est également accordée, dans ce climat d'incertitude, à la géolocalisation qui contribue au travers de divers appareils à situer en temps réel et constamment les individus les uns par rapport aux autres

Mots-clés : problématique de l'identité, traces numériques, présentation de soi, société incertaine, estime de soi, considération, lien social, géolocalisation.

Uncertainty, Social Cohesion and the Tracking of Personal Data

This paper explores an approach to personal identity issues that offers an alternative to police surveillance for investigating digital traces created or left behind by people who use the Internet and information technology in general. The approach covers all traces, whether digital or not. The paper posits a recent trend in which personal identities are presented in a public sphere that has begun to exhibit information of a type that was formerly divulged only in intimate circles. The ensuing hypothesis is that there is a link between the public display of more detailed personal identities and people's awareness of living in a society of uncertainty. If this is indeed the case, then the reason underlying the display of one's private identity in public is a quest for self-esteem and for the esteem of others – both being integral to the social cohesion now being undermined by uncertainty in society. In this context of uncertainty, particular attention is given to geolocation, which, through various technical systems, enables individuals to locate each other in real time, and at any time.

Keywords: *identity issues, digital traces, display of the self, uncertain society, self-esteem, esteem of others, social cohesion, geolocation.*

Louise MERZEAU, *Du signe à la trace : l'information sur mesure*

L'environnement numérique oblige à revoir les modèles sur lesquels se fondent les sciences de l'information et de la communication. La pensée du signe, du message et du document doit en effet évoluer vers une pensée de la traçabilité. Indicielle et détachable, automatique et malléable, la trace est un objet paradoxal, qui atteste le caractère indissociablement technique et politique de la présence numérique.

Dans le règne de l'information sur mesure, la personnalisation nous rend plus actifs, tout en nous exposant au profilage. Elle va jusqu'à redéfinir l'identité comme une collection de traces que nous devons apprendre à protéger, mais aussi à administrer.

Cette nouvelle économie des empreintes enchevêtre les hiérarchies entre stock et flux comme entre contenu et relation. Recyclant nous-mêmes les traces que d'autres ont déposées, c'est désormais dans l'ombre numérique de la cité que nous sommes appelés à naviguer. Au-delà de la défense de la vie privée, il en va donc aussi de la mémoire et de l'oubli qui nous relie.

Mots-clés : *trace, réseau, Internet, Web 2, identité numérique, théorie de l'information et de la communication, technique, politique, mémoire.*

From Signs to Traces - Reflections on Customized Information

The digital environment is forcing us to re-think the models on which media studies and information science are based. Theories of signs, messages and documents need to evolve towards reflections on traceability.

Traces are paradoxical objects: linked to the personal yet detachable, automatic yet malleable, they bear witness to the inextricable links between the technical and the political in the digital sphere.

In an age of "customized information", personalization makes people more active, and also exposes them to profiling, to the point where identity is being redefined as a collection of traces which we must learn to protect, and also to manage.

This new economy based on digital "footprints" is overturning the hierarchical relationships between stock and flow, and between content and interaction. As we ourselves recycle the traces that others have left, we are having to find our way through the shadowlands of digital citizenship. Over and above privacy protection, what is at issue are the memories, but also the forgetting, that bind us to each other.

Keywords: *trace, network, Internet, Web 2, digital identity, Information and Communication Theory, techniques, politics, memory.*

Olivier ERTZSCHEID, *L'homme, un document comme les autres*

Les réseaux sociaux posent aujourd'hui, au sens propre, la question documentaire appliquée au facteur humain. La gestion des identités numériques laisse entrevoir la constitution d'un pan-catalogue des individualités humaines, ouvert à l'indexation par les moteurs de recherche, et pose ainsi la question de la pertinence des profils humains. Ceux qui aujourd'hui indexent indistinctement des informations de nature publique, privée ou intime ont une connaissance très fine de « ce que dit de nous » la somme des documents dont nous sommes entièrement ou partiellement responsables. Il devient nécessaire de questionner le processus qui après avoir ouvert l'indexation à la marchandisation, après l'avoir parée de vertus « sociales », place aujourd'hui l'homme au centre même du cycle documentaire, non plus comme sujet acteur, mais comme un objet documentaire parmi d'autres. La question qui se pose est donc clairement celle du caractère indexable de l'être humain. Celle de savoir si l'homme est, ou non, un document comme les autres.

Mots-clés : documentation, identité numérique, indexation, réseaux sociaux, moteurs de recherche.

Human Beings as Documents

Social networking sites (SNS) offer possibilities for cataloguing human beings as if we were documents. The management of digitized identities is pointing towards the creation of a global catalogue of human individuality that can be trawled and indexed by search engines, raising the problem of the relevance of human profiling. These social networking sites and search engines index data regardless of whether it is public, private or intimate, and they contain minutely detailed information on "what is said about us" in a mass of documents for which we are wholly or partly responsible. It is becoming imperative to question the process that, having opened up indexes to commercial use and attributed a gloss of social virtue to the fact of doing so, has placed human beings at the core of the documentation cycle, not any longer as an active subject but as documentary objects amongst others. The question, clearly, is how far human beings can be indexed: in other words, whether a human being is merely a document like any other.

Keywords: *documentation, digital identity, indexing, search engines, social networking sites.*

Frank BEAU et Oriane DESEILLIGNY, *Une figure du double numérique : l'avatar*

Qu'ils soient en ligne ou hors ligne, les mondes virtuels cristallisent nombre d'espoirs, de craintes, de fantasmes liés à l'innovation technologique, à la gestion et aux formes de l'identité contemporaine, et à l'évolution des médias de communication. Les emplois désordonnés de la notion d'avatar et les projections associées témoignent des paradoxes à l'œuvre dès lors que l'on tente de comprendre des pratiques et des technologies nouvelles.

Mais l'avatar ne représentant qu'une partie du mode opératoire d'une personne dans un monde virtuel, il conviendra, dans une approche systémique, de préciser l'étendue de la présence du sujet dans ces mondes pour mieux informer la notion de données personnelles dans ce contexte spécifique. Comment ces identités et données virtuelles sont-elles gérées, traitées, appréhendées individuellement et collectivement, tant par les internautes que par les acteurs techniques et industriels ?

Mots-clés : avatar, identité, média, communication, représentations, jeux vidéos, jeux de rôle en ligne, simulateurs de vie.

The Avatar as a Digital Double

Virtual worlds, whether multiplayer online games or three-dimensional virtual worlds like Second Life, crystallize a multitude of hopes, fears and fantasies that are linked with technological innovation, with contemporary forms of identity and their management, and with developments in communication media. Today's unregulated uses of the avatar concept and associated projections reveal the paradoxes that arise when we attempt to understand new practices and technologies.

However, the avatar only partially represents the way people function in a digital world, and any systemic study therefore needs to specify the extent of the subject's presence in a virtual world, in order to give a clearer idea of what is personal data in this specific context. How are these virtual identities and items of information managed, treated and individually and collectively apprehended, by Web surfers themselves and by the technical and industrial spheres concerned?

Keywords: avatar, identity, media, communication, video games, large-scale online multiplayer games, Second Life.

Emmanuel KESSOUS et Bénédicte REY, *Économie numérique et vie privée*

L'usage du monde numérique, et plus particulièrement de l'Internet, crée des traces qui constituent la source de services que les utilisateurs contribuent à personnaliser eux-mêmes. En échangeant leurs favoris, leurs photos, leurs informations de toutes sortes, les utilisateurs révèlent leurs préférences et renforcent l'utilité du service qu'ils sont en train d'utiliser. Une

première génération de services s'appuie sur les mécanismes d'une rationalité exploratoire, tirant bénéfice du savoir collectif (modèle de suggestions d'Amazon). Une seconde génération de services va plus loin en utilisant les préférences déclarées pour connecter des individus « qui se ressemblent » (modèle des plateformes de réseaux sociaux). Ces évolutions suggèrent le passage d'une économie de stock à une économie de flux où le bien rare est moins l'information que l'attention nécessaire pour la traiter. Elles ont des conséquences sur la gestion de l'identité numérique des individus et rend de moins opérant la notion juridique de la *privacy*.

Mots-clés : vie privée, traces, réputation, économie de l'attention, identité numérique, plateforme de réseaux sociaux, Web 2.

Privacy and the Digital Economy

Using the digital world, and especially the Internet, generates traces that become the basis for services which are customised by the contributions of users themselves. As they share their favourites, photos and information of all kinds, users not only disclose their preferences but also strengthen the utility of the service they are using. Some first-generation services rely on mechanisms based on exploratory rationality and drawing on collective knowledge (such as Amazon's recommendations engine). A second type of service goes a step further by using displayed preferences to connect people who are "alike" (social networking model). These trends suggest a switch from a stock-based economy to a flow-based economy, where the most valuable asset is not information as such but the attention it attracts. These developments are creating issues relating to the management of individual digital identities, and bringing the relevance of the legal notion of privacy into question.

Keywords: *privacy, traces, reputation, attention economy, digital identity, social networking websites, Web 2.*

Caroline LANCELOT MILTGEN, Enquête auprès des internautes : entre croire, dire et faire

La collecte et l'utilisation efficace des données clients constituent un enjeu stratégique et éthique majeur pour les entreprises. Depuis les années 1990, l'arrivée des NTIC est venue bouleverser la manière avec laquelle ces données sont collectées, stockées puis utilisées. Ces pratiques ne s'opèrent pas sans que les consommateurs y trouvent à redire, considérant souvent celles-ci comme une intrusion dans leur vie privée. Ce phénomène est prégnant sur Internet qui présente un environnement dans lequel les menaces sur la vie privée sont renforcées. De plus en plus d'internautes ont dès lors pris des mesures pour se protéger, y compris des restrictions sur leurs échanges d'informations et leurs achats en ligne. Ce constat

invite à mieux comprendre les réactions des consommateurs face à la collecte de leurs données personnelles sur Internet. Les résultats de nos enquêtes montrent un écart entre les protections offertes par le droit et les perceptions des consommateurs à ce sujet. Ils confirment aussi un écart entre les intentions déclarées et les comportements réels. Des recommandations visant à inciter les acteurs à adopter des pratiques éthiques dans ce domaine sont présentées.

Mots-clés : respect de la vie privée, données personnelles, Internet, réglementation, éthique.

A Web Surfer Survey - What we Believe, What we Say and What we Do

The collection and efficient use of customer data is a major strategic and ethical issue for companies. Since the 1990s, ICTs have brought radical changes in the way these data are collected, stored and used. Most consumers see these practices as an intrusion into their private life. The phenomenon pervades the Internet, an environment where threats to privacy are increasing. More and more Web surfers have consequently taken measures to protect their privacy, for example by restricting exchanges of information and online purchases. This observation has prompted a survey aiming to gain a better understanding of consumer reactions to the collection of their personal data on the Web. The results of our investigations show that the legal privacy protection does not match consumer perceptions in this regard. They also confirm a difference between declared intentions and actual consumer behaviour. The concluding recommendations are designed to promote ethical data use among companies.

Keywords: *privacy, personal data, Internet, legal privacy protection, ethics.*

Dominique CARDON, *L'identité comme stratégie relationnelle*

La réussite des plateformes relationnelles du Web 2.0 doit beaucoup au fait que les personnes prennent des risques avec leur identité en rendant publiques des informations sur elles-mêmes. Aussi, est-il nécessaire de comprendre les ressorts sociaux, culturels et psychologiques de ce phénomène. Car l'exposition de soi ne signifie pas un renoncement au contrôle de son image. Elle témoigne, au contraire, d'une volonté que l'on pourrait presque dire stratégique de gérer et d'agir sur les autres en affichant et en masquant certains traits de son identité. C'est ce paradoxe qui se trouve au cœur des débats sur la *privacy* dans le Web 2.0 et dont cet article cherche à éclairer quelques aspects à travers la lecture de travaux de recherche récents.

Mots-clés : identité numérique, vie privée, réseaux sociaux de l'Internet, Web 2.0.

Identity as a Relational Strategy

The success of Web 2.0 relational platforms owes a lot to people who take risks with their personal identities by making information about themselves public. There is therefore a need to understand the social, cultural and psychological mainsprings of this phenomenon. The exhibition of the self on the Internet does not mean that people are losing control over their image. Rather, it reflects a strategic attempt to manage and influence others. This paradox lies at the heart of Web 2.0 privacy debates, which this paper seeks to shed light on through a reading of recent research work.

Keywords: *digital identity, privacy, social networking sites, Internet, Web 2.0.*

Pierre PIAZZA, L'extension des fichiers de sécurité publique

La mobilisation par les pouvoirs publics de fichiers contenant des informations à caractère personnel à des fins de sécurité s'ancre dans une histoire longue. Ces dernières décennies, on constate pourtant une évolution significative de ces fichiers du fait de l'extension de leur nombre, de leur ampleur et de leur champ d'application. Cet article s'intéresse à ce phénomène en analysant certains problèmes dont il est à l'origine. Tout d'abord, les dysfonctionnements que l'exploitation de ces fichiers occasionne. Ensuite, l'accroissement des pouvoirs de police résultant de la transformation de la finalité de certains de ces fichiers. Enfin, le caractère insatisfaisant de la protection des individus face à l'utilisation qui est faite de leurs données personnelles.

Mots-clés : fichiers, sécurité, police, biométrie, protection de la vie privée et des libertés individuelles.

The Growth of Police Records

Public authorities have used records containing personal information for security reasons for a long time. However, there have been significant developments in recent decades, with records increasing in number, including more data and covering a broader scope. This paper analyses some of the problems caused by this process of expansion. Firstly, we review the administrative dysfunctions that the exploitation of such records may cause. Secondly, we look into the increase in police powers that result from changes in the aims pursued by some filing systems. Finally, we examine the issue of inadequate protection of individual privacy and liberties against the misuse of personal data.

Keywords: *data files, security, police, records, biometrics, protection of privacy and individual liberties.*

François-Bernard HUYGHE, *Téléphonie mobile : capter la vie numérique des autres*

Dans un contexte où les technologies numériques favorisent la traçabilité des échanges et tandis que se répand l'appréhension d'une surveillance globale, le citoyen pourrait craindre que ses télécommunications soient bien davantage écoutées ou écoutables par l'État *Big Brother* qu'à l'époque des « bretelles » sur téléphones filaires.

Or, sans même parler des progrès des protections légales, ce scénario cauchemar « panacoustique » se heurte à la complexité des protocoles et vecteurs de communication, comme aux stratégies d'anonymisation ou de furtivité contre les écoutes légales.

En revanche, des acteurs privés, souvent criminels, exploitent les failles sécuritaires notamment des téléphones mobiles des nouvelles générations ; truands ou officines peuvent souvent savoir ce que le juge d'instruction ne pourra découvrir, tandis que le matériel d'espionnage privé se banalise. Ce phénomène pose des questions politiques concernant la souveraineté et le contrôle des moyens de violer les secrets.

Mots-clés : surveillance, écoutes, interception, téléphone, mobile, technologie, Big Brother, libertés publiques, télécommunications, vie privée, privatisation, GSM, Internet.

Mobile Phones - Capturing the Digital Existence of Others

In a context where digital technologies are making it easier to keep track of various types of communication, with attendant fears of globally expanding surveillance, citizens may well suspect that their telecommunications are, or are capable of, being monitored to a much greater extent by the Big Brother State than in the days when surveillance was limited to wiretaps on landlines.

However, this nightmare “global phone-tapping” scenario has to contend not only with advances in legal protection but also with the complexities of communication protocols and vectors and with the various counter-measures that have developed to secure anonymity against legal eavesdropping.

However, private groups, often with criminal intent, are becoming adept at exploiting security loopholes, especially in late-generation mobile phone systems. Criminals and shady commercial establishments can often find information that no magistrate would have access to, while private surveillance equipment is becoming available practically over-the-counter. All these developments raise political issues of sovereignty and control over means of violating privacy.

Keywords: *surveillance, wiretapping, eavesdropping, mobile phones, technology, Big Brother, privacy, public liberties, privatization, telecommunications, GSM, Internet.*

Hubert BOUCHET, *La surveillance numérique au travail*

Avec le salariat et le rassemblement des ouvriers sur les mêmes lieux, dans le même temps et pour une tâche commune, la surveillance est apparue comme plus « nécessaire ». Les techniques se sont naturellement installées dans l'univers de la surveillance au travail, marquant plusieurs étapes. Autrefois, vigiles, contremaîtres et cadres assuraient la surveillance. Une seconde étape a été matérialisée par l'installation des automatismes de première génération, avec les badges notamment. La troisième étape a enrichi les dispositifs du recours à la vidéo, avec la capture des images et des sons. Plus récemment, la cyber-surveillance a pris place, avant que les techniques biométriques n'apparaissent. Le caractère de plus en plus intrusif des moyens de la surveillance apparaît avec leur possible mise en œuvre à l'insu des « surveillés ».

Dans cet univers, la Cnil doit s'assurer du respect de l'esprit et des termes de la loi Informatique et Libertés. Mais chacun doit être appelé à la vigilance et veiller personnellement au bon usage des traces qu'il laisse et qui peuvent aller sommeiller dans un fichier jusqu'au jour où... !

Mots-clés : caméras, identité numérique, surveillance, métamorphose du travail, vie privée.

Digital Supervision in the Workplace

With salaried employment and the presence of an entire workforce in the same premises and at the same time, supervision is considered as increasingly "necessary". Technology has naturally become established in the world of workplace supervision, developing through different stages. In the past, the task was entrusted to security guards, foremen and supervisors. Next came first-generation automation, particularly with the introduction of badges. The third phase brought in video recordings, with image and sound capture. More recently, cyber-supervision was frequently used before being superseded by biometric techniques. With today's possibilities for installing work supervision systems without the knowledge of those being supervised, they have become increasingly prevalent.

The French data protection authority (CNIL) is responsible for enforcing observance of the terms and the spirit of the French data protection act (LIL). However, it is up to each one of us to be vigilant and to make sure, individually, that the digital traces we leave behind us are properly used and are not waiting patiently in some obscure archive for the day when ...

Keywords: video cameras, digital identity, supervision, transformation of work, private life.

Alain BAUER et Christophe SOULLEZ, *La concession de vidéosurveillance*

Depuis plus de vingt ans, le développement de la vidéoprotection fait l'objet de nombreux débats, parfois passionnés, tant en ce qui concerne son utilité en vue de lutter

contre la délinquance que pour ses éventuelles conséquences en matière d'atteintes aux libertés individuelles. En France, l'installation de systèmes de vidéoprotection sur la voie publique est encadrée par les dispositions de la loi du 21 janvier 1995. La vidéoprotection n'est qu'un outil parmi d'autres au service de la prévention et de la lutte contre la criminalité. Elle peut être efficace lorsque sa mise en œuvre répond à des objectifs clairement définis. En revanche, certains problèmes demeurent lorsqu'elle est mal utilisée. L'usage des nouvelles technologies par l'État ne doit pas être systématiquement abordé sous l'angle symbolique ou du militantisme. La problématique n'est pas dans leur essor, car il est incontestable que les progrès technologiques contribuent à une meilleure sécurité des citoyens, tant à charge pour les criminels, qu'à décharge pour les personnes injustement poursuivies, mais dans les moyens et les procédures de contrôle de ces outils. Là est l'enjeu.

Mots-clés : vidéosurveillance, vidéoprotection, contrôle, libertés, criminalité, technologies.

Video-monitoring Concessions

The development of video-monitoring has been a subject of considerable and often heated debate for over twenty years, both as regards its effectiveness against crime and its potential for infringing civil liberties. In France, the installation of video-monitoring systems in public places is regulated by the Act of January 21st, 1995. Video-monitoring is one of a range of tools used in preventing and fighting crime. When implemented with clearly defined objectives, it can be effective. However, the misuse of video-monitoring raises a number of problems. The use of new technologies by the State should not be systematically viewed in symbolic terms or from the angle of political activism. The problem at issue is not the boom in video-monitoring in itself, as it cannot be denied that technological progress is contributing to better security for citizens, both against criminals and in the defence of persons unjustly charged, but rather the means and procedures for controlling its use.

Keywords: video-monitoring, video-protection, control, civil liberties, crime, technology.

Claire LEVALLOIS-BARTH, *La géolocalisation : un nouvel impératif*

L'offre de services de géolocalisation via un téléphone mobile implique de connaître la localisation et l'identifiant du téléphone, donc de collecter des données relatives à un utilisateur identifié ou identifiable. À ce titre, la loi Informatique et Libertés exige que l'utilisateur consente en toute transparence à bénéficier d'un service géolocalisant et que ses données de localisation soient détruites ou anonymisées une fois la prestation fournie. Si, dans certains cas, l'utilisateur aspire à être localisé, dans d'autres cas, la personne concernée ignore que sa position géographique est connue de tiers. Cette traçabilité subie laisse entrevoir de redoutables perspectives de contrôle ou d'abus tant de la part des services répressifs que des

entreprises. L'enjeu ne porte pas uniquement sur les risques d'atteinte à la liberté d'aller et venir, et au respect de la vie privée. De façon plus pernicieuse, l'autonomie informationnelle et décisionnelle du citoyen peut être remise en cause.

Mots-clés : géolocalisation, loi Informatique et Libertés, vie privée, télécommunications, Cnil.

Emerging Issues in Location Based Services

Location Based Services (LBS) are information services that can be accessed with mobile phones. They rely on the system's knowledge of the geographical position and the identifier of the phone being used, and therefore on collecting data on an identified or identifiable user. In this respect, the French data protection act stipulates that users agree to be supplied with an LBS service on a fully transparent basis and that their location data must be erased or made anonymous once the service has been provided. In some cases, location-based services are provided on the user's own request, but in other cases, the individual concerned is unaware of the fact that third parties know where s/he is. This creates potential for surveillance and misuse on the part of both police and businesses. What is at stake here is not only the right of individuals to freedom of movement and to privacy but also, and more perniciously, citizens' autonomy with regard to information and decision-making.

Keywords: geolocation, personal data, privacy, telecommunications.

Michel ARNAUD, *Le WHOIS, talon d'Achille de la protection des données personnelles*

Ce texte entend montrer les enjeux en termes de protection des données personnelles de l'accès au service WHOIS. Avec la création massive de nouveaux noms de domaines rendue possible par la migration des serveurs racines vers IPv6, la question de l'accès au WHOIS devient critique. Une régulation tendant à mieux assurer la protection des données personnelles est à envisager dans un autre contexte, l'Icann ne souhaitant pas la mettre en place. Mieux vaut se replier sur les noms de domaines contrôlés par les organismes respectant les directives européennes, à l'image de ce que pratique l'Afnic, assurant la protection des données personnelles des propriétaires des noms de domaine tout en permettant d'y avoir accès dans des conditions bien spécifiées.

Mots-clés : WHOIS, IPv6, Icann, Afnic, nom de domaine, adresse IP, log, protection des données personnelles.

WHOIS, the Achilles'Heel of Data Protection

This paper aims to show what is at stake in terms of data protection with access to the WHOIS service. With the exponential growth of TLDs offered by the migration of root servers

to IPv6, access to WHOIS has become a critical issue. A regulation to ensure better protection of personal data needs to be envisaged in a different context, since ICANN does not wish to implement it. A better option would be to use TLDs under the control of organisations that abide by EU rules, as AFNIC is doing by protecting the personal data of domain name owners while allowing access to them under specified conditions.

Keywords: WHOIS, IPv6, ICANN, AFNIC, domain name, IP address, log, privacy protection.

Karine DOUPLITZKY, *Le commerce du moi, modèle économique du profilage*

On n'a pas attendu le Net pour établir un commerce profitable des données personnelles. Depuis la vente par correspondance aux cartes de fidélité, des milliers de fichiers sont venus grossir les bases de données des grandes marques qui stockent, nettoient et monnayent leurs informations clientèle. Dans le monde réel donc, il semble presque consensuel d'être fichés et démarchés par des enseignes. En revanche, sur le Net, les internautes semblent davantage inquiets du devenir des traces qu'ils laissent en ligne. Qu'est-ce que l'arrivée du Net change à ces pratiques commerciales ? Prenons-nous davantage de risque quand nous remplissons un questionnaire en ligne ?

Cette forme de profilage est pourtant indispensable à la survie d'un modèle économique qui a la gratuité comme principe et la publicité comme outil. Mais doit-on payer la gratuité au prix fort, c'est-à-dire celui de la perte de protection des données personnelles ? D'autant plus que les internautes semblent aujourd'hui plus occupés à se rendre visibles sur les réseaux sociaux qu'à rester anonymes : un changement de comportement qui modifie le rapport du consommateur à la marque.

Mots-clés : protection, données personnelles, modèle de gratuité, cartes de fidélité, anonymat, visibilité, publicité, marques.

Trading our Identities - Profiling as an Economic Model

Profitable businesses based on personal data were not invented with the Web. From mail order to loyalty cards, thousands of files have swollen the data banks of big corporate brands that collect, clean up and trade their customer data. In the real world, being contacted by commercial firms that have one's personal details on file seems to be an acceptable fact of life. However, people surfing the Web seem to be far more concerned about leaving traces that can be monitored. What has changed in commercial practice with the advent of the Web? Are the risks greater when we fill in an on-line questionnaire than one on paper?

This kind of profiling is essential to the survival of an economic model which has "free of charge" as a fundamental principle and advertising as its tools. But are we paying too high a price for these free Web services, by losing protection for our personal data? Web surfers

nowadays seem to be much more concerned with being visible on the Web through social networks than with preserving their anonymity, and this change in behaviour has altered consumer relationships to brands.

Keywords: *data protection, free of charge, loyalty cards, visibility, advertising, anonymity, brands.*

Philippe LEMOINE, *L'avenir de l'échange : monde plat ou nouveau soulèvement alpin ?*

Sur la base de visions alternatives de l'avenir de l'échange (monde plat, monde contrasté), le présent article situe dans une topographie analytique quatre arguments qui militent en faveur d'une vision qui laisse la place à l'inattendu et à la variabilité. Il entend souligner que le droit reste un moyen d'action privilégié pour construire les futurs possibles.

Mots-clés : vision alternative, échange, inattendu, variabilité.

The Future of Exchanges - Flat Earth or New Seismic Upheavals?

Starting from alternative visions of the future in terms of what is exchanged and traded, and how, this paper maps out a topographical analysis (from flat-earth to seismic upheavals) of four arguments favouring a vision that leaves room for the unexpected and for variability, and underlines the role of Law as a key factor in building possible futures.

Keywords: *alternative vision, exchanges, unexpected, variability.*

Michel ARNAUD, *Authentification, identification et tiers de confiance*

Cet article explore les méthodes et moyens à mettre en œuvre pour reconstruire la séparation entre espaces public et privé, mise à mal par la connexion continue sur les réseaux. Il est difficile et pourtant indispensable de proposer un nouveau paradigme garantissant l'exercice de la liberté individuelle car celle-ci n'est plus assurée selon le cadre fixé par la Déclaration des droits de l'homme. Dans une première partie, nous abordons les contradictions de la situation actuelle, avant de proposer ensuite des solutions autour de la pseudonymisation et de terminer par une réflexion sur les conditions à réunir pour la nécessaire multiplicité des identités numériques gérée par la personne assurant ainsi l'exercice de sa liberté.

Mots-clés : espace public, espace privé, liberté individuelle, authentification, identification, tiers de confiance.

Authentication, Identification and Trusted Third Parties

This paper explores ways and means of rebuilding the separation between private and public spheres that is being broken down by continuous network connection. Difficult as it may be, it has become essential to propose a new paradigm to guarantee individual liberties, as these are no longer protected under the framework established by the Declaration on human rights. In the first part of this paper, we examine the contradictions of the current situation. We then propose solutions based on pseudonym use, before concluding with a discussion on the conditions required for individuals to manage their necessarily multiple digital identities themselves, and thereby guarantee their own freedom of choice.

Keywords: *public sphere, private sphere, individual liberties, authentication, identification, trusted third party.*

André VITALIS, « Informatique et Libertés » : une histoire de trente ans

En 1978, une loi a institué en France, un des premiers dispositifs de protection des données personnelles. Trente ans d'application de la loi permettent aujourd'hui d'évaluer à grands traits, la régulation que la Commission nationale de l'informatique et des libertés (Cnil), au centre de ce dispositif, a réussi à établir et les difficultés qu'elle a rencontrées dans cette tâche. Des secteurs d'activité se sont montrés réfractaires à la nouvelle culture ; le pouvoir politique est intervenu à partir du milieu des années 1990, pour abaisser le niveau de protection ; l'opinion publique s'est peu mobilisée pour faire valoir ses droits et les représentations sociales ont appréhendé les techniques d'information de manière de plus en plus positive.

Mots-clés : loi Informatique et Libertés, autorité administrative indépendante, régulation, évaluation.

Privacy Protection Law, 30 Years On

In 1978, one of the first systems for the protection of personal data was established under French law. Thirty years on, the time has come for a broad assessment of how far the CNIL, the French data protection authority at the core of the system, has succeeded in regulating the use of personal data, but also of the main difficulties it has encountered. Some branches of industry proved recalcitrant, politics intervened from the mid-1990s to lower the level of protection, public opinion slowly began to lay claim to data protection rights, while social representations of information processes became increasingly positive.

Keywords: *Privacy Protection Law, independent administrative authority, regulation, assessment.*

Éric BARBRY, *Cohérences et incohérences des législations*

Mondialisation oblige, il existe aujourd’hui un développement sans précédent des échanges de données à l’intérieur de l’Europe et hors de l’Union. Par ailleurs, les données personnelles sont devenues un élément important du patrimoine immatériel des entreprises – petites ou grandes – et un élément de leur développement durable. Or il n’existe pas de définition juridique précise de la notion de flux. Les réglementations sont très disparates hors de l’Europe et, même au sein de l’Union, les différences résiduelles ne permettent pas de traiter les flux avec une sécurité juridique maximale.

Sont proposées ici quelques pistes de réflexion sur l’évolution possible du droit des données personnelles face à cette mondialisation, notamment :

- La nécessité d’une graduation d’application des règles, entre petites, moyennes et grandes entreprises.
- La possibilité de permettre au CIL (correspondant Informatique et Libertés) d’avoir un vrai pouvoir s’agissant des flux de données avec la mise en œuvre d’un régime adapté.
- L’établissement de règles plus claires et plus accessibles à toutes les entreprises y compris les PME et un allègement des procédures.

Mots-clés : loi Informatique et Libertés, correspondant Informatique et Libertés (CIL), flux transfrontières, directive, sphère de sécurité.

Coherence and Inconsistency in Privacy Laws

Globalization has brought an unprecedented increase in exchanges of data both inside and outside the European Union. Personal data have become major intangible assets for companies, however small or large, and are instrumental in maintaining corporate sustainability. Yet there is no precise legal definition of what constitutes a data flow. Regulations vary widely outside the EU, and residual differences even within it mean that flows cannot be treated with maximum legal security.

This paper suggests how laws on personal data could be remodelled to cope with globalization, in particular to:

- *Tailor regulations to the size of the company (small, medium, large).*
- *Give DPOs (data protection officers) greater powers over data flows.*
- *Establish clearer rules for all companies, including SMEs, and streamline procedures.*

Keywords: *data protection and privacy, data protection officer (DPO), transboundary flows, directive, safe harbour.*

Alex Türk, *Bilan et perspectives de la Cnil*

La Cnil est confrontée à une évolution technologique incessante et considérable face à laquelle elle doit rester vigilante. La question des usages se pose au regard des menaces vis-à-vis de l'exercice des libertés. Un double traçage dans le temps et dans l'espace se produit, cristallisant les discours et la personnalité d'un individu de manière indélébile. La protection des données personnelles est appliquée de manière très inégale dans le monde tandis que le G29 fait respecter la législation de l'Union européenne sur son territoire. Alors que la Cnil est amenée à assurer de plus en plus de contrôles, elle manque de moyens qu'il faudrait lui procurer en demandant des contributions aux collectivités territoriales et aux entreprises.

Mots-clés : traçage, droit à l'oubli, protection des données personnelles, Cnil, G29, Safe harbor.

The French Data Protection Authority (CNIL): Review and Perspectives

To exercise the vigilance required of it, the CNIL – the French Data Protection Authority - has to deal with a continuous stream of technological development, which is often of major significance. The issue of data use needs to be addressed because it raises potential threats to civil liberties. Data leave traces both in space and time, generating indelible snapshots of individual discourses and personalities. Personal data protection is unevenly applied around the world, while the G29 enforces European data protection legislation within Europe. The CNIL is required to apply ever more controls, but lacks the financial resources to do so. These should be provided by contributions from territorial authorities and private companies.

Keywords: tracking, right to oblivion, personal data protection, CNIL, G29, safe harbour.

Danielle BAHU-LEYSER, *Une éthique à construire*

La rapidité d'appropriation, par les utilisateurs, des évolutions technologiques des TIC, la mouvance des usages et l'internationalisation des réseaux entravent la volonté des États et des acteurs de faire obstacle aux atteintes aux données personnelles et sensibles des individus et des organisations. *A fortiori*, l'arrivée dans le monde virtuel des réseaux sociaux, la mondialisation des moteurs de recherche et des services d'infogérance constituent de nouvelles formes de risques d'atteintes aux données personnelles ou sensibles des personnes et des organisations. De ce fait, les utilisateurs des TIC se trouvent confrontés soit à une régulation et une réglementation existantes mais inaptées à les protéger, soit face à un vide juridique propice à toutes les dérives. La sensibilisation des citoyens à la vigilance, le renforcement des législations nationales, la mise en place d'une gouvernance internationale sur un « socle minimal de protection des données » (cf. la proposition de « Kyoto des données

personnelles » d'Alex Türk, président de la Cnil), tels apparaissent les trois piliers d'une éthique à construire.

Mots-clés : éthique, gouvernance, mondialisation, régulation, réseaux sociaux.

Building up a Data Use Ethic

The speed with which users have appropriated technological developments in the ICTs, the shifting trends in their use and the globalisation of networks are all working against the will of States and other agencies to prevent the misuse of personal and sensitive data belonging to individuals and organisations. The advent of social networking in the virtual world and the globalisation of Web search engines and outsourcing services have introduced new kinds of risks to such personal or sensitive data. ICT users are therefore either confronted with existing rules and regulations that do not offer adequate protection, or with a legal vacuum that encourages abuses of every kind. Strengthening citizens' awareness, reinforcing national laws and international governance based on a core system of data protection (cf. proposal for a "Kyoto protocol on personal data" from Alex Türk, chairman of the CNIL), should be the foundations of the data protection ethic we need to build up.

Keywords: Ethics, globalisation, governance, regulation, social networks.

Jean Marc MANACH, Contourner les systèmes de traçabilité

Brian Gladman est un ancien directeur des communications électroniques stratégiques du ministère de la Défense britannique et de l'Otan ; Ian Brown, est un cryptographe anglais, membre de l'ONG Privacy International. En l'an 2000, ils rendaient public un texte expliquant comment contourner, en toute légalité, les diverses mesures de « cybersurveillance » adoptées par les législateurs. Ces techniques s'avéreraient en effet « techniquement ineptes et inefficaces à l'encontre des criminels » et risqueraient, *a contrario*, de « saper le droit à la vie privée et à la sécurité des citoyens et du marché ».

Leur démarche est d'autant plus salutaire que les gouvernements se contentent généralement, au mieux, d'expliquer que toute action informatique laisse des traces, et que l'on est de toute façon surveillé (mais sans jamais, étrangement, expliquer comment s'en protéger), au pire, de passer des lois sécuritaires renforçant cette cybersurveillance, contribuant d'autant à créer un climat de peur, loin du climat de confiance nécessaire à toute démocratie.

Mots-clés : Internet, vie privée, sécurité, anonymat, pseudonymat, surveillance.

Bypassing Data Tracking Systems

Brian Gladman is a former Director for strategic electronic communications for the British Ministry of Defence and NATO; Ian Brown is a British cryptographer and a member of the NGO Privacy International. In 2000, they published a paper detailing various countermeasures that can be used, perfectly legally, to evade the technical systems that governments adopt in order to monitor what users are doing on the Internet. These systems are criticised as not only “technically inept and ineffective against criminals” but also liable to “undermine the privacy, safety and security of law-abiding citizens and businesses”.

Their work is all the more valuable as governments either, at best, merely explain that any IT activity leaves traces and that people are monitored in any case (but, curiously, they never explain how people can protect their privacy) or, at worst, pass laws on “security” that reinforce cyber-surveillance systems, thus helping to create a climate of fear that can only undermine the trust on which a democratic society relies.

Keywords: *Internet, privacy, security, anonymity, pseudonymity, surveillance.*

Renaud FABRE, La personne : une régulation par les normes ?

Les choix normatifs actuels du Web esquissent-ils une mutation des contours de la personne et, dans l’affirmative, quelle mutation ? Quelles régulations les normes actuelles autorisent-elles au regard de l’objectif permanent de sauvegarde d’une identité personnelle et d’une vie privée, et quels obstacles se dressent-ils dans ce sens ? En soutenant que des réponses évolutives sont en cours de construction, cet article suggère des buts et voies d’investigation, et conclut en proposant une typologie d’objectifs de régulation communs aux choix normatifs de production et d’échange de données personnelles.

Mots-clés : choix normatifs, données personnelles, régulation du profil personnel, « vis à vis » virtuel, « métalangue ».

Privacy and the Personal - The Case for Regulatory Standards

Are current standardization options for the Web pointing to a redefinition of the boundaries of what is personal? If so, how are they being redefined? What forms of regulation do current standards allow as regards the ever-relevant objective of safeguarding personal identity and privacy, and what obstacles are emerging to counter this aim? This paper argues that responses are developing to address the changing situation, and suggests aims and avenues for investigation. It concludes with a proposal for a typology of regulatory objectives that are common to standardization options as well as exchanges of personal data.

Keywords: *range of privacy, regulation through standards of identification and description, social networking, personal data, descriptive framework.*