CAHIERS IP
INNOVATION & PROSPECTIVE
N°01

VIE PRIVÉE À L'HORIZON 2020

PAROLES D'EXPERTS

Focus sur des transformations clés au croisement des usages, des technologies et des stratégies économiques

Quel paysage nouveau pour les données personnelles, les libertés et la vie privée ?

Protéger, réguler, innover demain

CNIL
Commission Nationale de l'Informatique et des Libertés

La collection des cahiers IP, Innovation & prospective, a vocation à présenter et à partager les travaux et études prospectives conduits par la Direction des études, de l'innovation et de la prospective de la CNIL et par son laboratoire d'innovation. Il s'agit ainsi de contribuer à nourrir le débat et la réflexion dans le champ Informatique et Libertés.

Commission Nationale de l'Informatique et des Libertés
Direction des études, de l'innovation et de la prospective
8 rue Vivienne – CS 30223 – 75083 Paris Cedex 02
Tél. : 01 53 73 22 32 – Fax : 01 53 73 22 00 – deip@cnil.fr
Édition semestrielle
Directeur de la publication : Édouard Geffray
Rédacteur en chef : Sophie Vulliet-Tavernier
Conception graphique : EFIL 02 47 47 03 20 / www.efil.fr
Impression : ImprimPlus (Essonne)
Crédit Photos : Fotolia, istockphoto, @identitywoman
ISSN : en cours
Dépôt légal : à publication

Suivez la CNIL sur...

COMMISSION NATIONALE
DE L'INFORMATIQUE ET DES LIBERTÉS

CAHIERS IP

INNOVATION & PROSPECTIVE

N°01

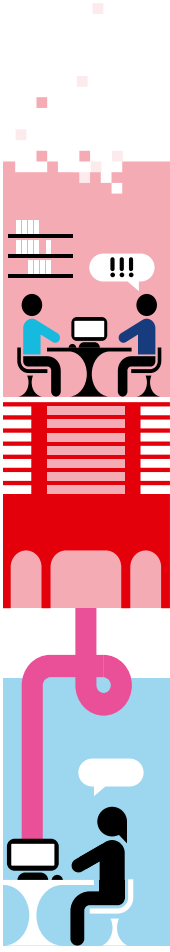
La rédaction de ce cahier ainsi que le suivi de sa conception et de son impression ont été assurés par la direction des études, de l'innovation et de la prospective de la CNIL (Olivier Coutor, Geoffrey Delcroix, Olivier Desbiey, Marie Leroux, Sophie Vulliet-Tavernier, avec l'aide de Caroline Chemouilli et de Nicolas Carougeau).

ÉDIT

Partie 0.1
Focus sur des transformations clés au croisement des usages, des technologies et des stratégies économiques

Partie 0.2
Quel nouveau paysage pour les données personnelles, les libertés et la vie privée ?

Partie 0.3
Protéger, réguler, innover demain



Quels seront à l'horizon 2020 les enjeux de la protection des données personnelles ? Quelle sera notre vie privée ? À l'heure du « tous connectés », où en seront nos libertés numériques ? Et quelles sont les formes que devra prendre la régulation pour répondre à ces nouveaux défis ? Telles sont les questions clés que nous avons posées entre l'automne 2011 et le printemps 2012 à plus de quarante experts d'horizons variés. En effet, à l'heure de l'explosion des données personnelles *via* le *Big Data*, de la multiplication des nouveaux usages toujours plus consommateurs de données, le régulateur ne peut et ne doit pas agir seul. Il a besoin d'écouter, de partager et de réunir autour de lui des communautés de points de vue afin de comprendre l'environnement complexe dans lequel il agit.

L'objet de ce premier numéro des Cahiers Innovation & Prospective, nouvelle publication de la CNIL, est de restituer ces paroles d'experts. Ceux-ci nous ont donné leurs visions – bien sûr parfois différentes – des transformations clés et des évolutions futures dans le champ de la vie privée, des libertés et des données personnelles, ainsi que leurs lectures – toujours très riches d'enseignements – des formes de régulation à venir. Nous allons les entendre, tenter de les comprendre et voir quels bénéfices le régulateur peut en tirer.

Cette intiative témoigne d'une impulsion nouvelle que je souhaite donner à la CNIL. Il est aujourd'hui nécessaire que celle-ci développe une culture de réseau et travaille de plus en plus avec toutes les « parties prenantes » à la régulation. Notre Commission doit savoir évoluer et ajuster ses modes d'intervention si elle veut rester pertinente. Elle doit développer ses capacités d'analyse prospective afin de mieux comprendre les évolutions technologiques et les nouveaux usages, anticiper et évaluer les nouveaux enjeux de protection des données. Elle doit s'affirmer comme un régulateur pragmatique et crédible, capable de proposer des solutions opérationnelles. Elle doit ainsi s'investir, dans la limite de ses moyens, dans les recherches menées en ces domaines, piloter ou commander des travaux qui lui semblent particulièrement importants.

En 2011, nous avons mis en place la direction de la prospective. Le Comité de la prospective, créé en mai 2012, a constitué une deuxième étape, ouverte cette fois vers l'extérieur en mobilisant des talents et personnalités diverses.

Le lancement des Cahiers IP et l'organisation d'une journée de débats autour de leurs contenus est une nouvelle étape. Ces Cahiers et le débat qui entourera leurs contenus vont permettre à notre institution de donner corps à une communauté de recherche (chercheurs, *think tanks*, développeurs, experts du secteur, français comme étrangers) sur les questions de la protection des données personnelles. La CNIL a besoin de cette communauté à multiples facettes pour réfléchir, trouver de nouvelles solutions, parfois se remettre en cause.

Notre société connaît des mutations profondes sous l'effet conjugué des évolutions des technologies, des modèles d'affaires émergents et des pratiques sociales toujours renouvelées du numérique. Alors qu'un nouveau cadre juridique se dessine au plan européen, la question de la protection des données personnelles est, plus que jamais, au cœur du débat. Elle concerne tous les acteurs – citoyens, Gouvernements, grands acteurs du monde numérique, autres entreprises, administrations… – et se retrouve au carrefour d'enjeux multiples – économiques, sociaux, juridiques… – tant au plan national qu'international.

Je forme le vœu que de la confrontation des points de vue et de la mise en commun d'idées et de ressources émerge de l'innovation, y compris dans le domaine de la régulation, pour construire, ensemble, le cadre éthique de l'univers numérique de demain.

Isabelle Falque-Pierrotin,
Présidente de la CNIL

42 EXPERTS RÉPONDENT À LA CNIL

Ce premier numéro des cahiers IP est consacré à la restitution d'un chantier prospectif qui a été lancé à l'automne 2011 par la direction des études, de l'innovation et de la prospective (DEIP) de la CNIL, sur le thème : « La vie privée, les libertés et les données personnelles à horizon 2020. Quels enjeux de protection, de régulation pour la CNIL ? Représentations, perceptions et attentes des acteurs. »

Ce chantier a consisté à réaliser, de septembre 2011 à avril 2012, plus de quarante entretiens auprès d'experts d'horizons variés : sociologues, économistes, philosophes, juristes, historiens, chercheurs en sciences de la communication ou en sécurité informatique, représentants du monde de l'entreprise et d'associations intervenant dans le champ du numérique ou de la défense des droits.

Il s'agissait de :

- doter la CNIL d'une analyse des représentations externes des transformations clés qui devraient interagir sur ses domaines d'intervention à l'horizon 2020 ;
- confronter ces représentations externes aux perceptions de la CNIL (par exemple au travers de débats, événements et journées d'études comme la journée « vie privée 2020 ») ;
- associer les experts aux travaux et réflexions prospectives de la CNIL dans un esprit de dialogue constructif.

À cet effet, une grille d'entretiens (voir page 58 « annexe »), a été établie sur la base de questions ouvertes, prenant en compte les aspects suivants :

- la perception des évolutions majeures (technologiques, économiques, sociétales…) dans le champ de la vie privée, des libertés et des données personnelles : tendances, incertitudes et ruptures possibles ;
- les transformations en cours et à venir de la relation des individus et de la société à la vie privée et aux données personnelles ;
- la vision des experts sur les formes de régulation à venir, leurs attentes et lectures du rôle des autorités de protection des données demain ;
- et, en fonction des acteurs, leurs projets, leurs orientations dans le champ concerné.

Ces entretiens ont donné lieu à une synthèse qui est donc le sujet principal de ce cahier. La journée d'études « vie privée 2020 », organisée le 30 novembre 2012, en est le prolongement.

Ce cahier IP n'a pas, bien sûr, vocation à être un document prospectif définitif et exhaustif autour du vaste sujet « vie privée 2020 » ou à exprimer la doctrine de la CNIL. Il vise plutôt à offrir un panorama dynamique des visions contrastées des grandes transformations à l'œuvre.

Comme la journée d'études vie privée 2020, ce cahier sera, nous l'espérons, le point de départ de sujets de recherche à explorer en commun et d'une réflexion prospective concertée.

REMERCIEMENTS

Nous souhaitons remercier ici encore très vivement l'ensemble des experts pour leurs contributions, toujours riches et passionnantes et pour avoir pris le temps de nous recevoir, de répondre à notre longue liste de questions, et d'échanger enfin sur le contenu de ce cahier.
Toute l'équipe de la DEIP remercie chaleureusement Nathalie Bassaler et François Bourse, consultants en prospective au sein de Magellis Consultants et GERPA, pour leur accompagnement, essentiel, dans la conduite de ce premier chantier.

LISTE DES 42 EXPERTS

Maryse Artiguelong Secrétaire générale adjointe de la Ligue des Droits de l'Homme (LDH)

Christine Balagué Titulaire de la Chaire réseaux sociaux à l'Institut Mines-Telecom. Co-présidente du think tank Renaissance Numérique

Arnaud Belleil Directeur général adjoint de Cecurity.com. Vice-président d'honneur de l'Association Française des Correspondants à la protection des Données à caractère Personnel (AFCDP)

Pierre-Jean Benghozi Directeur de recherche CNRS et Professeur à l'École Polytechnique, en charge du pôle de Recherche en Économie et Gestion et de la Chaire « Innovation et Régulation des services numériques ». Membre du comité de la prospective de la CNIL

Alain Bensoussan Avocat à la Cour d'appel de Paris. Chargé d'enseignement en droit de l'informatique à l'École Centrale de Paris

Dominique Boullier Professeur des universités. Enseignant en sociologie à Sciences Po Paris. Coordonnateur scientifique du Médialab de Science Po Paris

Stefana Broadbent Psychologue et professeur d'anthropologie du numérique à l'University College de Londres (UCL). Directrice du Master en Anthropologie du numérique dans le département d'Anthropologie de UCL. Membre du comité de la prospective de la CNIL

Dominique Cardon Sociologue au Laboratoire des usages SENSE d'Orange Labs. Chercheur associé au Centre d'étude des mouvements sociaux de l'École des Hautes Études en Sciences sociales (CEMS/EHESS). Membre du comité de la prospective de la CNIL

Antonio Casilli Sociologue et maître de conférences en « Digital Humanities » à Telecom ParisTech. Chercheur associé en sociologie au Centre Edgar Morin (EHESS, Paris)

Claude Castelluccia Directeur de recherche Inria. Responsable de l'équipe Inria Privatics (Informatique et protection de la vie privée)

Isabelle De Lamberterie Directrice de recherches au Centre d'études sur la coopération juridique internationale (CECOJI) du CNRS

Mireille Delmas-Marty Professeur de Droit et Titulaire de la chaire « Études juridiques comparatives et internationalisation du droit » au Collège de France. Membre de l'Académie des sciences morales et politiques

Dominique Desjeux Professeur d'anthropologie sociale et culturelle à l'université Paris Descartes, Faculté des sciences humaines et sociales Sorbonne

Yves Deswarte Directeur de recherche au CNRS au sein de l'unité de recherche LAAS (Laboratoire d'analyse et d'architecture des systèmes)

David Forest Avocat à la Cour d'Appel de Paris. Docteur en droit privé et docteur en science politique. Chargé d'enseignement en droit des technologies de l'information aux universités de Paris I, Paris VII, Paris XI

Jean Frayssinet Professeur émérite des universités Faculté de Droit de l'Université Aix-Marseille III. Membre de la Commission de contrôle des fichiers d'INTERPOL

Paul-Olivier Gibert Président de Digital & Ethics. Président de l'Association française des correspondants à la protection des données à caractère personnel (AFCDP)

Olivier Iteanu Avocat à la Cour d'appel de Paris. Chargé d'enseignement en droit du numérique aux universités de Paris XI et Paris I

Francis Jauréguiberry Sociologue et professeur à l'Université de Pau et des Pays de l'Adour. Directeur du laboratoire Société Environnement Territoire (SET) au CNRS

Josiane Jouët Professeur et directrice de recherches en Sciences de l'information et de la communication à l'université Panthéon Assas. Docteur en sociologie

Daniel Kaplan Cofondateur et Délégué Général de la Fondation Internet Nouvelle Génération (FING)

Emmanuel Kessous Professeur de sociologie à l'Université de Sophia-Antipolis. Chercheur au GREDEG (UMR CNRS 7321) et chercheur associé au GEMASS (Paris IV - UMR CNRS 8598)

Caroline Lancelot-Miltgen Maître de Conférences en Sciences de Gestion à l'Université d'Angers. Chercheur au GRANEM (Groupe de Recherche angevin en Économie et Management)

Daniel Le Métayer Directeur de recherche Inria. Responsable de l'Inria Project Lab CAPPRIS sur la protection de la vie privée. Membre du jury de thèse Informatique et Libertés de la CNIL

Yann Leroux Docteur en psychologie. Membre de l'observatoire des mondes numériques en sciences humaines

Philippe Lemoine PDG de l'entreprise LaSer. Président de la FING et du Forum d'Action Modernités. Ancien membre de la CNIL et ancien commissaire du gouvernement de la CNIL

Nathalie Mallet-Poujol Directrice de recherche au CNRS. Directrice de l'Équipe de Recherche Créations Immatérielles et Droit (ERCIM) UMR 5815, Université Montpellier I. Membre du jury de thèse Informatique et Libertés de la CNIL

Jean-Marc Manach Journaliste à Owni.fr et InternetActu.net. Auteur du blog Bug brother pour le Monde.fr

Meryem Marzouki Chargée de recherche au CNRS au laboratoire d'informatique de Paris VI (LIP6, CNRS/Université Paris VI). Présidente de l'association « Imaginons un réseau Internet solidaire » (IRIS)

Nicolas Nova Professeur à l'Université d'Art et de Design de Genève (HEAD-Genève) et à l'École Nationale Supérieure de Création Industrielle (ENSCI-Paris). Consultant et chercheur pour « Near Future Laboratory »

Pierre Piazza Maître de conférences en sciences politiques à l'université de Cergy-Pontoise (CESDIP/LEJEP). Membre du Centre de recherches sociologiques sur le droit et les institutions pénales (CESDIP)

Yves Poullet Recteur des Facultés Universitaires Notre-Dame de la Paix (FUNDP). Professeur à la Faculté de droit des FUNDP et de l'Université de Liège (Ulg)

Alain Rallet Directeur du laboratoire Analyse des Dynamiques Industrielles et Sociales (ADIS) de l'Université Paris Sud. Directeur du Master « Industries de Réseau et Économie Numérique » (IREN)

Fabrice Rochelandet Économiste. Professeur en sciences de la communication à l'Université Sorbonne Nouvelle Paris III et au sein du master IREN à l'Université Paris Sud. Membre du jury de thèse Informatique et Libertés de la CNIL

Françoise Roure Contrôleur général économique et financier. Présidente de la section « Technologies et Société » du Conseil général de l'économie, l'industrie, l'énergie et des technologies (CGEIET). Présidente du groupe de travail sur les nanotechnologies de l'OCDE

Antoinette Rouvroy Chercheur qualifié du FRS-FNRS en philosophie du droit, associée au Centre de Recherche en Information, Droit et Société (CRIDS) de l'Université de Namur. Membre du comité de la prospective de la CNIL

Bernard Stiegler Philosophe. Directeur de l'Institut de recherche et d'innovation (IRI) au sein du Centre Georges-Pompidou. Professeur et directeur de l'unité de recherche « Connaissances, organisations et systèmes techniques » à l'Université de technologie de Compiègne (UTC)

Cécile de Terwangne Professeur à la Faculté de Droit. Directrice de recherche à la cellule Libertés et Société de l'information du CRIDS. Facultés Universitaires Notre-Dame de la Paix (Namur, Belgique)

Henri Verdier Créateur d'entreprise, spécialisé dans les « Big Data ». Président du pôle de compétitivité Cap Digital. Membre du conseil scientifique de l'institut Mines-Télécom. Membre du comité de la prospective de la CNIL

Jean-Claude Vitran Responsable de la commission « Libertés et TIC » à la Ligue des Droits de l'Homme (LDH). Administrateur de la Fondation Sciences Citoyennes (FSC)

Dominique Wolton Directeur de l'Institut des Sciences de la Communication du CNRS. Directeur de recherches au CNRS. Membre du jury de thèse Informatique et Libertés de la CNIL

Jérémie Zimmermannn Porte-parole et cofondateur de la Quadrature du Net. Ingénieur consultant en technologies collaboratives

Les propos recueillis lors des entretiens sont des points de vue personnels, ils n'engagent pas les organismes pour lesquels travaillent les experts.


vote électronique
consentement
cryptographie
surveillance
cloud
dictature des algorithmes
espaces publics
opt-out
immersion
juridictions
NIR
dispersion au travail
archives
identité numérique
négligence
vidéosurveillance
corps
plateformes
pédagogie
2020
capacité de détachement
manière de penser
publications
déconnectés
outils de protection
sécurité
cerveau
logiques prédictives
maîtrise
fragilité
big other
dévoilement
protection
algorithme
neurosciences
small data
vulnérabilité technique
débat
illusion de contrôle
webification
vulnérabilité humaine
cyborg
génétique
rapidité
homme augmenté
labels
dématérialisation
VRM
fichiers
geeks
expertise
non connectés
transparence
quantified-self
dénumérisés
biométrie
analyse comportementale
design
pseudonymat
calculés
SSI
univers persistants
secret
chiffrement
exposer
espaces privés
multitâche
ADN
nanotechnologies
vie
temps réel
innover
normes
fractures
géolocalisation
intime
droit au mensonge
fuites de données
regard
vulnérabilité matérielle
open data
data-mining
libertés
paraître
marketing de soi
code is law
technologie
ON-OFF
web social
risques
privée
régulation
mots de passe
droits
privacy in context
grand public
interfaces
privacy paradox
réseaux sociaux
se rétracter
observation satellitaire

VIE PRIVÉE À L'HORIZON 2020

La société est en train de se transformer de manière radicale sous l'effet de plusieurs facteurs, parmi lesquels :

- l'influence croissante des technologies de l'information et de la communication sur l'organisation de la société, au point que la norme du « tous connectés » paraît irrésistible et irréversible ;
- le développement de l'interopérabilité entre les dispositifs technologiques et de leur convergence avec diverses disciplines scientifiques, telles que les sciences du cerveau et la génétique ;
- l'explosion des usages des réseaux sociaux qui contribuent de plus en plus à l'expression de l'individu et, par ailleurs, sont de plus en plus consommateurs de données personnelles ;
- le changement de statut du téléphone portable (smartphone), en lien avec la multiplication des usages de l'Internet mobile ;
- la banalisation des captations automatiques de données personnelles ;
- la porosité croissante entre vie publique et vie privée, notamment dans le domaine professionnel du fait de la déterritorialisation du travail et de la sortie du temps cloisonné.

Les cahiers présentent donc une synthèse des contributions des experts.

La première partie présente quelques-unes des transformations clés, déjà en cours, qui mêlent innovation technologique, construction de nouveaux modèles économiques et mise en place de nouvelles pratiques sociales. Y sont successivement abordés le web social, la monétisation des données personnelles, le *Big Data* et la place prise par les algorithmes dans le traitement des données personnelles, la géolocalisation, les techniques biométriques, l'Internet des objets et les nanotechnologies.

À l'aune de ces transformations, la deuxième partie analyse l'évolution des notions clés de « donnée personnelle » et de « donnée sensible » et des concepts de « *privacy paradox* », « identité numérique » et « fracture numérique ».

La dernière partie suggère plusieurs pistes pour l'élaboration de la régulation de demain, en recentrant le questionnement autour des libertés à préserver, en envisageant le développement de nouveaux modes de régulation tant juridiques qu'extra-juridiques et en proposant une réflexion sur la reconnaissance de nouveaux droits individuels, regroupés sous une catégorie qui est peut-être à créer : les Droits de l'Homme numérique.

01

Partie 0.1

FOCUS SUR DES TRANSFORMATIONS CLÉS…

AU CROISEMENT DES USAGES, DES TECHNOLOGIES ET DES STRATÉGIES ÉCONOMIQUES

LA RÉVOLUTION DU WEB SOCIAL : DEMAIN, TOUS DES *PEOPLES* ?

« L'essor des réseaux sociaux est la grande évolution de ces dix dernières années. Les sociologues n'ont pas vu venir cette « dynamique expressiviste » qui conduit à l'augmentation du désir d'expression des individus. L'intime est devenu une valeur personnelle, individualisée : il se définit par rapport à un contexte et les comportements individuels en la matière semblent durablement divergents. La vie privée devient un élément qui définit l'autonomie, le libre arbitre. Certains la rapprochent de plus en plus des questions de dignité de la personne. Chacun veut donc garder une marge de manœuvre. En revanche, ce serait une erreur fondamentale de penser que le sens de la vie privée disparaît : en effet, plus je m'expose, plus la vie privée aura de la valeur pour moi, je veux pouvoir gérer la frontière entre l'exposition et l'intime. Le sens du secret reste bien présent. Par exemple, il est frappant de remarquer que sur Facebook la majorité des gens ne parlent pas de l'intimité amoureuse. De même, les stratégies de publication des photos sont souvent très sophistiquées. »

Dominique Cardon

LES RÉSEAUX SOCIAUX SONT-ILS DES ESPACES PUBLICS ?

L'essor des blogs, des sites d'avis en ligne, puis des réseaux sociaux a contribué à développer un Internet de plus en plus organisé autour du profil des utilisateurs, un web social. Ce web social s'est construit autour des différentes facettes de l'identité numérique, projetées différemment selon le type de visibilité que chaque plateforme confère à ses membres. Selon nos experts, ces espaces font naître de nouvelles interrogations parce qu'ils ne sont ni tout à fait publics, ni tout à fait privés. Ces zones où les individus dévoilent publiquement une partie de leur intimité sont décrites comme un clair-obscur par Dominique Cardon. Les utilisateurs y partagent leur vie sociale en s'adressant à un réseau composé de proches, qui reste difficilement accessible pour les autres. S'ils ont plusieurs centaines d'amis sur les réseaux sociaux, en ce qui concerne les conversations personnelles ils ne communiquent en réalité qu'avec une dizaine d'entre eux. Seul ce cercle restreint se sent autorisé à intervenir dans les conversations. C'est à l'occasion de discussions plus générales, moins intimes, que les autres interviennent. De cette manière, ils font « respirer leur identité ». Le propre des réseaux sociaux est de jouer avec cette frontière entre l'espace de la conversation personnelle, privée et celui de la publication totalement publique. Les possibilités de partager menacent en permanence le cloisonnement de certaines publications et les individus redoutent le « débordement ».

Au sein de ces espaces de clair-obscur, se dévoiler prend un nouveau sens. Le néologisme « extime » consacre cette dimension dans laquelle les individus partagent publiquement une partie de leur intimité.

TRANSPARENCE, DÉVOILEMENT ET MARKETING DE SOI

Une des conséquences de la démocratisation des réseaux sociaux est que le partage au sein de ces espaces ne se fait pas totalement au hasard. En effet, il y a aujourd'hui une pression normative à la présence sur ces réseaux, si bien que les cercles « d'amis » sont de plus en plus étendus – pouvant inclure des collègues, des connaissances plus éloignées – alors que ces espaces étaient initialement plutôt réservés aux intimes (famille, amis proches). Les contenus partagés sont également plus divers, incluant davantage de photos et de vidéos par exemple.

Dans ce contexte, l'expérience de l'exposition de soi est en train d'évoluer vers une plus grande

« BIG OTHER » ET SURVEILLANCE LATÉRALE : LES AUTRES FORMENT-ILS UNE NOUVELLE AUTORITÉ ?

L'expansion de la surveillance latérale (ou mutuelle) est une question qui intéresse plusieurs de nos experts. Pour Dominique Cardon elle désigne l'ensemble des comportements intrusifs des utilisateurs les uns envers les autres. Antonio Casilli explique que « pour comprendre qui est à l'écoute, il faut émettre des signaux qui vont provoquer des réactions, des commentaires ». C'est donc le niveau de participation qui détermine la force de la surveillance participative de tous par tous : le monde du « Big Other ». L'acceptation sociale de cette surveillance par les pairs est peut-être plus importante chez les jeunes générations. C'est en tout cas le point de vue de Yann Leroux pour qui cette « violence » est mieux perçue, car plus séduisante et moins brutale que celle qui serait exercée par une autorité. Chacun a ce pouvoir de surveillance sur autrui, ce qui tranche avec le modèle social classique, celui du panoptique. Si, dans le cas d'une surveillance institutionnelle, la régulation la plus adaptée est certainement juridique, dans le cas de la surveillance mutuelle, la régulation est plus complexe à organiser car les utilisateurs affichent leur identité de manière volontaire. Elle doit donc être plutôt sociale et culturelle et passe par l'auto-organisation. Dominique Cardon propose de transférer la critique de ceux qui s'exposent à ceux qui regardent. S'il est difficile de se prononcer sur ses conséquences à long terme, Yann Leroux s'interroge sur cette nouvelle forme de surveillance : comment grandir si ce n'est en s'opposant à une figure d'autorité ?

maturité dans les pratiques et, pour certains utilisateurs, un meilleur calcul qui accompagne des stratégies sophistiquées de dévoilement. Pour Pierre-Jean Benghozi, ces stratégies peuvent être la transparence, le cloisonnement ou l'obfuscation. Le web social permet à chaque utilisateur de commenter, partager ses intérêts, ses avis qui vont avoir une résonnance auprès de son public. Il y a peut-être là un risque de fracture numérique (voir «Vers de nouvelles fractures numériques ?» page 40) dans la maîtrise de son dévoilement, entre ceux qui vont savoir gérer habilement les différentes facettes de leur identité numérique (cloisonnement ou croisement d'attributs personnels et professionnels) pour en tirer parti (visibilité, trouver un emploi), et ceux qui au contraire vont subir cette exposition. Selon Dominique Cardon, il y a une vraie « carrière d'utilisateur avec ses troubles, ses anicroches qui même s'ils sont peu nombreux font partie de l'apprentissage ». En focalisant l'activité sur la création et la mise en scène de la face publique qui constitue le profil, les réseaux sociaux incitent leurs membres à penser le marketing de leur propre identité. Les utilisateurs font en permanence des études de marché sur eux-mêmes et développent des compétences de « sculpture de soi ».

... PARAÎTRE, S'EXPOSER, SE RÉTRACTER : UN MEILLEUR CONTRÔLE ET DE NOUVEAUX DROITS

Pour autant, la vie privée ne disparaît pas, au contraire. Plus les individus se dévoilent, plus leur vie privée prend de la valeur ; en fait, ils savent gérer la frontière entre ce qu'ils souhaitent exposer et ce qu'ils considèrent comme devant rester intime.

Un élément essentiel, souligné par les chercheurs, est la préservation du contexte (Dominique Cardon, Danah Boyd). Plus que le contenu lui-même, ce que les individus souhaitent contrôler c'est le contexte, le sens d'une publication : le lieu, le moment, les « destinataires » et la tonalité générale. La polémique de septembre 2012 autour du « *Bug* de Facebook » qui aurait occasionné la publication de messages privés sur la partie publique du « mur » souligne l'importance du contexte originel. Il illustre cet effet de débordement où des publications réservées aux « amis » sortent du cercle pour circuler de manière publique. La confusion dans l'esprit des utilisateurs est notamment venue d'une nouvelle manière choisie par le réseau social pour présenter d'anciennes publications en les déliant de leur contexte. La disparition du sens initial des publications a rendu particulièrement difficile, plusieurs années plus tard, d'en déterminer le caractère véritablement public ou privé, ce qui a contribué à crédibiliser le *bug* présumé.

Pour Alain Bensoussan, Facebook est un monde merveilleux où l'entrée en matière se fait par « avoir des amis » et par dire « j'aime ». Il n'y a pas d'exposition de soi, c'est plutôt le paradigme du paraître qui prévaut. Les réseaux sociaux sont l'expression de la valeur universelle du « droit de paraître ». Ils permettent de se montrer sans limite de temps, de lieu, d'événement. Dominique Cardon milite pour un « droit à s'exposer » et son symétrique un « droit à se rétracter ». ■

LA DONNÉE AU CŒUR DES MODÈLES D'AFFAIRES : DEMAIN, TOUS TRADERS DE DONNÉES ?

« L'économie des données personnelles repose sur un fort effet de levier (grâce à un coût d'acquisition faible). Le dévoilement de soi est consubstantiel au développement des services marchands web 2.0. Ce qui est difficile à garder en tête pour les utilisateurs, c'est qu'un marchand est présent, il joue le rôle d'intermédiaire. Il ne faut jamais oublier que sur Facebook, votre premier « ami », c'est Facebook : il voit tout et scrute toutes nos activités. La question de la « valorisation » des données personnelles est un problème, d'autant qu'on ne dispose pas d'indicateurs fiables sur ce point. Cependant, ce qui est certain, c'est que les données à caractère personnel n'ont pas de valeur absolue ou intrinsèque : cela dépend du contexte et de l'entreprise concernée. C'est un sujet d'évaluation contingente (et si… alors…). On constate en tout cas que les individus sont peu cohérents sur ces sujets : ils peuvent dans un sondage se dire prêts à payer 100 € pour que Facebook ne vende par leurs données personnelles à des tiers, mais à côté de cela ils sont prêts à livrer toutes celles-ci à leur supérette de quartier pour participer au programme de fidélité et obtenir quelques euros de bons d'achats. Il est donc difficile d'attribuer une valeur financière aux données personnelles. La mise en place d'un droit à compensation en cas d'exploitation des données personnelles d'un individu n'en serait que plus difficile, même si l'on reconnaît que ce droit relève d'une logique de responsabilité juridique et non de propriété. Cette économie est largement une économie de l'immatériel, donc de l'invisible : il faut rendre visible l'invisible (en particulier l'exploitation commerciale des données transmises à l'insu de l'individu), imposer de la transparence. »

Alain Rallet et Fabrice Rochelandet

PLATEFORMES ET GRANDS OPÉRATEURS DE DONNÉES, LES NOUVEAUX MAÎTRES DU MONDE ?

Économie de la contribution, économie de l'attention : des modèles économiques nouveaux ont émergé avec le web 2.0. L'implication de l'utilisateur y est toujours centrale et la monétisation des données personnelles présente partout, à tel point que l'on entend régulièrement parler d'elles comme du « pétrole de l'économie numérique ». Comme le disent Alain Rallet et Fabrice Rochelandet « ces services marchent au dévoilement de soi comme une voiture marche à l'essence ».

Même si le *freemium* gagne du terrain, le modèle principal des activités sur le web consiste à offrir le service aux utilisateurs en le faisant payer par des annonceurs. Ce modèle, qui est celui des plateformes et opérateurs comme Google et Facebook, conduit à des rapports ambigus entre plateformes et utilisateurs, qui ne sont pas à proprement parler des clients. D'autant que les spécificités de l'économie numérique transforment ces grands opérateurs en des sortes de monopoles naturels (intérêt commun à une certaine standardisation, effet réseau). Ces acteurs ont acquis, peut-être temporairement, une place très particulière en devenant « la colonne vertébrale, l'infrastructure indispensable des données personnelles ». Peut-être faut-il, comme Daniel Kaplan, penser à un statut particulier pour ces très grandes plateformes, « qui ne sont pas des opérateurs comme les autres ». Ces plateformes du numérique sont des dépositaires particuliers de données personnelles : elles en sont devenues des gardiens et leur modèle repose autant sur elles que sur la confiance (peut-être un peu naïve) des utilisateurs. Leur responsabilité n'en est que plus importante.

... QUELLE MONÉTISATION DE NOS TRACES ET PUBLICATIONS ?

Cette monétisation est donc partout présente et insaisissable, comme le soulignent Alain Rallet et Fabrice Rochelandet. Pour autant, est-ce vraiment une bonne idée « d'économiser » ce thème ? Selon Pierre-Jean Benghozi, « le pour, c'est que cela crée des mécanismes d'arbitrages, une forme de régulation entre l'offre et la demande et cela sensibilise les consommateurs au fait que ce qu'ils révèlent a un prix, une valeur. En revanche, rien ne prouve que les mécanismes de marché soient plus efficaces dans le domaine des données qu'ils ne le sont déjà dans le domaine de la finance ou de l'industrie classique ». Cette imperfection du marché paraît très probable, étant donné la nature des asymétries : « La contrepartie n'étant pas très claire autour de la monétisation de ces données, il est relativement facile d'identifier ce que l'on achète, pas forcément ce que l'on vend. D'autre part, la démultiplication des données ne permet pas de contrats vraiment clairs : on finira toujours par avoir un marché proposant des paiements forfaitaires. »

LA MAÎTRISE DES DONNÉES, SOURCE DE NOUVELLES ACTIVITÉS ÉCONOMIQUES ?

La protection des données personnelles est plutôt aujourd'hui synonyme de contraintes pour les entreprises, et non d'opportunités d'affaires, comme l'ont souligné les experts. Pour autant, l'avenir pourrait être

différent et la gestion et la protection des données devenir une source d'activité économique à moyen terme. Ainsi, « la *privacy* peut devenir un sujet d'avantage concurrentiel » et d'innovation pour Jérémie Zimmermannn, qui pense également qu'un vrai marché de la protection des données existera autour des questions de sécurité informatique, de chiffrement... quand ces sujets seront « dégeekifiés ». L'essor du *Cloud Computing* grand public pourrait être un déclencheur de ce marché de gestion du patrimoine numérique.

Pour Dominique Boullier, repenser l'économie des données dans une logique assurantielle serait la meilleure chance de réduire une certaine porosité que l'actuel dispositif marchand transactionnel ne fera que renforcer : « Les assureurs seront les intermédiateurs qui entreront en conflit avec ceux qui veulent s'approprier les données personnelles. Ce n'est en soi pas un problème que les données circulent, à condition de donner aux gens les moyens de comprendre et d'agir, par exemple avec l'aide de ces intermédiateurs. Un modèle de régulation associé à l'assurance serait peut-être une mécanique vertueuse. »

Enfin, une voie innovante émerge à partir de l'idée d'un partage réciproque des données entre clients et entreprises, selon le principe résumé par Daniel Kaplan : « Si l'entreprise a une information sur le client, le client doit l'avoir aussi » (projets MesInfos et MiData), alors qu'actuellement les clients savent de moins en moins ce que les entreprises savent d'eux.

Comme l'explique Daniel Kaplan, « cette idée s'inscrit dans le concept de *Vendor Relationship Management* (VRM) créé par Doc Searls pour équilibrer le *Customer Relationship Management* (CRM) », dont les dérives provoquent paradoxalement une chute de plus en plus forte de la fidélisation.

Pour Doc Searls, le seul endroit où le 360° est réellement possible, c'est du côté du client et le mouvement VRM veut poser les bases d'une relation client saine dans l'ère de l'industrialisation du numérique, « une personnalisation demandée remplaçant une personnalisation subie » grâce par exemple à des outils émergents visant à « outiller » le client et à assurer son *empowerment* face aux entreprises, comme les *Personal Data Stores* (MyDex, Privowny, personal.com...).

Mais à quoi ces données vont-elles pouvoir être « réutilisées » par les individus ? Daniel Kaplan évoque le mouvement de « quantification de soi » (*quantified-self*) : avec ses données de consommation, l'individu pourrait réfléchir à sa mobilité, à son empreinte carbone, enrichir son bilan de compétence, appliquer des mesures d'éco-responsabilité à sa consommation...

Ces initiatives sont globalement jugées positives, même si certains experts y voient un leurre. Ainsi, pour Antoinette Rouvroy, ces projets sont un peu naïfs s'ils font fi du profilage et des velléités d'anticipation. Pour Meryem Marzouki, le danger est de transformer le droit d'accès individuel en une sorte d'*Open Data* généralisé, permettant sur simple consentement l'accès de toutes les entreprises à des données transactionnelles détenues par les autres... ■

LA « DICTATURE » DES ALGORITHMES : DEMAIN, TOUS CALCULÉS ?

« Tout ce qui se passe aujourd'hui concernant les données à caractère personnel rejoint un mouvement général de « grammatisation ». Ce concept, inventé par Sylvain Auroux en 1995, évoque un processus de « discrétisation » c'est-à-dire un codage inventé par les individus en société par exemple par la création de l'alphabet, par le fait de compter sur ses doigts… Le numérique est un nouveau stade de la grammatisation. Le premier a été l'alphabet, le deuxième l'impression. Le troisième stade a émergé dans la révolution industrielle et la division du travail : la machine-outil à commande discrète a « grammatisé » le travail. Dans un quatrième stade, photo, cinéma et télévision ont grammatisé perception, ondes et comportements. Dans l'actuel cinquième stade de grammatisation numérique, tout devient porteur de grammaire numérique, ce qui se généralisera par l'Internet des objets. Le numérique est un nouveau milieu social, un nouvel espace public et un nouveau stade de l'écriture : on y produit des données. Il est aussi un troisième stade industriel, voire hyper-industriel : on industrialise, automatise même le rangement de sa bibliothèque. Chaque phase de grammatisation crée un processus inédit de prolétarisation, c'est-à-dire de privation du savoir qui est délégué au système. Ainsi, Platon expliquait déjà dans *Phèdre* que l'écriture pouvait produire de l'atrophie de la mémoire et être nuisible à l'homme en ne mettant plus en jeu l'oralité, la pensée en soi-même. La grammatisation industrielle a prolétarisé la production (fin de l'artisanat, des compagnons…). Dans la séquence de grammatisation précédente, analogique, c'est la consommation qui s'est prolétarisée, en accroissant la dépendance à la consommation de masse des individus. Aujourd'hui, ces processus existent également : par exemple, nous oublions les numéros de téléphone, ou les médecins font de plus en plus de diagnostics assistés par ordinateur. »

Bernard Stiegler

BIG DATA, SMALL DATA, CLOUD : LA NOUVELLE RÉVOLUTION DES DONNÉES ?

Le concept de *Big Data* est certainement l'un des thèmes les plus évoqués lors des entretiens par les experts s'exprimant sur les évolutions pouvant avoir le plus d'impact dans les 10 prochaines années. Encore flou et difficile à synthétiser, il peut s'articuler autour de trois V : il faut certes un facteur de *volume* important de données, mais ce seuil n'a de sens que si l'on y associe leur *variété* (de sources diverses…) et un facteur de *vélocité* du traitement. Des technologies offrant toujours plus de puissance de calcul, aisément *scalables* car hébergées sur le *Cloud* et permettant de traiter de nouveaux types de données notamment non-structurées, ont favorisé l'émergence d'une industrie qui pesait près de 700 milliards d'euros en 2011 (IDATE, *Cloud* et *Big Data*, mai 2012). Mais ce déluge des données est avant tout intrinsèquement lié à l'évolution des usages : les utilisateurs partagent une diversité toujours plus importante de contenus (photos, vidéos, billets de blog, micro-conversation, capteurs personnels) et le taux d'équipement en smartphones et tablettes progresse, favorisant encore davantage le partage de ces données. Pour Dominique Boullier, deux grandes nouveautés émergent autour de ces données disponibles et donnent du corps à la notion de *Big Data*, au-delà du traitement classique de *data-mining*. Tout d'abord, la donnée traitée n'est plus statique mais dynamique et en temps réel : « avant on suivait un état, aujourd'hui une pulsation à haute fréquence », comme le montrent les exemples de *yield management* qui changent les prix en temps réel. L'autre nouveauté, c'est la « facilité à changer d'échelle et de passer du *Big* au "micro/nano" Data que représente

l'individu ». Les statisticiens avaient pour habitude d'agréger les données et de traiter les agrégats, il est désormais possible de « zoomer » au sein de ces données pour s'approcher de l'individu. Une partie des enjeux porte bien sur cette frontière entre le niveau macro où les données sont agrégées et le raccrochement potentiel à un individu. On crée des profils, on impute aux gens des désirs et besoins qu'ils n'expriment à aucun moment et on prend le risque de les enfermer dans ces avatars comportementaux. C'est ce que souligne David Forest, pour qui le danger n'est pas dans les données statistiques prises de façon isolée, mais bien dans le recoupement de données en apparence anodines qui peut aboutir à un traitement discriminant. D'autant que l'algorithme qui traite ces données est « une boîte noire, comme la recette du Coca-Cola » si bien qu'il n'est pas possible de connaître la logique qui sous-tend la prise de décision.

Pour certains de nos experts, le caractère révolutionnaire du phénomène *Big Data* est cependant à relativiser. C'est notamment le point de vue que défend Daniel Kaplan, qui y voit plutôt le chant du cygne d'une « informatique productiviste, trop centrée sur une force brute pour mobiliser plus de données et de puissance de calcul ». Selon lui, le *Big Data* n'est pas suffisamment au service des individus et il préfère une forme de *Small Data* où il s'agirait d'outiller les individus pour qu'ils puissent exploiter eux-mêmes leurs propres données (voir « La donnée au cœur des modèles d'affaires : demain, tous traders de données ? », page 15). Pour Emmanuel Kessous, si le *scoring* se généralise, on prive l'individu de la liberté de choisir l'entreprise avec laquelle il souhaite avoir une transaction, pour offrir cette liberté de choisir (son client) à l'entreprise.

TOUS GOUVERNÉS PAR DES ALGORITHMES ?

C'est la thèse d'Antoinette Rouvroy qui livre un regard critique sur ces dispositifs de prise de décision automatique et en particulier sur les algorithmes qui les gouvernent. Selon elle, ils structurent *a priori* le champ d'action possible des individus et incarnent une nouvelle « gouvernementalité algorithmique » : il faut comprendre le *Big Data* comme s'insérant « dans le contexte global du capitalisme ...

informationnel », au sein duquel on survalorise le caractère prédictif des données. On y trouve une forme de règne de la prise de décision automatique alors que la machine ne peut pas tout prendre en compte, notamment les causes.

On passe alors « du déductif à un inductif purement statistique en ne retenant que ce que l'on peut mesurer, dans une sorte de réductionnisme informationnel ». Tout ce qui passe par la conscience humaine devient de fait suspect, et certains pans de la réalité nous échappent car ce qui n'est pas mesurable n'existe plus. Le *Big Data* favorise le « comportementalisme numérique » permettant d'anticiper des comportements, des appartenances, de classifier les personnes en fonction des risques et opportunités qu'elles présentent sans plus avoir à les faire comparaître, à les entendre. C'est donc à une forme de « personnalisation » ambivalente que nous avons affaire : le *data-mining* et le profilage permettent de mieux cibler la surveillance, les contrôles, d'individualiser les offres de service, d'information, mettant le citoyen, le consommateur, l'utilisateur, « au centre » des dispositifs, tout en ne lui donnant plus l'occasion de faire entendre quelles sont ses intentions, ses désirs, ses motivations, ses préférences, inférés automatiquement par les dispositifs numériques. Pour la prise de décision, ces technologies tendent à dispenser de l'interprétation et de l'évaluation humaine, ainsi que du débat public concernant les critères de mérite, de besoin, de désirabilité, de dangerosité, de justice et d'équité au profit d'une gestion opérationnelle en temps réel, systématique plutôt que systémique, des situations. Dans un tel contexte, « une vision et une démarche éthique des TIC sont donc plus que nécessaires » (Antoinette Rouvroy).

Yves Poullet souligne également que la « réduction » de la personne est de plus en plus forte : « L'individu est aujourd'hui réduit à ses données et à des construits faites à partir de ces données, les "profils", des avatars algorithmiques. C'est une construction statistique dangereuse des personnes. »

Pour Henri Verdier, ce sujet renvoie à une sorte d'« euphémisation des pouvoirs » semblable à celle perçue par Michel Foucault dans son analyse de la biopolitique. Si avec la naissance de la CNIL, les enjeux étaient le recueil de données pour de mauvais usages, aujourd'hui c'est l'interopérabilité qui est la nouvelle question centrale. Le traitement statistique permet de brasser des informations qui ne sont pas intrinsèquement personnelles : « elles parlent des gens sans être nominatives ». Les sciences autour des données vont progresser et on ne fera plus le détour par l'identification ou par l'espionnage du sujet (comme connaître son orientation politique). Si le pouvoir devient totalement abstrait, invisible, statistique et probabiliste, alors la protection des libertés devrait peut-être le devenir.

Pour Antoinette Rouvroy, le *data-mining* et le profilage peuvent être encadrés, en immunisant certains secteurs — ceux dans lesquels les théories de la justice auxquelles nous adhérons collectivement exigent que les critères de mérite, de besoin, de désirabilité, de dangerosité... soient délibérés collectivement et démocratiquement — et en incluant la gestion des traces numériques dans les enjeux relevant de la responsabilité sociétale des entreprises. Celles-ci pourraient ainsi s'intéresser à la minimisation de leur impact sur l'environnement informationnel dans « une approche comparable à celle qui prévaut concernant le respect de l'environnement ». ■

GÉOLOCALISATION : OÙ ALLONS-NOUS ?

« La géolocalisation est une donnée pour laquelle il est nécessaire d'avoir l'autorisation de l'individu et qui est vraiment très intéressante au niveau économique. Elle permet notamment à de nombreux petits commerçants de mettre en avant leurs produits. Mais il faut sensibiliser les gens à l'importance de ces données. Les sociologues travaillent d'ailleurs actuellement sur la notion de géolocalisation et essaient de comprendre ce phénomène du point de vue de l'utilisateur : pourquoi les gens se géolocalisent-ils ? »

Christine Balagué

LE BOOM DES SERVICES BASÉS SUR LA GÉOLOCALISATION

La plupart des experts rencontrés ont insisté sur l'exceptionnelle rapidité de l'adoption des services utilisant la géolocalisation : ces usages se sont répandus à un rythme inédit même pour le numérique, essentiellement par la généralisation des smartphones (environ 75% des téléphones mobiles vendus en 2012 en France). En quelques dizaines de mois, la proportion de Français utilisant plus ou moins régulièrement un service nécessitant la géolocalisation est devenue extrêmement importante et, à la question du CREDOC « Souhaiteriez-vous avoir la possibilité d'interdire la transmission de votre localisation à des entreprises commerciales ?», 81% des utilisateurs de mobiles répondaient « oui » fin 2011 (voir encadré page 22).

Cet engouement peut s'interpréter de plusieurs manières : avant tout, les services localisés sont si pratiques que bien souvent « les essayer c'est les adopter ». Si l'expression à la mode en 2011 pour qualifier les impératifs des services « gagnants » du e-commerce, SoLoMo (pour Social — Local — Mobile) place le « local » au centre de sa dynamique, ce n'est pas pour rien : la géolocalisation est vue comme un graal par beaucoup de spécialistes de e-commerce, car elle permet d'accroître la pertinence des propositions et recommandations.

Qui plus est, sa dimension ludique est réelle : Dominique Cardon note ainsi que nombreux sont ceux qui se localisent dans des lieux festifs ou branchés (bars...) pour finalement « se mettre en scène » mais aussi « pour créer du conversationnel » autour d'un thème, d'un lieu, d'une expérience... « un peu comme sur les réseaux sociaux » (voir « La révolution du web social : demain, tous des *peoples* ?», page 12).

Mais il faut aussi garder à l'esprit une vision plus réenchantée de ces technologies, comme nous l'a rappelé Alain Bensoussan : « La géolocalisation est en effet une expérience au quotidien de la fusion maintes fois annoncée du « monde réel et du monde numérique », puisqu'elle impose à notre esprit une fusion et une synchronisation de ces deux réalités, la physique et la numérique, le monde des octets et le monde des molécules : « elle permet le droit à l'existence dans les deux mondes, d'y être simultanément présent, de vivre en modes synchrone et asynchrone en même temps. »

SIGNAL FAIBLE : DEMAIN, DEVRA-T-ON ACCEPTER LA GÉOLOCALISATION PERMANENTE POUR ACCÉDER À DES SERVICES MOBILES ? L'EXEMPLE DE « GOOGLE NOW »

Un conseil courant pour se prémunir contre des abus de collecte de la géolocalisation est de n'activer cette fonction que lorsqu'on s'en sert, par exemple lors d'une recherche d'itinéraire. Ce conseil sera-t-il toujours applicable demain ? Outre le manque de clarté et de simplicité des réglages du téléphone, certains services innovants demandent une géolocalisation permanente pour optimiser leur fonctionnement. C'est le cas de la fonctionnalité « Google now », intégrée dans la version 4.1 du système d'exploitation pour mobile Android de Google. « Google now » se veut un assistant personnel « prédictif » dont le slogan est un peu de répondre à vos questions avant que vous ne les posiez. Ainsi, connaissant vos habitudes quotidiennes de transport, il affiche une notification vous indiquant quand vous devez partir pour arriver à l'heure à un rendez-vous en fonction de votre lieu actuel. Le service a donc « besoin » pour améliorer sa précision que la localisation soit non seulement captée au moment utile, mais en réalité en permanence (pour apprendre vos habitudes de trajets, de modes de transport…). Comment alors s'assurer demain du devenir de ces « graphes de localisation » permanents ?

La situation est-elle pour autant stable sur ce sujet ? Si le GPS existe depuis un certain temps, il ne faut pas oublier que ces services plus « riches » sont jeunes. Nicolas Nova, pense qu'il faut admettre que le domaine est toujours en phase de maturation, autour de 3 types d'usages : proposer des publicités plus ciblées en fonction de sa localisation, savoir où se trouvent ses amis et relier un message ou un commentaire au lieu où on se trouve. Or beaucoup de ces usages peuvent rapidement dépasser ce qui est « acceptable » par les utilisateurs.

ÊTRE GÉOLOCALISABLE VA-T-IL DEVENIR LA NOUVELLE NORME ?

La géolocalisation est donc passée selon nos experts en quelques années d'un acte exceptionnel à un acte quasi-quotidien. Est-elle pour autant devenue anodine ? Selon Nathalie Mallet-Poujol, les comportements nouveaux qui entourent l'émergence et maintenant la généralisation de la géolocalisation ludique se traduisent par un degré d'acceptation plus important de ces technologies par les individus.

Être géolocalisé devient plus banal, même si les utilisateurs seraient certainement gênés d'apprendre à quel point ces données peuvent être facilement transmises à certains acteurs (voir encadré ci-contre).

Demain, la géolocalisation ne sera peut-être plus du tout intermittente mais permanente car les services « innovants » exigeront cette permanence (voir encadré). Pour Paul-Olivier Gibert, « d'ici 3 ou 4 ans, on sera quasiment obligé de se géolocaliser pour bénéficier de certains services (taxis…). Or le problème n'est pas tellement dans la donnée "instantanée" que dans l'accumulation et l'historisation, la trace de ces données. Ce qui n'est pas, en soi, une information très sensible, le devient dès lors qu'elle permet des recoupements ». Francis Jauréguiberry y voit même une possible prochaine étape de l'injonction de connexion : « Aujourd'hui, le fait d'être déconnecté et de ne pas répondre immédiatement à son portable nécessite de plus en plus souvent des explications et relève finalement de la justification. Sans que personne ne l'ait

vraiment décidé, la norme sociale tend vers la connexion permanente. Il semble que nous empruntions le même chemin pour la géolocalisation et l'on peut sans peine imaginer que refuser d'être géolocalisé apparaisse d'ici peu comme asocial voire suspect. Asocial, car la ville intelligente ne fonctionne par exemple que si chacun accepte que ses traces individuelles de localisation soient traitées pour le bien commun. S'y opposer risque de devenir synonyme d'incivilité. Suspect, car dans un environnement où la norme deviendrait la géolocalisation généralisée, s'y refuser entraînerait immanquablement soupçons et suspicions.»

La géolocalisation et surtout peut-être l'historique dans le temps de nos localisations deviendront alors particulièrement sensibles outre le fait qu'il est très difficile de les anonymiser comme le montrent les travaux de Sébastien Gambs (chercheur à l'IRISA) car il sera très facile d'en déduire des événements et habitudes de vie. Une série de données spatio-temporelles de qualité sur une personne peut permettre d'inférer par exemple ses lieux d'habitation et de travail, son identité, ses centres d'intérêts, ses habitudes... voire une déviation par rapport à son comportement habituel.

Avec la géolocalisation permanente, il sera demain de plus en plus difficile de sanctuariser cette donnée sensible : si elle est captée, enregistrée, elle pourra être diffusée, stockée «dans les nuages», transmise à des tiers, représentant un immense défi pour la protection de la vie privée. Mais la géolocalisation *pervasive*, comme elle commence à l'être, ouvre aussi des perspectives fascinantes aux chercheurs, par exemple autour de ce que Nicolas Nova appelle «la cartographie des passages», par laquelle il est permis maintenant de penser à la cartographie dynamique des flux de la ville. ■

BIOMÉTRIES : LE NOUVEAU SÉSAME ?

« Il y a une tendance lourde et historique en matière de fichage depuis le « bertillonnage » : celle d'un fantasme identificatoire de la population par la rationalisation scientifique. Les logiques de fichage s'ancrent toujours dans des pratiques qui visent à discriminer, à catégoriser. Sur les dix dernières années, un saut technologique s'est accompli avec la biométrie, les puces RFID, les systèmes de géolocalisation : ces technologies vont plus vite que l'environnement juridique, le retard du droit est donc croissant. Or, les effets du 11 septembre 2001 ont donné un coup d'accélérateur à la problématique du fichage policier, en favorisant un mode de gouvernance par la peur, l'inquiétude. Des franges de la population de plus en plus larges sont dès lors concernées par le traçage. Déjà, à l'époque de Bertillon, ce dernier souhaitait travailler sur les récidivistes, puis cela a été élargi aux fous, aux nomades et ensuite à tous les délinquants. Cette finalité de populations ciblées avec ensuite une extension de plus en plus large suit toujours le même processus, qui tend *in fine* à faire de chacun un suspect. Avec le passeport biométrique et le projet de carte d'identité biométrique, chacun est rendu transparent aux yeux de l'État. »

Pierre Piazza

Citée par plusieurs experts comme faisant partie des tendances lourdes pour les dix prochaines années, la biométrie reste encore assez peu utilisée dans la vie quotidienne, hors des usages de souveraineté (documents d'identités et fichiers de police). Cependant, l'émergence de la reconnaissance faciale et vocale dans des produits ou applications grand public (smartphones, réseaux sociaux...) est peut-être le signal d'une plus grande présence de la biométrie dans la vie quotidienne. Comme le souligne Yann Leroux, le rapprochement des technologies et du corps humain est peut-être l'enjeu majeur pour après-demain.

LE MYTHE DU CORPS COMME MESURE DE L'IDENTITÉ

La biologisation de l'identité est pour Pierre Piazza une tendance lourde et ancienne pour les États. L'idée que le corps est un identifiant n'est pas neuve. Cependant, aujourd'hui, elle se double d'une nouveauté : « le corps comme mot de passe » (Antoinette Rouvroy). On voit ainsi l'hypothèse de la validation du paiement par empreinte digitale ressurgir régulièrement, tout comme des tentatives, peu couronnées de succès pour le moment, d'utiliser la biométrie en contrôle d'accès pour des produits grand publics. Selon Antoinette Rouvroy, la force de ce mythe naît dans « la présomption que le corps ne ment pas ». Pour Jérémie Zimmermannn, ces nouvelles formes d'identification, non révocables et qui échappent au contrôle de l'individu, comportent des risques spécifiques.

Mais, comme le souligne Dominique Boullier, les données biométriques sont dépendantes de la technologie et ce sont des données à caractère biologique qui ne disent finalement pas grand chose de l'identité sociale. La donnée brute biométrique n'a aucun sens seule, mais on tend à tomber dans le piège de l'illusion de garantie biologique. Cette croyance en des références biologiques qui donnent plus de garanties est assez typique d'une vision scientiste qui paraît impossible à mettre en doute. Le risque est alors de « biologiser » des identités alors qu'il s'agit d'un montage, d'une fiction de garantie biologique : il y a un chaînage de référence entre le corps et la donnée, et donc même dans ce cas, il y a un code, un référent, une chaîne, une institution, et pas une donnée « objective ».

QUELLE ACCEPTABILITÉ SOCIALE DE LA BIOMÉTRIE ?

Les traitements de données biométriques sont considérés comme comportant des risques spécifiques d'atteinte à la vie privée et aux libertés et sont soumis de ce fait, en Europe, à un encadrement particulier (en France, un régime d'autorisation). Mais,

paradoxalement, les citoyens semblent peu conscients de ces risques et, excepté quelques mouvements associatifs, affichent au mieux de l'indifférence, au pire une certaine fascination. Pierre Piazza relève que la population est en général d'une grande passivité et fait preuve d'accoutumance à ces technologies, notamment par manque d'information, et à cause du discours de légitimation qui est fait par les industriels. Les jeunes, quant à eux, semblent ne pas s'intéresser spontanément à ces questions. Peu d'études ayant été publiées sur ce point, un état des lieux reste à faire sur le réel niveau de perception, au-delà de l'acceptation, de ces technologies par la population.

Pour Christine Balagué, il y a d'abord un enjeu de « compréhension, au-delà de l'acceptation sociétale ». Une étude européenne de l'Institut pour les études de prospective technologique a montré, en 2005, que ces techniques d'identification sont source de fascination mais qu'il existe aussi une méconnaissance totale des individus sur ces sujets. Le fait que la biométrie ne soit pas encore très présente dans leur quotidien l'explique sans doute en grande partie. Ce que Dominique Cardon résume en indiquant que lorsqu'on questionne des individus lambda sur leur vision de la biométrie, on les interroge plus, finalement, sur leur fascination pour les films de science-fiction que sur leur quotidien et leur vécu... De même, le fait qu'avec la biométrie — comme d'ailleurs aussi avec le « sans contact » — l'impression de « donner » de la donnée soit amoindrie compte tenu des possibilités de capture automatique, ne facilite sans doute pas l'appréhension par le grand public de ces techniques. Pour Nathalie Mallet-Poujol, la biométrie — comme d'ailleurs les nanotechnologies — est davantage subie et pourra d'ailleurs de plus en plus se faire à l'insu de la personne.

Meryem Marzouki, tout en observant que *via* la vidéosurveillance et la biométrie (par exemple dans les cantines scolaires) le contrôle social s'étend aussi aux déplacements et même aux corps, souligne que le plus étonnant est certainement de constater que cette logique de contrôle social est acceptée, voire appropriée par les individus pour des raisons de confort ou de sécurité. Pour Alain Bensoussan, il faut d'ailleurs changer de paradigme et « libérer la biométrie », que chacun puisse utiliser des données biométriques sans autorisation pour des raisons de confort ou de sécurité, mais avec des protections : « L'individu doit par exemple pouvoir décider lui-même de payer avec son doigt si cela lui facilite la vie. »

RECONNAISSANCE FACIALE : LA MENACE MAJEURE ?

Photos et images sont devenues omniprésentes dans le monde numérique, en particulier grâce aux smartphones et aux réseaux sociaux (300 millions de photos sont publiées chaque jour sur Facebook, d'après les résultats du 1er trimestre 2012 du réseau social). Les outils de « *tagging* » (étiquetage) et d'identification automatique des photos se généralisent. Comme le souligne Stefana Broadbent, on communique de plus en plus avec les photos et de nouveaux genres communicationnels se créent. Le post et surtout le « taggage » et « détaggage » des photos est devenu un geste social important très intéressant à analyser (« le fais-je ou pas ? » et pour quelles raisons ?). Ainsi, selon l'étude *Pew Internet « Privacy management on social media sites »* de février 2012, 37% des utilisateurs américains de réseaux sociaux ont « détaggué » une ou des photos en 2011. Ils n'étaient que 30% à le dire en 2009. Il serait utile d'avoir une vision plus complète des comportements et usages réels des utilisateurs. Appliquent-ils des règles particulières aux choix des photos publiées, à leur accessibilité, au « taggage » de personnes ? Et ce pour les différents types de photos (photos de profil, photos personnelles...) ? Comment conçoivent-ils le respect de l'intimité de leurs proches et amis ? De quelle façon assurent-ils les droits des tiers ?

Autre axe de réflexion : ces technologies de reconnaissance faciale voire vocale sont-elles reproductibles (*scalables*) au niveau du web ? Dans un avenir proche, peut-on imaginer que la reconnaissance faciale soit possible sur l'ensemble des photos disponibles sur le web ?

Pour Dominique Cardon, ces évolutions technologiques autour de la photographie sont la menace absolue : la reconnaissance faciale transforme l'image en texte, en code et finalement en un identifiant, tout en ôtant le contexte (voir « Identité(s) numérique(s) : tous authentifiés ?», page 38). Et Yves Deswarte souligne que la reconnaissance faciale étant aujourd'hui très facile, les photos deviennent donc des données biométriques. Il serait facile de tenter d'en extraire automatiquement des informations sensibles, par exemple ethniques ou de localisation.

VIDÉOSURVEILLANCE ET ANALYSE COMPORTEMENTALE

La vidéosurveillance se banalise et explore, elle aussi, de nouvelles pistes comme celle du *Big Data* et des outils d'analyse algorithmique pour détecter les comportements « suspects ». Ainsi, de nombreux projets de recherche comme DAS (projet de la police de New York) ou INDECT au niveau européen se développent. Laisser des systèmes automatisés définir ce qui est suspect et ce qui ne l'est pas ne va pas sans poser de graves questions éthiques. Pierre Piazza s'interroge dans ce contexte sur ce que deviendra l'anonymat au sein de l'espace public dans l'avenir : « Il tendra à disparaître, si l'individu est confronté à la fois à la biométrie banalisée, fonctionnant "à la volée", à la vidéosurveillance et à la géolocalisation. » ■

NANOTECHNOLOGIES, GÉNÉTIQUE, NEUROSCIENCES, « HOMME AUGMENTÉ » : QUELLES VISIONS POUR L'HUMANITÉ DE DEMAIN ?

« Les nanotechnologies suscitent une sorte de fascination parce que "l'on met de l'intelligence dans des objets". En fait, on confond intelligence et interaction. Les nanotechnologies risquent d'être à l'origine d'une perte d'autonomie de l'individu sur son environnement. L'exemple du GPS est révélateur : la vision anthropomorphique de l'ordinateur conduit à dire que celui-ci est plus fort que le cerveau humain. »

Dominique Wolton

Le développement et la convergence des biotechnologies, des sciences du cerveau, des nanotechnologies et de l'intelligence artificielle annoncent-ils une transformation radicale de l'humanité ?

LA « WEBIFICATION » DU MONDE RÉEL

La baisse continuelle du coût des puces RFID favorise l'émergence d'un « Internet des objets ». Les objets connectés (voiture, télévision, maison équipée en domotique, « réseaux intelligents »...) vont se multiplier. Si de nouveaux services en résultent, cette évolution sera aussi à l'origine de nouveaux risques pour la vie privée des usagers, conclut Henri Verdier. Des données très intimes, transmises directement par les objets en fonction de leur utilisation, seront créées et diffusées. Pierre-Jean Benghozi ajoute que les traces d'activité ainsi créées pourront aisément être « désanonymisées », au risque de dévoiler le mode de vie des usagers et de servir à leur profilage. Elles pourraient aussi être détournées à des fins d'espionnage industriel (par exemple, les entrées et sorties de camions d'un lieu de production, dévoilées par des puces RFID, seront autant d'indices de son activité). Pour Françoise Roure, les nanotechnologies ne porteront atteinte à la vie privée que si nul n'y prend garde, en particulier si elles donnent naissance à des outils miniaturisés, invisibles, de traçage et de surveillance en continu des personnes.

Comment se prémunir contre la mise en place d'une société de surveillance généralisée, contre les *small* et autres *nano Brothers* ? Jean-Marc Manach répond que le principe de précaution doit jouer pour éviter que le recours aux nanos ne soit subi ou rejeté. C'est dans cette logique que l'Union européenne a demandé que les nanos fassent l'objet d'une étude d'impact sur les libertés. L'essentiel, pour Jean Frayssinet, est que les consommateurs se voient reconnaître le droit de bloquer et désactiver à tout moment les dispositifs RFID fixés sur les objets qu'ils utilisent. Sans cela, un équilibre ne pourra pas être trouvé entre l'intérêt du commerçant et les droits du client qui doivent constituer une frontière infranchissable. La prise en compte de règles de protection des données dès la conception d'un service devrait, à cet égard, être à l'avantage des entreprises européennes (voir « Innover dans la régulation », page 50).

LA GÉNÉTIQUE ET LES NEUROSCIENCES AU SERVICE DES LOGIQUES PRÉDICTIVES

Arnaud Belleil insiste sur les graves atteintes aux libertés qui pourraient naître si l'ADN devait être utilisé dans des logiques économiquement rationnelles qui seraient comparables aux analyses statistiques des concepteurs de scores des organismes financiers. D'ici 2020, le domaine des données

génétiques va aussi constituer un « champ de bataille » considérable (médecine prédictive, assurances, traitement automatisé de l'ADN...) auquel les acteurs de la régulation et les citoyens ne sont pas du tout préparés. De leur côté, les neurosciences sont de plus en plus utilisées, par exemple aux États-Unis pour évaluer la responsabilité et la dangerosité des prévenus. Plus généralement, la rapidité avec laquelle les sciences du cerveau s'insinuent dans la société est frappante. D'ores et déjà, on parle de neuro-économie, de neuro-marketing, de neuro-informatique, de neuro-psychanalyse, de neuro-justice... Le tout, parfois, dans un contexte idéologique de réductionnisme biologique des comportements et de défiance vis-à-vis de tout ce qui passe par la conscience humaine.

C'est ainsi que les neurosciences du consommateur explorent les actions de la vie quotidienne, les habitudes domestiques et les décisions d'achat des consommateurs afin de chercher à comprendre les processus mentaux qui entrent en jeu dans les décisions de consommation, puis de les utiliser en complément des outils classiques du marketing.

LA TENTATION DU CYBORG

Les idéologies post-humanistes voient la technologie comme un vecteur de rupture. Elles affirment que l'humanité doit s'ouvrir au non humain (clones, objets « intelligents »...) pour que l'espèce humaine perde son privilège au profit de nouveaux individus, façonnés par la technologie. Dans la même logique, les transhumanistes militent pour une amélioration de la condition humaine (élimination du processus de vieillissement, amélioration des potentiels humains...) grâce aux biotechnologies. Aux États-Unis, un vaste programme de recherche, doté de plusieurs milliards de dollars, est consacré depuis plusieurs années à l'approfondissement de la convergence entre quatre voies technologiques, pour permettre à l'homme de faire mieux que la nature : les biotechnologies ouvriraient la voie vers la post-humanité, avec l'appui des nanotechnologies, des technologies de l'information et des sciences cognitives. Ce programme est perçu par certains comme la première pierre vers le transhumanisme, lui-même étant compris comme une étape intermédiaire vers le post-humanisme.

Pour Arnaud Belleil, le passage est étroit entre l'homme « réparé » et l'homme « augmenté ». Bientôt, il sera possible d'intégrer des technologies (puces électroniques dans le cerveau pour renforcer la mémoire, caméra oculaire, exosquelettes intelligents...) dans le corps. Ces appareils seront-ils choisis ou imposés ? Serviront-ils à l'autonomie, à l'épanouissement de l'individu ou à sa surveillance ? Il serait bon de poser des garde-fous sans attendre.

LA RAPIDITÉ DES INNOVATIONS : UN RISQUE DE RUPTURE SOCIALE ?

Bernard Stiegler l'avait déjà dit il y a plus de quinze ans : « La rapidité avec laquelle les innovations contemporaines se succèdent ne laisse aucun répit, d'où une désorientation sociale et psychologique sans précédent dans l'histoire. » Le rythme du changement étant de plus en plus rapide, Yves Poullet et Cécile de Terwangne craignent que l'adaptation de la société ne puisse plus se faire après un temps de réflexion, que les individus deviennent les outils et les acteurs du fait accompli, que le temps de la réflexion n'existe plus et que les changements technologiques deviennent de plus en plus imprévisibles. Contester et anticiper restent-ils encore possible ? Ou bien ne reste-t-il plus qu'à s'ajuster et à accompagner ? Ne faudrait-il pas faire sortir l'innovation des laboratoires et organiser sa discussion sur la place publique, puisque c'est la vie quotidienne des citoyens qui est en jeu ? Pierre Piazza insiste, pour sa part, sur le fait que les innovations technologiques vont plus vite que l'environnement juridique. Le retard du droit serait donc croissant. ■

GOOGLE CRÉE UN « CERVEAU INFORMATIQUE »

Google vient de créer un « cerveau informatique », un réseau de machines « intelligentes » constitué de 16 000 processeurs. Le New York Times a annoncé en juin 2012 que ce réseau de neurones artificiels avait « réinventé » le concept de chat au vu d'une base de 10 millions de vidéos de chats mises en ligne. Une seule consigne lui avait été donnée : apprendre par soi-même. Même si ce réseau semble bien réduit par rapport au cortex visuel humain, c'est la première fois qu'un logiciel apprend automatiquement à utiliser les données qui lui ont été confiées.

0.2

Partie 0.2

QUEL NOUVEAU PAYSAGE POUR LES DONNÉES PERSONNELLES, LES LIBERTÉS ET LA VIE PRIVÉE ?

TOUT DEVIENT-IL DONNÉE PERSONNELLE ?

« On ne parle plus désormais de données personnelles, mais de données relationnelles et de données transactionnelles. Il faut sortir de la vision des « données personnelles » comme une propriété et une chose bien définie. Sinon, on évoque un domaine fermé. Or, même une pièce d'identité est transactionnelle. C'est le cas aussi des données du mobile, des données bancaires. Toutes les données sont relationnelles ou transactionnelles. Parler de « donnée personnelle » donne l'impression qu'il s'agit d'un attribut de la personne. Les données transactionnelles sont, quant à elles, une « entre-prise » : par exemple entre la personne d'une part et une institution d'autre part. Les données transactionnelles donnent prise aux autres. C'est ce que j'appelle l'habitèle : nous ne possédons pas des données, nous les habitons, tout comme nos habits, nos habitats, l'habitacle de notre voiture. On considère qu'on laisse des traces, mais tout cela constitue un ensemble, une enveloppe grâce à l'interopérabilité des données. Nous sommes donc « enveloppés » comme dans un habitat. Comment pilote-t-on cette enveloppe et sa porosité ? Dire qu'il faut « protéger les données personnelles » sous-entend « créer une bulle », ce qui est contraire à la notion de transaction, de relation. L'habitèle ne se pilote donc que dans la relation. Il faut donc faire émerger l'idée d'une situation de co-fragilité, comme par exemple sur les réseaux sociaux. Cette réciprocité est le contraire des concepts de « maître du fichier » et permet alors la relation et la transaction. Les définitions des données personnelles et de la vie privée sont, quant à elles, des fictions inopérantes. »

Dominique Boullier

L'IMPOSSIBLE DÉFINITION DES « DONNÉES PERSONNELLES »

Tous les entretiens menés ont eu un point commun : ce qui peut paraître comme le point de départ obligatoire et la question la plus simple de la réflexion, à savoir la définition de la notion de données personnelles, s'est révélée être un véritable casse-tête. En réalité, définir la notion de données personnelles simplement et efficacement a paru à beaucoup d'experts comme une perte de temps voire une impasse. À tel point qu'il est devenu légitime de se demander si la notion de « données personnelles » n'est pas une notion en fin de vie.

En réalité, elle paraît si mouvante, mobile, évolutive et, pour tout dire, subjective, que si l'on ne peut faire l'impasse de son utilisation, il paraît contre-productif de vouloir la figer : les données personnelles sont tout simplement de plus en plus subjectives, relatives, et contextuelles.

Par exemple, pour Christine Balagué, la donnée personnelle intéressante en termes de marketing change. Sur les réseaux sociaux il peut s'agir de données de la vie quotidienne : ce que j'ai fait, ce que j'écoute... et non plus seulement de données de qualification (je suis un homme ou une femme de tel âge vivant à tel endroit).

Les objets connectés (télévision connectée, voiture connectée...) et l'Internet des objets posent à cet égard des problèmes radicalement nouveaux, encore peu discutés aujourd'hui, concernant la captation et l'exploitation de données triviales, voire insignifiantes par elles-mêmes, mais susceptibles de contribuer à un profilage très fin des individus, et de produire à leur propos un « savoir » (probabilistique plutôt que de certitude) de leurs propensions personnelles et intimes, de leurs croyances religieuses, de leurs opinions politiques, de leur orientation sexuelle, de leur mode de vie et de bien d'autres aspects de leur vie personnelle et intime.

À côté des données personnelles « classiques », il faut donc s'intéresser à d'autres données, par exemple celles que Jean Frayssinet appelle des « données personnalisées », comme les adresses IP utilisées pour créer des profils qui sont des identités anonymes au sens strict mais qui au final définissent bien une personne. Ces identités anonymes permettent en effet « de viser juste et posent la question du contrôle sur l'assemblage et le profilage ». Finalement l'identité réelle importe assez peu dans ce contexte.

ADRESSES IP, ADRESSES MAC, UDID : IDENTIFIÉS ET TRACÉS PAR NOS MACHINES

Après plusieurs années, le débat sur le caractère identifiant de l'adresse IP semble tranché définitivement : pour Yves Deswarte, cette question ne se pose plus quand il s'agit d'un particulier : « Avant, les adresses IP étaient dynamiques, maintenant l'adresse IP est fixe dans la majeure partie des cas. Cela résout le débat : l'adresse IP est bien une donnée identifiante. » Jérémie Zimmermannn défend la même position, rappelant que la Cour de Justice de l'Union européenne a estimé en 2011 que l'adresse IP était une donnée personnelle (affaire Scarlet Extended vs SABAM). Aujourd'hui, cette analyse peut s'étendre à d'autres numéros identifiants uniques des machines comme les adresses MAC (identifiant physique stocké dans une carte réseau) ou l'UDID des iPhones qui sont, eux aussi, des repères très efficaces pour suivre des utilisateurs : il arrive que le meilleur moyen de suivre un individu soit de suivre ses appareils.

Selon Christine Balagué, les dix prochaines années seront marquées par la « multiplication des données récupérables et collectées et leur mise en relation cartographique, par exemple avec des outils de graphes sociaux ». Ce qui placera certainement pour elle au centre des attentions la question de la standardisation des formats de récupération de données.

UN AVENIR OÙ TOUT EST « DONNÉE À CARACTÈRE PERSONNEL » ?

En réalité, la tendance semble plutôt être à la facilité croissante de ré-identifier des personnes même au sein de jeux de données supposés anonymisés. Ainsi, pour Daniel Le Métayer et Claude Castelluccia, c'est la capacité à combiner les données qui change tout : « N'importe quelle donnée peut devenir identifiante une fois combinée "à d'autres" ? Par exemple, la combinaison du code postal et de la date de naissance peut souvent permettre d'identifier une personne. On peut donc dorénavant inférer une donnée sensible de données qui ne le sont pas. Au-delà de l'identification, se pose la question de la constitution de profils, qui peut conduire à de fortes discriminations dans tous les domaines d'activités. »

En effet, pour Pierre-Jean Benghozi, tout traitement un peu sophistiqué de traces de ce type peut aboutir à « désanonymiser » les données, comme l'ont prouvé des expériences comme celle réalisée sur les acheteurs de vidéos chez Netflix par Arvind Narayanan et Vitaly Shmatikov, ou encore celle de Latanya Sweeney. En 1997, cette dernière, doctorante du MIT, parvint à retrouver les données de santé du gouverneur de l'État au sein des données anonymes publiques en utilisant d'autres données ouvertes (lui permettant de définir son âge, code postal et sexe).

C'est ce que Paul Ohm a résumé dans un article publié en 2010 sous le titre « Promesses non tenues concernant la vie privée : réagir au surprenant échec de l'anonymisation » : la confiance dans le pouvoir protecteur des techniques d'anonymisation a certainement été surévaluée. Si des techniques statistiques permettent de désanonymiser facilement des individus, alors il faut cesser de faire passer la limite centrale de nos réflexions entre les données directement et indirectement identifiantes.

Comme l'a résumé Yves Poullet, « d'un point de vue anthropologique, nous ne sommes plus face à un problème de protection des données sensibles mais dans une problématique de quadrillage à partir de données triviales ». Il devient donc beaucoup plus difficile de classifier la donnée elle-même, isolée, en fonction de sa sensibilité (voir « De nouvelles données sensibles ? », page 34). Que se passera-t-il demain si ces données triviales se multiplient comme l'évoquent les analystes en parlant du *Big Data* ? D'autant qu'avec ce qu'Antoinette Rouvroy appelle « l'ubiquité croissante des dispositifs », il devient de plus en plus difficile d'isoler un système pour mesurer ses risques : « On a moins affaire à des artefacts localisés qu'à des logiques de partage, de circulation de données. Dans un tel contexte, c'est à la fois la trajectoire et les significations potentielles de "ses" données qui échappent à l'individu. »

À l'horizon des prochaines années, l'avènement de l'Internet des objets transformera peut-être tout objet communiquant en un producteur potentiel de données à caractère personnel par croisement, mélange, analyse, computation. Il y aura certes toujours une gradation : certaines données sont plus ou moins identifiantes. Mais le monde des données personnelles et des traces devrait grandir au moins aussi vite que le monde des données en général, c'est-à-dire à une vitesse exponentielle. ■

DE NOUVELLES DONNÉES SENSIBLES ?

« Avant, les données sensibles étaient une partie des données à caractère personnel. Aujourd'hui, potentiellement, même des données à caractère non personnel peuvent devenir sensibles grâce au *data-mining*, dans la mesure où elles sont très révélatrices de notre mode de vie [...] ; le comportementalisme numérique peut permettre d'anticiper des comportements, des appartenances, de classifier les personnes dans des catégories vulnérables. »

Antoinette Rouvroy

Qu'entend-on par données sensibles ? Au regard des lois européennes de protection des données personnelles, ce concept définit certaines catégories de données considérées comme présentant des risques spécifiques d'atteinte à la vie privée et aux libertés, voire à l'identité humaine, et qui, de ce fait, bénéficient d'un statut particulièrement protecteur. Origines raciales ou ethniques, opinions politiques, syndicales ou religieuses, santé, vie sexuelle, infractions, condamnations, identifiant national sont ainsi placés sous un régime d'encadrement strict. Comme le rappellent nos experts, notamment Philippe Lemoine et David Forest, la notion de donnée sensible renvoie plus fondamentalement à des préoccupations historiques. Ainsi, si la religion et la race sont incluses dans les données sensibles, c'est parce que la loi de 1978 puise ses racines dans l'Histoire, notamment celle concernant le fichage des populations juives françaises pendant l'Occupation. Pour Olivier Iteanu, les données sensibles correspondent surtout à des valeurs, à l'histoire du pays. De ce fait, comme le rappelle Dominique Desjeux, il y a bien évidemment de grandes différences entre les pays selon les cultures : ainsi, aux États-Unis, on parle facilement de race ou de religion, ce qui n'est pas le cas de la France. Et comme le souligne Jean-Marc Manach, le débat français sur les statistiques ethniques comme les difficultés parfois rencontrées par les chercheurs pour mener à bien leurs études illustrent combien une application rigoureuse peut, paradoxalement, conduire à une connaissance insuffisante des phénomènes de discrimination. Or, la problématique est plus celle de la sécurisation et de l'anonymat des statistiques.

UN CONCEPT ÉVOLUTIF ?

La plupart des experts rencontrés s'accordent à considérer que le concept de donnée sensible est forcément évolutif dans le temps et fonction du contexte, des technologies, de l'usage qui est fait des données, voire de l'individu lui-même. Faut-il repenser la liste des données sensibles ? Faut-il par exemple continuer à faire référence à la notion de race ? La LICRA pense qu'il ne faut plus utiliser ce terme qui n'a pas de réelle valeur scientifique. Allant au-delà, Dominique Boullier estime qu'on fonctionne aujourd'hui avec un modèle abstrait par rapport à la réalité des échanges (toutes nos données sont en effet des traces d'affiliation). C'est un régime qui n'est donc plus opératoire, même si on comprend son importance dans le modèle républicain français. Isabelle de Lamberterie souligne en revanche que le régime particulier est important symboliquement. Établir un « pot commun » risque de limiter la protection. Il est préférable de conserver une distinction entre les données sensibles par nature et les autres, même si parfois cette frontière est

LE NIR : UN DÉBAT DÉPASSÉ ?

Historiquement porteur d'enjeux lourds en termes de libertés individuelles, ce numéro d'identification national — créé sous le régime de Vichy — signifiant (car indiquant le sexe, le mois, l'année et le lieu de naissance de son titulaire) et emblématique des interconnexions de fichiers (et notamment du projet SAFARI à l'origine de la loi française de protection des données), est-il toujours sensible ? Curieusement, alors qu'il reste un symbole fort de la problématique Informatique et Libertés française, notamment pour la CNIL, il n'a été que très rarement évoqué par les experts si ce n'est pour mentionner sa charge symbolique qui reste importante (« le NIR, cet équivalent de l'ADN » selon Jean-Claude Vitran) et le fait que, finalement, interconnexions et bases centrales sont aujourd'hui monnaie courante même sans NIR et que les enjeux en termes de traçage et d'identification ne se situent, bien évidemment, plus autour de la question du NIR...

floue. Pour Yves Deswarte comme pour Caroline Lancelot-Miltgen, il y a là, en tout cas, une vraie question sur la classification même des données et leur sensibilité : le niveau de sensibilité est en effet en train de changer. Par exemple, quel est aujourd'hui et quel sera demain le statut de la photo, notamment avec la reconnaissance faciale ? À cet égard, comme le rappelle Pierre Piazza, la biométrie change indéniablement la donne : on tend vers une « biologisation » de l'identité, qui se retrouve « figée » et conduit à une traçabilité dans le temps et l'espace. Pour Yves Poullet, les données biographiques deviennent moins importantes que les données de « référence » (IP, cookies, RFID, géolocalisation...) : ce seront demain les vraies données sensibles. Ainsi, pour la Ligue des Droits de l'Homme et en particulier Jean-Claude Vitran, s'il faut bien sûr garder le socle actuel, il faut aussi prendre en compte de nouvelles données sensibles.

Qu'est-ce qui sera jugé discriminatoire dans 10 ans ? Arnaud Belleil souligne que les données sensibles peuvent être notamment celles qui sont transmissibles aux générations suivantes, à l'image des données génétiques. D'autres données très sensibles relèvent du domaine de la santé en général, des condamnations et des difficultés sociales et financières de type interdit de paiement, curatelle... Les données ethniques ou d'orientation sexuelle ont un degré de sensibilité qui peut évoluer : dans une logique de *scoring* automatisé, une adresse postale pourra être très discriminante et finalement devenir plus sensible que l'orientation sexuelle.

Emmanuel Kessous observe que les données les plus sensibles aujourd'hui sont celles qui peuvent être à l'origine de discriminations, par exemple les données de santé. L'orientation sexuelle est, quant à elle, de moins en moins privée, tout comme les choix religieux. Cela résulte de l'exposition que les gens en font volontairement. « Aujourd'hui, c'est donc l'utilisation possible des données qui en définit la sensibilité. Par exemple, c'est le système de santé de plus en plus "assurantiel" qui rend les données médicales sensibles. » L'unité de mesure et d'analyse a donc changé.

TOUT EST DONNÉE SENSIBLE ?

Pour Stefana Broadbent, on pense toujours que l'information critique est ponctuelle. Alors que l'information pertinente, la vraie révélation, vient de l'accumulation d'informations et des nouvelles techniques d'analyse algorithmique des données.

Aujourd'hui, comme le souligne Antoinette Rouvroy, il y a des données sensibles non seulement au sein des données à caractère personnel mais également au sein des données à caractère non personnel. Et pour Daniel le Métayer, la loi devra se saisir de ces nouveaux enjeux en tenant compte notamment des possibilités de recoupement des données.

Alors, finalement est-ce la donnée qui est sensible ou le traitement qui lui est appliqué ? Pour Nathalie Mallet-Poujol, si les données « sensibles » existent toujours dans le *offline*, en ligne elles sont d'une autre nature : mêmes banales, elles peuvent devenir sensibles du fait de leur accumulation sur Internet et du traitement qui leur est appliqué : ne faut-il pas, dès lors, travailler davantage sur le concept de traitement sensible ? ■

PRIVACY PARADOX : UN MYTHE DE NÉGLIGENCE GÉNÉRALISÉE ?

« Lors d'une réflexion sur la notion d'identité numérique, la FING s'est trouvée confrontée à un problème de catégories et de concepts inopérants autour du *Privacy Paradox*. En effet, l'étude *Sociogeek* montrait par exemple qu'en réalité, soit les individus ne ressentent pas de besoin d'exposition publique, et ils divulguent dans ce cas peu de choses, soit ils ressentent fortement ce besoin, et dans ce cas se mettent en scène de manière stratégique sur le web 2.0 et les réseaux sociaux. L'analyse des questions de vie privée dans le monde du 2.0 ne pouvait donc passer uniquement par le prisme de la notion de protection, de sécurité. En réalité, il y a trois motivations principales à la divulgation d'informations personnelles sur Internet : la connaissance et la fabrication de soi, la commodité, la réduction de la complexité (optimisation, personnalisation, etc.) et la projection et la valorisation de soi : cela permet d'aller vers les autres. La motivation principale des individus au dévoilement, c'est la projection de soi. Dans ce contexte, la protection n'est qu'une condition d'exercice. On peut même dire que l'utilité de la protection de la vie privée, c'est de permettre aux individus d'avoir une vie publique sans dangers excessifs. Plutôt que des identités multiples, il faut penser une identité à facettes multiples. Du coup, le fameux *Privacy Paradox* existe plus dans le regard de l'observateur que dans les faits et les comportements. »

Daniel Kaplan

LE *PRIVACY PARADOX* EST-IL UNE RÉALITÉ OU UN SIMPLE PRÉSUPPOSÉ ?

L'évocation du *Privacy Paradox* est devenue en quelques années un passage obligé dans toute réflexion sur les questions de vie privée. Selon cet axiome, les individus exprimeraient une inquiétude de plus en plus grande face aux divers risques liés aux données personnelles (vols d'identité, surveillance généralisée) et pourtant, dans le même temps, divulgueraient avec légèreté de plus en plus de données personnelles — même sensibles — sans la moindre garantie ou le moindre contrôle, sur les réseaux sociaux, dans leurs relations avec des entreprises... Il y aurait donc une incohérence apparente des personnes qui se dévoilent sur le web et dans les réseaux sociaux malgré l'inquiétude qu'elles expriment d'une perte de contrôle de leur vie privée.

Mais, comme le souligne Daniel Kaplan, finalement est-ce un paradoxe ou une illusion d'optique ?

En réalité, les utilisateurs des réseaux sociaux ne paraissent pas si naïfs que cela pour la plupart des experts rencontrés. Ainsi, les plus aguerris d'entre eux n'affichent pas toujours la même identité selon l'attente du moment et ils ont tendance à restreindre (lorsqu'ils maîtrisent bien les paramétrages) l'accès à leurs profils. Finalement, Arnaud Belleil s'interroge : « L'exposition de soi est-elle alors une erreur de jeunesse ou un acte témoin d'une vraie rupture générationnelle ? »

Même pour ceux qui sont moins aguerris dans leurs usages des technologies, le fait de chercher dans ce paradoxe une clé d'explication à une apparente irrationalité des individus est certainement une voie erronée. Si pratiques réelles et sentiments ou craintes divergent parfois, c'est aussi parce que la complexité des usages des technologies trouble les individus eux-mêmes, sans les rendre négligents ou absurdes pour autant. Finalement, pour Daniel Kaplan comme pour beaucoup des experts, tout se passe comme si ce fameux *Privacy Paradox* existait plus dans le regard de l'observateur — et de certains analystes — que dans les faits et les comportements réels. Raccourci commode, le *Privacy Paradox* serait donc en réalité une impasse méthodologique.

LE RELATIVISME ABSOLU EST-IL LE SEUL SCÉNARIO D'AVENIR DU CONCEPT DE VIE PRIVÉE?

Pourquoi alors un fantasme de ce type a-t-il la vie aussi dure ? Selon Antonio Casilli, la conception dominante de la vie privée est toujours marquée par l'idée qu'elle est un « cœur isolé » absolu, dans la droite ligne du concept américain de « *right to be left alone* ».

Cette vision reste naturelle pour la plupart des observateurs et trouble les analyses : il y a quelque chose de beaucoup plus contre-intuitif dans la notion de vie privée telle qu'elle se développe aujourd'hui. Comme nous l'a rappelé Alain Bensoussan, pourtant, il ne faut pas confondre secret et privé : la couleur de ma voiture est visible dans la rue, la grossesse d'une femme enceinte aussi, ça n'empêche pas ces informations d'être privées. Yves Poullet et Cécile de Terwangne ont également insisté sur ce changement dans la notion de « zone personnelle » (citant l'arrêt Rotaru de la Cour Européenne des Droits de l'Homme de 2000 et l'importance du débat européen autour des notions de « zone personnelle » et de « *expectations of privacy* »). « Ce que vous faisiez chez vous, montrer des photos, jouer, gérer des contacts, jouer à un jeu vidéo, gérer l'agenda... se retrouve dans le *Cloud*. Cela reste personnel mais nécessite des acteurs techniques intermédiaires. Le fonctionnement de la sphère personnelle repose sur des acteurs. Le droit s'immisce chez les individus *via* des outils impliquant des intervenants tiers. Face à cela, soit on considère que dès lors qu'il y a un outil, il y a des tiers et ce n'est plus personnel. L'exception à des fins personnelles et domestiques ne joue alors plus : la sphère totalement privée est préservée, mais il n'y a plus rien dedans, c'est une coquille vide. Soit il faut ouvrir notre notion de la sphère personnelle et créer en conséquence des responsabilités pour ces tiers. »

En réalité, la vie privée peut être vue non pas comme un noyau isolé et protégé, mais comme une négociation permanente avec nos interlocuteurs. Selon les travaux d'Irwin Altman sur la *social penetration theory*, les relations interpersonnelles se développent au fur et à mesure du temps en « oignon » : chaque couche s'ouvre l'une après l'autre, dans le cadre de chaque relation entre deux personnes. L'accès des autres à cette sphère intime est donc guidé par une approche personnelle, individuelle. Tout l'enjeu est donc d'arriver à marier demain cette négociation permanente avec des outils numériques comme, par exemple, ceux des services de réseaux sociaux : pour Antonio Casilli, le problème devient alors technique, puisque nous devons résoudre une équation complexe afin d'arriver, avec l'aide des plateformes uniques, à gérer des accès de plus en plus différenciés.

En réalité, les outils conceptuels pour comprendre les « dynamiques expressivistes » — c'est-à-dire cette tendance lourde à l'augmentation du désir d'« expression » des individus — ont longtemps manqué car, comme le rappelle Dominique Cardon, « jusqu'en 2002 les blogueurs étaient vus comme des gamins ou des journalistes ratés, y compris par les chercheurs ».

La variété des attitudes face au dévoilement des informations personnelles et la multiplicité des stratégies individuelles pour gérer leur(s) identité(s) numérique(s) (transparence, cloisonnement, pseudonymes, etc.) conduisent à une lecture très différenciée des enjeux de protection et de sa régulation. La vie privée est un problème de contextualisation, et sa valeur principale est peut-être, comme le résume la FING dans l'ouvrage « Informatique, libertés, identités » (FYP Editions, avril 2010), de pouvoir choisir et conduire sa vie publique sans renoncer à l'intime et au secret. ■

IDENTITÉ(S) NUMÉRIQUE(S) : TOUS AUTHENTIFIÉS ?

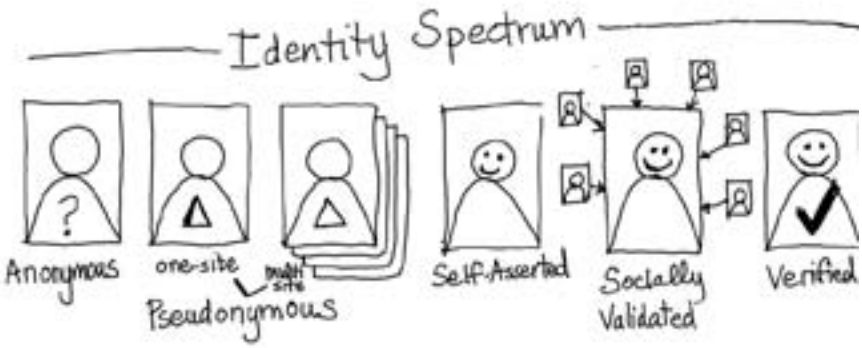
« L'identité numérique n'existe pas.
On confond trop souvent dans le discours courant identité, identité numérique et identifiant. L'identité numérique est un agrégat, aux contours assez flous, de notions éparses : pseudo, identifiant, log, donnée à caractère personnel et/ou technique, IP… Si l'on demeure au plan du droit, ce concept d'identité, invoqué à tout crin, n'existe pas. On parle de nom, prénom, sexe et tout le reste échappe pour l'essentiel au droit, ou est présent de manière parcellaire *via* des dispositions ponctuelles. Le délit d'usurpation d'identité a été inséré en droit positif par le législateur, mais on ne sait toujours pas ce qu'il recouvre précisément ! La loi récente sur la protection de l'identité tente de la réduire à des caractéristiques invariables, comme des données biométriques. C'est trop réducteur pour une notion si complexe, il faudrait idéalement pouvoir intégrer la notion d'identité au sens psychologique et sociologique dans le Code Civil. Tout ceci constitue un vaste chantier que la CNIL pourrait, pourquoi pas, ouvrir. »

David Forest

IDENTITÉ OU IDENTITÉS ?

L'identité numérique est une notion complexe à appréhender tant les contours sont variables selon le contexte. Un point de départ peut être de l'approcher par les attributs d'identité : un attribut renvoyant à une caractéristique d'un individu (âge, sexe, adresse, employeur, taille, pointure, etc.) qui, combiné à d'autres, peut permettre de constituer un profil qui lui est propre. Ainsi, bien que les individus n'aient qu'une seule « identité réelle », les manières de la représenter sont multiples. Le passage en ligne, qui implique une déclinaison dématérialisée, démultiplie les espaces de projection pour un individu qui va ainsi gérer plusieurs identités numériques. L'identité numérique d'un utilisateur est nécessairement fragmentée sur différents espaces, où chaque bribe peut avoir sa vie propre. Le « spectre de l'identité » est tout aussi varié et ses différentes formes peuvent aller de l'anonymat à l'identité vérifiée en passant par le pseudonyme ou un profil sur un réseau social (voir illustration page ci-contre). C'est d'ailleurs tout le paradoxe de la vie numérique, souligné par Daniel Kaplan, où il n'est pas plus possible d'être véritablement identifié (un utilisateur ne peut pas prouver qui il est vraiment) que d'être complètement anonyme (adresse IP, cookies, historique de navigation permettant une identification indirecte). Cette double spécificité est à la fois source de richesse et de difficultés. Pouvoir gérer le degré de correspondance entre une identité en ligne et une identité réelle et l'adapter aux différents univers en ligne, qu'ils soient personnels ou au contraire professionnels, constitue une véritable liberté pour les internautes. Alain Bensoussan considère d'ailleurs que la dignité numérique englobe un ensemble de droits parmi lesquels : le droit à la « multivie », aux avatars et à l'anonymat. Toutefois, la gestion de cet hétéronymat est coûteuse en temps et en organisation pour les utilisateurs. Devoir s'identifier à de nouveaux services en renseignant toujours les mêmes informations favorise le développement de solutions permettant la délégation d'authentification, plus confortables, qui permettent de se *logger* en un seul clic. Sur cette fonctionnalité, c'est le bouton *Facebook Connect* qui est le grand gagnant, si bien que les différents espaces en ligne deviennent de plus en plus interconnectés, limitant encore davantage la possibilité d'être véritablement anonyme. Henri Verdier estime qu'il serait dangereux que Facebook devienne le connecteur public universel, en particulier pour les grandes entreprises pour qui le réseau social deviendrait le *Customer Relationship Management* (ou CRM). Il milite pour un système public d'authentification, rejoignant Alain Bensoussan pour qui Facebook est en train de remplacer les identifiants de souveraineté.

La pression s'exerce aussi du côté des services en ligne qui, pour des besoins marketing ou de sécurité, souhaitent posséder le plus de garanties possible sur l'identité de leurs utilisateurs. Dans un contexte où l'identité numérique est majoritairement déclarative, les possibilités d'usurpation sont réelles et pour certains services (banques en ligne, e-administration, jeux en ligne par exemple) posent un problème de confiance suffisant pour souhaiter des modalités d'authentification plus sécurisées permettant de certifier l'identité d'un internaute. Ce débat existe aussi dans des domaines moins concernés



Le spectre identitaire : de l'anonymat à l'identité certifiée par Kaliya « Identity Woman » Hamlin.
© @identitywoman

a priori par la sécurité. L'Association française de normalisation (AFNOR) devrait prochainement proposer une norme visant à fiabiliser les avis de consommateurs en ligne, avec au cœur de la problématique la question de l'identification de leurs auteurs.

VERS LA FIN DE L'ANONYMAT ?

Les grands acteurs comme Facebook ou Google incitent eux aussi clairement leurs utilisateurs à être présents présents sous leur « véritable identité ». Facebook mobilise le *crowdsourcing* et propose à ses utilisateurs d'identifier au sein de leurs contacts ceux qui recourent à des pseudonymes. Google, qui n'autorisait pas les pseudonymes au moment du lancement de son réseau social Google+, a fait machine arrière, mais parallèlement incite à utiliser le même nom d'utilisateur sur l'ensemble de ses services en vue de fédérer une identité unique. La tendance semble donc s'orienter vers une identité en ligne au plus proche de l'identité réelle. Les technologies biométriques comme la reconnaissance faciale constituent la menace absolue pour Dominique Cardon (voir « Biométries : le nouveau sésame ? », page 24) partie sur la biométrie. Ces évolutions tranchent selon lui avec l'histoire d'Internet qui porte dans ses gènes la culture de « l'anonymat des pionniers ». La démocratisation d'Internet lève cette logique lettrée et tire vers la conversation et le réalisme. Le développement de la géolocalisation, consistant à remonter une position géographique réelle dans le monde numérique, contribue à ce rapprochement (voir « Géolocalisation : où allons-nous ? », page 21). Yann Leroux confirme cette tendance d'une fusion toujours plus forte entre le corps et la technologie. Il en conclut qu'à l'avenir, à moins de se couper d'Internet ou de se déconnecter, le droit à l'anonymat sera de plus en plus contesté. Pour preuve, dès lors qu'un internaute est « identifié », que ce soit par son historique de navigation, des cookies ou encore parce qu'il est connecté à un service (réseaux sociaux, microconversation), il n'est même plus assuré de pouvoir effectuer des requêtes de manière générique. C'est ce à quoi renvoie la « personnalisation du *search* » où les résultats d'une requête sur un moteur de recherche deviennent alors fonction du profil de l'utilisateur. Autrement dit, pour une même requête, les moteurs de recherches délivrent de moins en moins la même réponse à deux personnes différentes. Cette mise en danger de la neutralité du *search* fait peser un risque de fragmentation en adaptant le contenu aux goûts présumés des utilisateurs. Pour Antoinette Rouvroy, tout ceci n'est pas sans conséquence puisque ces filtres enferment les utilisateurs dans une bulle de contenus qui pourrait à terme modifier leur perception de l'information.

Yann Leroux estime qu'à l'avenir l'anonymat restera possible pour ceux qui disposent des capacités techniques leur permettant de se masquer au moyen d'outils cryptographiques. Sur ce point Jérémie Zimmermannn est plus optimiste et estime que les individus ont un vrai appétit de protection des données et qu'il suffit de simplifier et rendre accessible ces technologies de *geek* pour qu'elles soient utilisées par le grand public (voir « Vers de nouvelles fractures numériques ? », page 40). Pour la majorité de nos experts, l'horizon reste la possible disparition de l'hétéronymat puisque les différentes facettes d'une identité se croisent toujours, et qu'il est ainsi possible de reconstituer le profil d'un utilisateur. Jean-Marc Manach va encore plus loin en estimant que « le quart d'heure d'anonymat » va bientôt devenir un luxe. ■

VERS DE NOUVELLES FRACTURES NUMÉRIQUES ?

« Il y a trente ans, les non-usagers étaient ceux qui n'avaient pas accès, par manque d'intérêt ou de moyens financiers, aux nouvelles technologies de la communication. La mise en évidence de réelles inégalités statistiques quant à cet accès a conduit pendant plus de dix ans à se focaliser sur la question de la fracture numérique. Au fur et à mesure où celle-ci se comblait (ce qui est toutefois loin d'être totalement le cas), une catégorisation beaucoup plus fine et segmentée en terme d'inégalités d'usages est apparue, en particulier entre ceux qui possèdent les capacités cognitives et le capital culturel leur permettant de chercher une information adéquate en fonction de leurs besoins et attentes, de la traiter, de lui donner du sens et de la hiérarchiser selon un système de valeurs, et ceux qui n'ont pas les moyens d'y parvenir et donc d'en tirer de réels avantages. Mais depuis quelques années, une nouvelle forme d'inégalité se développe en plus autour d'un enjeu inédit : le droit à la déconnexion. Celui-ci renvoie à la défense d'un temps à soi dans un contexte de mise en synchronie généralisée, à la préservation de ses propres rythmes dans un monde poussant à l'accélération, au désir de ne pas être constamment dérangé dans l'environnement télécommunicationnel intrusif et à la volonté de prendre de la distance réflexive là où le heurt de l'immédiat et de l'urgence oblige à réagir trop souvent sous le mode de l'impulsion. L'idéal recherché n'est pas de se couper des flux télécommunicationnels mais de parvenir à leur maîtrise, c'est-à-dire à les utiliser sans en devenir l'esclave. Or cet idéal est très inégalement réparti entre ceux qui ont le pouvoir de se déconnecter sans que cela porte à conséquence et ceux qui ont le devoir de rester connectés, par obligations professionnelles ou relationnelles, sous peine de sanctions. »

Francis Jauréguiberry

NON CONNECTÉS, DÉCONNECTÉS, DÉNUMÉRISÉS

L'étude *Unplugged* d'Havas Media de septembre 2012 identifie deux catégories de déconnectés : les victimes de la fracture numérique et les « déconnectés choisis ». Selon le CREDOC, 25% des Français n'ont pas accès à Internet.

Ce chiffre monte à 44% pour les foyers au revenu inférieur à 1 500 € par mois. Après plusieurs années de baisse régulière, le nombre de « non-connectés subis » est, depuis 2010, relativement stable. Sans doute, la pénétration rapide des smartphones a-t-elle permis à des foyers d'avoir une connexion sans ordinateur. Mais leur coût, relativement élevé, interdit d'y voir la solution susceptible de résoudre la fracture numérique. Pendant ce temps, l'absence de connexion limite de plus en plus l'accès à des ressources, à des services. Elle tend à devenir un obstacle à l'intégration sociale, voire à l'emploi. La déconnexion subie devient une nouvelle source d'inégalité, qui se concentre sur les plus démunis de la population. Aujourd'hui un tiers des Français sont « hors du coup » car dénumérisés, ce que Christine Balagué appelle « le tiers-net ».

La déconnexion volontaire obéit à des logiques différentes, contestataires ou centrées sur la qualité de vie. Christine Balagué évoque les « indignés du numérique qui refusent l'infobésité » et prônent le *slow* aussi dans le numérique.

Pour Alain Bensoussan, la fracture digitale ne cessera pas d'augmenter. La réduire est l'un des rôles majeurs de la CNIL car elle crée un danger numérique : « Plus la fracture augmente, plus certaines populations seront en danger, notamment les enfants. Ceux qui ne sont pas aujourd'hui sur Facebook prennent du retard. »

DÉCONNECTÉ = SUSPECT ?

Les injonctions de recourir aux technologies numériques sont très fortes, tant au niveau professionnel que dans la société, souligne Josiane Jouët. C'est particulièrement vrai pour les personnes qui doivent se constituer un réseau personnel (professionnel, amical...). Francis Jauréguiberry estime que des irréversibilités sont d'ores et déjà en train de se mettre en place. « Dans un environnement augmenté, il va devenir de plus en plus difficile de se déplacer sans l'aide des technologies nomades. Dans une ville collaborative ou intelligente, décider de se passer de ces technologies revient non seulement à se compliquer considérablement la vie, mais aussi à courir le risque de se voir assimilé à un paria. » C'est ainsi que l'anonymat dans la ville est en train de s'évanouir, bien qu'il s'agisse d'une notion centrale de la modernité. Pierre Piazza souligne les résistances individuelles (par exemple, brûlure des empreintes digitales) ou collectives (Ligue des Droits de l'Homme, diverses associations...) qui existent bel et bien. Mais leur audience dans la société reste difficile à évaluer. La population en général semble d'une grande passivité et fait preuve

d'accoutumance aux technologies numériques. « On peut ainsi imaginer que ceux qui voudront échapper à ces technologies seront, par nature, suspects. » Il est donc particulièrement inquiétant que l'injonction de connexion, de présence numérique puisse se muer en une nouvelle norme sociale : « Si on n'est pas sur Facebook ou qu'on ne *tweete* pas » affirme Jean Frayssinet, « on en devient presque suspect, on est exclu socialement. »

Certains experts disent que le fait de ne pas être présent sur les services de réseaux sociaux pourrait être vu par certains employeurs comme un point négatif. Pour le moment, les injonctions de présence en ligne ne sont limitées qu'à certains métiers (par exemple, certains journalistes obligés de « *tweeter* »). Que se passera-t-il si l'absence sur Internet devient un handicap dans les processus de recrutement ou une nouvelle source de discrimination ? Nous ne sommes pas loin d'une application de ce qu'Antoinette Rouvroy appelle, après la juriste américaine Margaret Jane Radin, la « théorie des dominos » ou de « la pente glissante » : « La seule protection procédurale du droit à la vie privée informationnelle et l'exigence du consentement ne semblent pas suffisants pour garantir effectivement contre les pratiques discriminatoires dans un contexte où les disparités en termes de pouvoir ou de moyens ne placent pas les parties au contrat dans un rapport d'égalité. Un acte de renonciation à un droit comme la vie privée n'est pas qu'un *self-regarding act* : il a aussi un impact sur la société car la divulgation volontaire par certains d'informations personnelles dans des contextes compétitifs comme celui de l'emploi ou de l'assurance oblige tous les autres à divulguer eux aussi des informations du même type sous peine de subir un désavantage compétitif ou de voir leur refus de divulgation interprété — par l'employeur, par l'assureur — comme un indice de mauvais risque. »

CODER OU ÊTRE CODÉ ? LE RISQUE D'UNE FRACTURE ENTRE LES GEEKS ET LE GRAND PUBLIC

Mais une autre fracture numérique pourrait apparaître rapidement autour de la maîtrise des outils de contrôle et de protection. Ce que Henri Verdier résume en évoquant le risque de voir une « nouvelle aristocratie apparaître », une élite *geek* qui saurait assurer quand c'est nécessaire son anonymat ou sa tranquillité par l'usage d'outils sophistiqués (chiffrement, paramétrages complexes, outils d'anonymisation, réseau privé virtuel…), tandis que le reste de la population se verrait offrir cette seule alternative : ne pas utiliser ces outils ou accepter d'être lu à livre ouvert. Car, comme le soulignait le fameux « *code is law* » de Lawrence Lessig, de nombreux choix politiques sont désormais dissimulés dans des questions d'apparence technique : le choix, demain, ne sera-t-il pas entre « programmer ou être programmé », note Henri Verdier ?

Jérémie Zimmermannn relève que, en 1995, on pouvait espérer une généralisation des courriels chiffrés… qui n'a pourtant pas eu lieu. En effet, la bonne volonté et l'appétit des utilisateurs sont freinés par le manque d'accessibilité et de connaissance de ces technologies et par le fait qu'elles exigent toujours du temps. La commodité et la simplicité conduisent plutôt à négliger ces aspects, peu gratifiants pour ceux qui ne s'intéressent pas à la dimension technologique. C'est pourquoi il lui paraît essentiel de ne pas reproduire la même erreur et de ne pas s'adresser aux seuls *geeks* et autres enthousiastes des technologies. Pour éviter une nouvelle fracture numérique, il faut donc passer par un stade d'apprentissage et d'éducation au digital.

Cette question de la pédagogie « positivée » des usages est majeure pour Jean-Marc Manach, qui rappelle que « les jeunes générations se protègent mieux que les anciennes sur Internet. Ce sont donc les parents et les professeurs qu'il faut éduquer et former pour qu'ils arrêtent d'avoir peur ». Pour lui, le « vrai problème d'Internet, c'est ceux qui n'y sont pas et qui veulent y faire la loi ».

RÉDUIRE LA FRACTURE ENTRE INFORMATIQUE ET LIBERTÉS ET LE MONDE DU LOGICIEL LIBRE

Reste une fracture qui devrait être plus facile à résorber ! Philippe Lemoine relève que le monde Informatique et Libertés et celui du logiciel libre n'ont paradoxalement jamais eu de connexions fortes en France. Jusqu'à maintenant, les militants du libre voyaient ceux de la protection des données comme des adversaires, alliés des tenants des droits de propriété intellectuelle, bref « du monde ancien ». En réalité, ces deux mondes ont certainement beaucoup à s'apporter, en particulier pour créer de nouveaux modes de régulation. Ils ne peuvent que se rapprocher, par exemple dans leurs inquiétudes vis-à-vis du *Cloud Computing* généralisé. ■

03

Partie 0.3

PROTÉGER, RÉGULER, INNOVER DEMAIN

DÉFENDRE LA VIE PRIVÉE OU LES LIBERTÉS ?

« Le contexte historique de la loi Informatique et Libertés est devenu, pour certains, totalement anachronique. S'il est vrai que le débat de 1978 avait une forte dimension rétrospective, à une époque où l'on gardait à la mémoire les épreuves subies durant la période de l'Occupation, rien n'indique que les risques de discrimination à base communautaire, raciale, religieuse… n'appartiennent qu'au passé. Dès lors, la question reste posée : en cas de crise, comment rendre inoffensives ces technologies ? Par exemple, les risques pris en Inde par le fichage biométrique de l'ensemble de la population ont-ils bien été mesurés ? La version tragique de l'histoire existe aussi. Pourtant, les concepts autour de la question « TIC et libertés publiques » n'ont jamais paru aussi pertinents, comme le montrent les événements dans le monde arabe : la liberté dans l'utilisation des technologies de l'information et de la communication est devenue un élément substantiel de l'exercice des libertés individuelles et publiques. Mettre l'accent sur les effets des TIC sur les libertés permettrait de mieux apprécier toute la complexité et la dimension paradoxale de ces technologies. »

Philippe Lemoine

UN DÉPLACEMENT RÉCENT DU QUESTIONNEMENT

À en croire le discours général ambiant, l'objectif principal, voire unique, de la protection des données personnelles serait la préservation de la vie privée. Le concept, culturellement dominant aux États-Unis, de *privacy* prend, en effet, de plus en plus de place dans les réflexions européennes. Olivier Iteanu rappelle que la loi Informatique et Libertés visait à l'origine surtout les fichiers de souveraineté (police, justice, impôts…) et ceux qui touchaient les populations vulnérables. Le débat opposait avant tout les libertés individuelles et publiques à la sécurité publique, notions qui étaient présentées comme antagonistes. La vie privée était, quant à elle, surtout couverte par l'article 9 du Code civil… et invoquée par les *peoples*.

Pour Arnaud Belleil, un nouvel axe, entre transparence de la vie privée et préservation des secrets, a émergé ces dernières années du fait des nouvelles possibilités de captation de données, de la multiplication des informations diffusées sur Internet, du développement de l'exposition de soi sur les réseaux sociaux et de l'ambiguïté des politiques de confidentialité de certains d'entre eux. Ce nouvel axe n'a pas fait disparaître le précédent, opposant liberté individuelle et sécurité publique, mais il semble plus médiatique, parce que les acteurs en présence sont plus nombreux, plus diffus et parce qu'ils sont porteurs de contradictions, étant autant favorables à la transparence qu'à la protection de la vie privée.

LES PARADOXES DE LA MISE EN AVANT DE LA VIE PRIVÉE

Cette notion est actuellement en pleine évolution et donc de plus en plus difficile à saisir. On ne peut plus se référer à sa définition traditionnelle qui l'opposait à la sphère publique, car, souligne Josiane Jouët, l'époque est marquée par une forte porosité entre vie privée et vie publique. Même si la technologie n'en est pas le seul facteur explicatif, le caractère globalisant du numérique le distingue des anciens médias : aucun aspect de la vie sociale n'échappe à son processus d'innovation qui entre en interaction avec les innovations sociétales.

Pour Antoinette Rouvroy, « plusieurs tendances sont à l'œuvre, qui remettent en cause la notion de sphère privée : l'irréversibilité croissante des interactions avec les dispositifs technologiques ; l'interopérabilité croissante de ces dispositifs entre eux ; la confusion croissante des temps sociaux et intimes et des temps de travail et de loisirs qui est liée à l'importance du travail en réseau. Le travail se déterritorialise, le temps de travail se décloisonne. Avec l'immersion permanente que cela implique, c'est la notion de sphère privée qui devient problématique. »

Le grand tournant date de l'arrivée du web 2.0, explique Alain Rallet. Centré sur des contenus

LES TROIS DIMENSIONS DE LA VIE PRIVÉE DISTINGUÉES PAR FABRICE ROCHELANDET

1/ Le secret, qui implique la capacité à contrôler l'utilisation et le partage de ses données. Le droit à l'oubli y est rattaché.
2/ La tranquillité, le « droit à être laissé seul », à ne pas être perturbé par des sollicitations non désirées, ce qui suppose le contrôle de l'accessibilité à son domaine privé.
3/ L'autonomie individuelle, la souveraineté de chacun sur sa personne et ce dont elle souhaite garder la maîtrise, sans que cela soit nécessairement tenu secret. La vie privée correspond alors au « désir humain d'indépendance par rapport au contrôle des autres ». En France, le droit à la libre disposition de soi est traditionnellement rattaché à la liberté d'expression et à l'intégrité physique.

générés directement par les internautes et sur le dévoilement de soi, le web 2.0 implique beaucoup plus intimement les particuliers.

Par ailleurs, Emmanuel Kessous rappelle que, dans les sociétés modernes, sous l'influence du libéralisme politique, le pacte social prévoyait le contrôle de l'État en échange du respect de la sphère intime. Or, aujourd'hui, les technologies de prélèvement et de collecte de données remettent en cause cet équilibre. Il en découle parfois une mise en visibilité publique d'informations qui relèvent du domaine privé. Une évolution que percevait déjà dans les années 70 le sociologue Richard Sennett, dans son livre *Les Tyrannies de l'intimité*, lorsqu'il dénonçait la fin de l'homme public. Emmanuel Kessous ajoute que la notion de vie privée ne paraît, par ailleurs, guère en phase avec l'actuelle quête de visibilité sur les réseaux sociaux et l'émergence d'outils qui facilitent l'auto-dévoilement et la publicisation de l'espace privé. Dans ce monde, il faut attirer l'attention, « créer le *buzz* », être visible. La rupture date déjà des années 70, lorsque la publicité et le marketing commencèrent à justifier l'utilisation de données privées pour construire des biens marchands, quels que soient les risques de manipulation des personnes. Pour Nathalie Mallet-Poujol, il n'en faut pas moins combattre le discours de remise en cause du concept de vie privée, y compris au risque de protéger l'individu contre lui-même.

LA MONOPOLISATION DU DÉBAT PAR CERTAINS THÈMES

Des changements technologiques majeurs sont intervenus ces dernières années : le traçage par les réseaux sociaux, la biométrie, la géolocalisation, les nanotechnologies... Dans le même temps, Nathalie Mallet-Poujol constate que la compréhension des risques ne s'est pas améliorée, bien au contraire. D'une part, ces changements accentuent une tendance générale au nomadisme des individus et des données. D'autre part, ils détournent l'attention des juristes et de la doctrine des questions Informatique et Libertés classiques, celles qui ont trait aux fichiers de souveraineté et aux populations les plus vulnérables (étrangers, détenus...).

Jean-Claude Vitran et Maryse Artiguelong surenchérissent : « La présentation des réseaux sociaux comme étant plus dangereux que les initiatives gouvernementales en matière de fichage a conduit à une démobilisation partielle de la population et à la disparition de tout débat sur les dangers de l'interconnexion. C'est ainsi qu'il n'y a eu récemment de mobilisation citoyenne qu'à propos du fichage des enfants et des questions de santé. »

LES RISQUES LIÉS À L'OCCULTATION PROGRESSIVE DES ENJEUX EN TERMES DE LIBERTÉS

Il est à craindre que des aspects essentiels de la protection des données (la défense des droits individuels et collectifs, la lutte contre les discriminations) ne soient minorés, à un moment où certaines barrières risquent de disparaître. Pour Pierre Piazza, « les effets du 11 septembre ont donné un coup d'accélérateur à la problématique du fichage policier, en favorisant un mode de gouvernance par la peur, l'inquiétude. Avec le passeport biométrique, et le projet de carte d'identité biométrique, chacun est rendu transparent aux yeux de l'État ». Meryem Marzouki confirme qu'une rupture majeure dans le domaine de la protection du citoyen face à l'État s'est produite depuis le 11 septembre 2001. C'est ainsi que, là où la directive de 1997 concernant le traitement des données personnelles dans le secteur des télécommunications limitait la rétention des données personnelles, la logique s'est inversée depuis cette date. Le renforcement du contrôle social sur les individus, surtout vis-à-vis des catégories de population les plus fragiles, ne semble plus faire débat. Certains paraissent même souhaiter y participer, pour mieux contrôler leur entourage (exemple de la vidéosurveillance des nounous par les parents). La volonté de détecter très tôt toute forme de dangers (tendances délinquantes, clients à risque...), avant qu'ils ne se concrétisent, se banalise au risque de survaloriser le caractère prédictif des données traitées. La vidéosurveillance, la géolocalisation et la biométrie permettent d'étendre le contrôle social aux déplacements et même aux corps. ■

PROTÉGER QUI, PROTÉGER QUOI ET COMMENT ?

« On évolue vers une vision réductrice de la protection des données. On privilégie une approche anglo-saxonne « individualisante » centrée sur les données. À force de se focaliser sur la protection des données, on perd de vue la raison pour laquelle elle existe et ce qui est essentiel, à savoir les enjeux de vie privée et de libertés. Par exemple, sur les scanners d'aéroport, on a isolé le sujet protection des données, établit une balance précise des données susceptibles ou non d'être traitées, des utilisateurs légitimes ou non, de la durée de conservation plus ou moins longue et on a perdu de vue des questions plus essentielles de dignité de la personne humaine, de la liberté d'aller et venir, de la révélation ou non de son état de santé… La vision de la *privacy* comme mère ou plutôt condition de toutes les libertés est une vision européenne. Cette vision est peu partagée dans le reste du monde, où la *privacy* est comprise comme « confidentialité » et non « vie privée ». La vision européenne doit être préservée. La place de l'individu dans la société est en jeu. »

Yves Poullet

PROTÉGER LES DONNÉES PERSONNELLES OU LA PERSONNE ?

Lorsqu'on évoque la loi Informatique et Libertés française comme l'ensemble du corpus juridique européen en la matière, il est aujourd'hui d'usage courant de parler de protection des données personnelles, formule raccourcie, certes commode mais fort réductrice. Or, comme le rappelle Paul-Olivier Gibert, l'enjeu n'est pas la donnée, mais la souveraineté de l'individu sur ses données à caractère personnel.

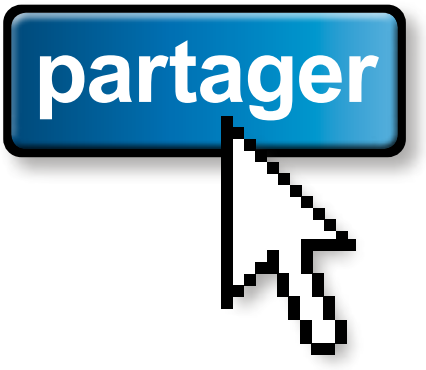
Car l'objectif poursuivi et rappelé dans le titre même de ces textes est bien de protéger les personnes à l'égard des traitements de données personnelles. Il s'agit donc certes d'assurer le droit de chacun à la protection de ses données personnelles (droit inscrit dans la charte européenne des droits fondamentaux) mais au-delà, comme le rappelle l'article 1er de la loi Informatique et Libertés, il s'agit aussi, plus fondamentalement, de garantir que l'informatique soit au service de chaque citoyen et ne porte atteinte ni à l'identité humaine, ni aux Droits de l'Homme, ni à la vie privée, ni aux libertés individuelles ou publiques.

Cette vision d'un individu isolé « face » à la toute puissance de l'informatique est-elle toujours de mise aujourd'hui ? Faut-il continuer à vouloir protéger les individus malgré eux ?

Les avis sont partagés. De nombreux experts considèrent que cette vision, qu'ils sont plusieurs à qualifier de « paternaliste » (comme le souligne Emmanuel Kessous, il est difficile de définir *a priori* et de manière identique pour tous l'autonomie. Celle-ci, en informatique, est en effet extrêmement dépendante des compétences techniques des individus), est effectivement dépassée et doit au moins être adaptée ou complétée à l'aune des nouvelles pratiques sociales.

Olivier Iteanu rappelle d'abord que, en 1978, la question de la vie privée n'était pas vraiment abordée : « La loi concernait surtout les fichiers et les questions de libertés publiques. Depuis 10 ans, le changement majeur est que l'exposition publique concerne tout le monde. De même, la diffusion est accessible à tous et elle n'est plus limitée aux médias traditionnels. Qui plus est, les opérateurs diffuseurs sont plus ou moins justiciables en France, ce qui est problématique. »

Ce constat est partagé par Paul-Olivier Gibert : « La loi Informatique et Libertés ne couvre plus tous les problèmes. Elle couvre très bien, en l'état, ce que peut faire une structure qui se retrouve dépositaire de données personnelles, dans le cadre de l'exécution d'un contrat ou d'une prérogative de puissance publique par exemple… Certaines problématiques en revanche sont beaucoup moins bien couvertes par exemple celles concernant l'autoproduction et l'autoédition de données à caractère personnel par la personne elle-même. Il s'agit alors d'une décision individuelle (ce n'est pas Facebook qui décide de la divulgation) : cette



problématique n'existait pas en 1978. Il faut donc aujourd'hui, à la fois protéger les personnes et avoir une approche leur donnant la possibilité de protéger d'un point de vue technique et juridique leurs données à caractère personnel et de maîtriser leur usage.»

Et selon Alain Bensoussan, «il faut d'abord reconnaître des droits, par la propriété des données, et dans un second temps accorder une protection par exception, si c'est nécessaire. Il faut prioritairement que l'individu puisse décider de la sensibilité qu'il accorde à ses données et de leur publication et utilisation, et introduire des valeurs de protection. Mais la liberté de décision doit être le principe fondamental et la protection, l'exception».

Antoinette Rouvroy est plus circonspecte : «Si l'approche individualiste des textes de protection des données (qui présuppose des individus libres, rationnels et autonomes, et du coup, protège peu les valeurs comme la vie privée en tant que telle) est peut-être opérationnelle, parfois elle sert aussi de dédouanement. Peut-être vaudrait-il mieux parfois ne pas avoir de régime de protection, comme c'est le cas aux États-Unis, où le droit à la protection de la vie privée n'est pas inscrit, ce qui permet du coup un débat permanent sur un *legitimate interest of privacy.*» Pour elle, «la régulation est certes utile, mais a des effets pervers : elle fausse le débat, voire dispense du débat public. Elle donne une impression de protection un peu excessive. Elle protège des droits formels, mais pose un problème d'effectivité des droits : la réalité ne va pas se conformer spontanément aux textes».

Dans le même esprit, Caroline Lancelot-Mitgen souligne que si les individus savent généralement qu'il y a une règlementation et connaissent la CNIL, ils ignorent tout du contenu de la loi ou des missions de la Commission : «En fait, ils se sentent faussement protégés par la loi et négligent de prendre des précautions. Les décisions, alertes et campagnes de communication de la CNIL peuvent donc aussi être contre-productives : elles donnent l'impression que la régulation limite les dégâts, qu'une autorité se saisit des sujets et que les individus n'ont de leur côté rien à faire. Aux États-Unis, les individus sont plus vindicatifs car ils n'ont pas cette illusion d'une protection institutionnelle.»

Jean Frayssinet fait un constat identique : «Depuis 1978, il n'y a pas eu vraiment de mobilisation, même au sein des associations de consommateurs, en comparaison avec les États-Unis, la Scandinavie ou l'Allemagne. La société française est passive, peu organisée ; elle ne se mobilise pas ou alors, elle "fait du bruit" sur des choses accessoires. Le garant est l'État. Les gens ont des droits, mais ne les utilisent pas». Et Françoise Roure en vient même à redouter qu'à l'horizon 2020, «il n'y ait plus de demande sociale en matière de protection de la vie privée parce que les gens ne seront plus dans la capacité intellectuelle de le faire, ne comprendront plus le sens d'une telle protection».

Philippe Lemoine nous met en garde : «Nous vivons dans un *momentum* de fascination pour la technologie, voire dans une véritable période de déterminisme technologique. En effet, face à une société qui a perdu nombre de ces repères, ces technologies apparaissent comme une source de stabilité et de progrès positif. Or, comme le soulignait Edgar Morin, l'enthousiasme n'est pas normal dans la société : c'est un marqueur sociologique important. Les technologies semblent prendre la place laissée vacante par d'autres concepts pour permettre aux individus d'avoir prise sur le monde.

En réalité, une telle phase de fascination ne peut qu'être temporaire, tant qu'elle reste synchrone d'une illusion de maîtrise. »

Yves Poullet rejoint ce point de vue. Le temps de réflexion n'existe plus car il ne peut pas être aussi rapide que les changements technologiques qui sont, qui plus est, « imprévisibles ». Dans ce contexte, le concept de consentement n'a plus guère de validité : par exemple, la question d'être, ou pas, sur Facebook ne se pose malheureusement plus.

FAUT-IL TRACER DE NOUVELLES LIGNES ROUGES ?

Rejoignant le point de vue de plusieurs experts, Daniel Kaplan estime certes que l'approche par la protection, seule, est insuffisante, car une « protection » trop forte peut aliéner l'individu, le « calfeutrer » à l'abri de la société. La démarche de protection ne fonctionne que si elle est liée à une action positive, proactive. Mais pour lui, « il y aura toujours besoin de lignes rouges : il y a une asymétrie de pouvoir et d'information et il y a encore des questions qu'on ne doit pas pouvoir poser. Il faut donc garder une régulation et agir dans trois axes : la protection (nécessaire mais insuffisante), la mise en capacité des individus (par la mise à disposition d'outils par exemple) et l'éducation et l'information ».

Antoinette Rouvroy défend aussi l'idée qu'il faut réglementer certains usages tels que par exemple le *data-mining* et le profilage — avis également partagé par David Forest, Daniel Le Métayer et Claude Castelluccia : « Il est notamment nécessaire d'approfondir la réflexion sur l'usage du profilage à des fins de traitements différenciés des personnes. Cette question dépasse les considérations juridiques et techniques ; il s'agit en fait d'une question politique et sociale : dans quels cas une pratique de traitement différencié des personnes doit-elle être considérée comme socialement acceptable et dans quel cas, au contraire, doit-elle être considérée comme discriminante et inacceptable. »

« Lutter contre les discriminations pour raisons médicales, à l'embauche, à l'accès au crédit, en fonction d'antécédents judiciaires… doit rester l'un des rôles les plus sensibles de la CNIL. *A contrario*, la lutte contre le spam doit pouvoir se réguler par le jeu du droit de la consommation, voire des dispositifs techniques ». Pour Arnaud Belleil, la CNIL doit donc faire des choix de priorités.

Meryem Marzouki considère, quant à elle, qu'il est temps « de mieux "sanctuariser" le biologique et la biométrie, qui sont les données les plus sensibles, tout comme on sanctuarise le corps, le sang et les organes. Pourquoi aurions-nous le droit de vendre nos données les plus intimes plus facilement que son sang ? Par ailleurs, évoquer des "droits de propriété" concernant les données personnelles n'a rien d'anodin : la protection des données personnelles ne serait plus alors un droit fondamental, juste un droit de propriété ? Or, sa protection en tant que droit fondamental est déjà mal aisée. Qu'en sera-t-il s'il ne s'agit plus que d'une simple question de protection de la propriété individuelle ? L'autorégulation étant largement un leurre, c'est la régulation marchande qui risque de s'imposer. Il faut donc préserver une loi protectrice, de la même façon qu'il existe une protection forte du consommateur, et aller vers un cadre juridique mondial qui reste le seul cadre efficace. La grande question est celle de l'efficacité réelle des droits existants. Ainsi, comment le consentement peut-il être réellement "éclairé" et "libre" par exemple dans le domaine du *Cloud Computing* ? De même, le droit d'accès est certes garanti, mais il n'est pas exercé : c'est un droit formel. Il faut trouver de nouvelles façons de l'appliquer ».

Isabelle de Lamberterie s'interroge : « Les utilisateurs des nouveaux médias sociaux ne devraient-ils pas être appréhendés comme des "consommateurs" peu responsables, que l'on doit protéger ? Certaines actions sont impulsives, sur certains aspects il faut protéger les citoyens contre leur comportement individuel. » À cet égard, l'édifice Informatique et Libertés devrait être renforcé sur ses principes. Certaines fictions sont à conserver (notamment le consentement, comme obligation « symbolique » selon l'expression de Christine Balagué) même si concrètement, elles sont difficiles à mettre en œuvre.

Dominique Wolton constate que, finalement, l'édifice Informatique et Libertés, robuste, tient

FAIRE INTERVENIR LE JUGE

Il faut favoriser l'émergence d'une jurisprudence judiciaire en matière d'Informatique et Libertés. Tel est l'avis de beaucoup d'experts rencontrés. Citons les propos de quelques-uns d'entre eux.

« Il manque une ou deux grandes décisions symboliques de justice, qui servirait de référence. Hormis quelques contentieux rares en matière de droit du travail, il n'y a en effet pas ou peu de jurisprudence vraiment marquante sur les réseaux sociaux (et notamment sur la question de la publication de photos), ce qui serait cependant fortement souhaitable : il serait nécessaire de disposer de signaux juridiques clairs, qui n'existent pas aujourd'hui. » - Dominique Cardon

« Comme les affaires de la CNIL ne sont quasiment jamais transmises au parquet, elles ne font pas jurisprudence ! » - Jean-Marc Manach

« Il existe en réalité peu de grande jurisprudence ou de grandes décisions auxquelles se référer dans le domaine Informatique et Libertés. Dans la branche pénale, les parquets ne voient pas le trouble à l'ordre public, alors que la Loi Informatique et Libertés est bien une loi pénale. Sur le plan civil, ce droit a également peu d'expressions judiciaires, peu d'"affaires". Les avocats font surtout du conseil ou des formalités préalables. La CNIL a pris plus de décisions et de sanctions que le juge pénal depuis 1978, mais elles sont assez peu commentées. » - Olivier Iteanu

« Il manque en France une décision de justice qui marquerait les esprits. » - Jean Frayssinet

« La CNIL a été prise dans une injonction paradoxale : elle devait communiquer et se faire connaître mais elle a fini par occuper tout l'espace du discours jusqu'à en devenir la voix dominante en occultant les débats, et aussi au détriment des juges. Elle n'est d'ailleurs pas tant vue comme un régulateur que comme un juge. Mais le juge des libertés, son garant, est et doit rester le juge judiciaire en vertu de la séparation des pouvoirs : c'est lui le juge naturel des données personnelles. Ce n'est pas le rôle de la CNIL d'être un "juge bis". Seule la menace judiciaire est compréhensible par les compagnies de culture anglo-saxonne, notamment les géants du web. C'est culturel : ils veulent à tout prix l'éviter. » - David Forest

bien la route, car il est fondé sur des valeurs et des principes qui n'ont pas besoin d'être adaptés à chaque technologie. Ce sont les nouvelles technologies qui doivent s'adapter à la loi qui doit garder une dimension universelle, avec si nécessaire des adaptations limitées rendues nécessaires par la vitesse d'évolution de la technologie.

Pour Dominique Boullier, « une législation Informatique et Libertés est nécessaire, mais l'actuelle est obsolète. Les données personnelles et la vie privée sont des fictions juridiques inopérantes (voir « Tout devient-il donnée personnelle ? », page 32) car les pratiques réelles sont contraires. Les données — que l'on peut qualifier aujourd'hui de données transactionnelles ou relationnelles et non plus personnelles — circulent de toute façon. On va avoir à faire face à de graves questions de sécurité… et, malheureusement, c'est seulement alors qu'on agira… La régulation est indispensable mais "pas équipée" si elle repose uniquement sur cette vision doctrinaire des données personnelles et de l'identité ».

Pierre Piazza considère qu'« il y a une double inadaptation de l'édifice Informatique et Libertés, tout d'abord, en raison de l'incapacité à faire appliquer les principes notamment vis-à-vis de certaines autorités étatiques. Quid des sanctions vis-à-vis des pouvoirs publics, quand l'État lui-même n'applique pas les règles ? Ensuite, du fait de l'internationalisation de l'échange des données et en particulier des échanges transatlantiques (*PNR*, affaire *Swift*…) ».

David Forest développe un point de vue contrasté : pour lui, la loi française de protection des données est bonne, car elle contient des notions à contenu variable, réglable et des principes généraux. Mais elle est « restée en jachère ». Elle a beaucoup été commentée mais, par exemple, le volet répressif a été peu appliqué. Il est donc difficile de faire un bilan de son application. Les entreprises commencent à peine à la considérer. Cela renvoie au rôle de la CNIL, qui a peut-être une trop grande place dans la loi.

Pour la plupart des experts, il faut donc adapter notre régulation, voire, pour Alain Bensoussan, songer même à écrire une loi des droits fondamentaux du numérique (voir « Repenser le droit du numérique », page 54). ■

INNOVER DANS LA RÉGULATION

« Alors, quelles régulations demain ? Les différents types de régulations : par les technologies, par les procédures ou par les institutions sont tous nécessaires. Les régulations à venir sont donc idéalement une combinaison entre ces différents volets, en plus de la vigilance de chaque individu et des bonnes pratiques personnelles. Sur le volet technique, la prudence doit être de mise : l'exemple des DRM ou celui des certificats pour les impôts en ligne montre bien que la vitesse d'innovation tue rapidement les régulations purement techniques. Il est plus facile d'adapter des mécanismes de régulation « *soft* ». Concrètement, le droit, les règles administratives ont certes leurs limites mais pas plus que l'implantation d'une technologie (par exemple une puce). Les entreprises semblent quant à elles prêtes à investir dans des processus de labellisation, au regard du succès par exemple des normes ISO. Ces processus garantiraient l'intégrité et la qualité dans la gestion des données. Mais s'il y a peu de contrôles et que les sanctions sont faibles, peu d'entreprises investiront dans des labels ou des *Privacy Impact Assessment*.
La difficulté est également de savoir ce qu'on labellise : une entreprise, un processus particulier de traitement des données, un produit ? Il ne faut pas labelliser une brique technologique isolée mais tout ce qui s'appuie sur les données. Cela doit concerner l'ensemble du processus de collecte, de traitement de l'information puis de sa revente.
Un système qui couplerait une norme de ce type et une sensibilisation des consommateurs à leurs données personnelles pourrait inciter les entreprises à acter de leur transparence, de leur excellence en matière de traitement des données. »

Pierre-Jean Benghozi

DE NOUVEAUX THÉÂTRES D'OPÉRATIONS À EXPLORER : GUERRE INFORMATIONNELLE, ESCARMOUCHES ET MAÎTRISE SOCIÉTALE

Le théâtre d'opérations de la régulation est devenu plus complexe et plus fragmenté, selon la majorité des experts rencontrés. Il n'y aurait plus de régulation qui puisse opérer efficacement sur la base des seules réglementations : technologies, standards et labels, tiers de confiance, marchés devront être de plus en plus mobilisés, complétés par des comportements personnels de vigilance. La régulation demain doit s'organiser autour de dispositifs mixtes regroupant droit, économie, nouveaux outils, diffusion de technologies, communication et pédagogie. Elle doit être accompagnée d'une mise en capacité des individus par l'éducation au numérique qui ne doit pas être seulement — ni même majoritairement — une éducation à ses risques : il faut privilégier une pédagogie des usages et des bonnes pratiques, plus efficace qu'une pédagogie des risques (qui ne fonctionne pas ou plus, comme le rappelle entre autres Jean-Marc Manach). En réalité, comme l'affirment Alain Rallet et Fabrice Rochelandet, dans un tel contexte la régulation doit passer par une sorte de « guerre informationnelle » avec les acteurs clés de l'économie numérique : une série « d'escarmouches » sur le plan de l'opinion publique peut en effet faire bouger des lignes dans un sens ou dans l'autre, et permettre l'émergence de la future norme.

Pour Arnaud Belleil, au-delà d'une vision anglo-saxonne (qui change par ailleurs elle-même plus qu'on ne le pense) d'un système où l'autorégulation et le marché suffisent *a priori*, il faut conduire à l'avenir la régulation, pour citer Pierre Tabatoni, avec un « système de protection » regroupant droit, économie, militantisme et technologies et où toutes ces composantes se renforcent mutuellement. Il ne faut pas non plus négliger l'hypothèse de nouveaux acteurs prenant une place non négligeable dans la régulation de demain. Ainsi, pour Emmanuel Kessous, l'instauration de système de tiers certificateurs afin de garantir une transparence vis-à-vis du consommateur (quel type de données, combien de temps elles seront conservées...) doit être explorée. Cette voie de l'émergence d'intermédiaires, assureurs (Dominique Boullier pense ainsi que les assureurs pourraient faciliter l'internalisation des risques dans les coûts de transaction, comme c'est le cas pour les cartes bancaires) et auditeurs est certainement à explorer si la « mise en conformité » devient une mission essentielle des autorités de protection des données, car comme le rappellent Daniel Le Métayer et Claude Castelluccia, si la CNIL ne peut pas tout auditer elle-même, elle doit être en mesure de distribuer et de superviser les contrôles. Certains pensent également que, à condition de disposer de l'autonomie et des compétences nécessaires, le Correspondant Informatique et Libertés pourrait devenir demain un vrai « responsable de la conformité » de son organisation. Selon Yves Poullet et Cécile de Terwangne, ce qui compte *in fine*, c'est que la société doit se prononcer, et il y a plusieurs moyens d'organiser cette « maîtrise sociétale », par exemple par des mécanismes de *class action* ou par le développement des débats au niveau européen et par des prises de position claires des

législateurs. Arnaud Belleil pense également que la France aurait besoin dans ce domaine d'un dispositif de type « action collective ».

REMETTRE L'INDIVIDU AU CŒUR DE LA RÉGULATION

L'action de régulation doit s'attacher à réduire les asymétries d'information et de pouvoir entre les acteurs économiques ou institutionnels et les individus, par une meilleure information de ceux-ci et par la création d'outils et de services centrés sur eux. L'*empowerment* de l'individu, le fait de l'aider et de le mettre en capacité de protéger ce qu'il souhaite et d'exercer ses droits est un axe majeur pour la régulation de demain. Pour autant, ce serait à coup sûr une erreur de croire que l'individu peut gérer le poids de la régulation : s'il doit avoir sa place et si les actions de régulation doivent conduire à son *empowerment*, il ne peut s'agir de lui donner ce fardeau à lui seul. Pour Alain Rallet et Fabrice Rochelandet, si ce sont les individus qui doivent porter la charge de la régulation, c'est inefficace et injuste, même si cela favorise un nécessaire apprentissage. Il faut donc que le coût de la régulation porte aussi sur les exploitants tout en faisant attention à ne pas contraindre l'innovation.

D'autant que, comme ils le rappellent, les travaux des économistes comportementalistes montrent que faire peser un poids trop important sur les choix des individus peut être contre-productif. Ainsi, Alessandro Acquisti a montré qu'il arrive que les individus dévoilent beaucoup plus de données lorsqu'ils pensent en avoir le contrôle, que ce contrôle soit substantiel ou non, ce qu'il appelle « l'illusion de contrôle ».

Les cas de faille de sécurité montrent également que tant qu'aucun dommage n'est visible, les individus semblent oublier rapidement ces cas. Jérémie Zimmermannn insiste d'ailleurs sur le fait qu'il faut augmenter le « coût », à la fois financier et d'image, de ces failles pour responsabiliser les entreprises, qui sont aujourd'hui plutôt tentées de taire ou de minimiser ces fuites, par exemple en créant dans le droit des obligations de notification précise, individuelle et ciblée de toutes les données personnelles qui ont « fuité ».

Pour certains, tout cela suggère que les *Privacy Enhancement Technologies* (*PETs*) seront indispensables pour outiller les individus demain. Mais s'agissant de leur intérêt, les lectures des experts interrogés sont contrastées. Pour Daniel Le Métayer et Claude Castelluccia, globalement, plusieurs types de *PETs* sont déjà disponibles. On peut notamment citer les outils d'anonymisation, les outils de contrôle (qui permettent à chacun d'exprimer finement ses volontés en matière de protection de ses données personnelles), les outils de bruitage ou de perturbation de données (quand l'exactitude absolue n'est pas requise) ou encore des outils de chiffrement (dont Yves Deswarte et Jérémie Zimmermannn soulignent l'importance).

Cependant, pour eux, il n'est pas garanti qu'un marché des *PETs* mature se développe : personne n'y investit massivement car le « consentement à payer » des utilisateurs paraît très faible pour le moment. Pour d'autres, l'optique d'une réconciliation par la technologie est illusoire, voire dangereuse : « La surveillance et la vie privée s'opposent et doivent rester en conflit. Les *PETs* sont nécessaires et utiles, mais ne doivent pas dispenser du débat démocratique à propos des enjeux collectifs, irréductibles aux solutions techniques augmentant le contrôle individuel des utilisateurs sur "leurs" données » (Antoinette Rouvroy). Pour Caroline Lancelot-Miltgen, une autre voie pour redonner du pouvoir aux consommateurs pourrait être de favoriser des mécanismes de « contrôle par les usagers » au moyen de systèmes qui noteraient et « rankeraient » les entreprises. On voit déjà énormément de protestations contre des pratiques commerciales émerger sur Facebook ou Twitter : il ne faut pas négliger l'idée que parfois, comme le rappelle Daniel Le Métayer, « les utilisateurs votent avec leur souris ».

Finalement, une solution d'avenir est peut-être surtout, comme le recommande Dominique Cardon, de transférer nos critiques « de ceux qui s'exposent à ceux qui regardent » et faire en sorte que la régulation concerne ainsi au premier chef celui qui regarde et non celui qui s'expose (voir « La révolution du web social : demain, tous des *peoples* ? », page 12).

« La régulation *a priori* est devenue et sera à l'avenir de plus en plus difficile à exercer. La régulation *a posteriori* prend donc de l'importance : il faut que ceux qui utilisent des données rendent des comptes. En réalité, de même que l'on ne se permet pas en société d'épier les habitants d'une maison à travers leurs fenêtres, on ne devrait pas pouvoir inférer sur eux en toute impunité : l'utilisation des données doit laisser des traces vérifiables par des tiers. Et pour permettre cette vérification, la partie « design de l'interface » est importante, comme le montre l'exemple du *dashboard* (tableau de bord) de Google où l'utilisateur peut avoir un aperçu des informations qu'il partage avec le service, mais elle ne suffit pas. Dans tout système d'*accountability*, il faut s'appuyer sur un principe de sincérité, sur des « comptes » rendus et sur la possibilité de vérification par un contrôleur. L'autorité de protection des données personnelles pourrait faire l'effort d'établir recommandations et standards permettant d'encadrer les procédures des responsables de traitements, qui elles-mêmes faciliteraient les contrôles. Le responsable de traitement saurait ainsi ce qu'il doit conserver et être en mesure de présenter en cas de contrôle pour prouver qu'il s'est comporté de manière loyale. Ce type de processus donnera du corps au principe de l'*accountability* dans les données personnelles et permettra l'émergence d'une sorte de norme de qualité « CNIL ». Il faut se demander parallèlement à cela comment « outiller » les individus, même si les outils seuls ne suffisent pas. Par exemple, on peut imaginer des agents logiciels qui seraient des « représentants » de la personne sur la machine, pour la gestion de leurs données personnelles, ce qui reviendrait à une forme sophistiquée de paramétrage. »

Daniel Le Métayer et Claude Castelluccia

... QUEL RÔLE POUR LES AUTORITÉS DE PROTECTION DES DONNÉES DEMAIN ?

L'évidence de l'insuffisance du seul cadre national est telle que tous en appellent à une plus grande coopération entre les autorités au niveau international, et singulièrement au niveau européen. Ces échanges doivent se faire à la fois sur la définition de normes, mais également dans le dialogue avec les grands acteurs publics comme privés. Pour Yves Poullet et Cécile de Terwangne, les autorités sont des « chiens de garde de la vie privée », tendant de plus en plus vers des « juridictions » parce qu'on leur donne des missions de contrôle et de par leur composition : elles deviennent donc des administrations juridiques classiques. Ces commissions de protection ne sont donc pas des lieux de débat, elles sont cadenassées dans leur mission de protecteur. Elles doivent demain se positionner en amont, au niveau des réflexions, des analyses prospectives et des agendas de recherche, comme l'évoquent par exemple Françoise Roure et Antoinette Rouvroy. Meryem Marzouki pense d'ailleurs qu'il faut absolument favoriser le *privacy by design* dans les contrats de recherche. Un vrai travail dans la durée doit émerger entre les autorités et la communauté des chercheurs. Il est en effet primordial, pour Pierre-Jean Benghozi, de coupler, au niveau européen, politique de protection et politique d'ouverture et de facilitation afin de favoriser l'innovation dans des conditions acceptables. Selon Yves Deswarte, la CNIL pourrait motiver les organismes de financement de la recherche, ou encore aider à lancer des projets-pilotes d'outils de protection de la vie privée. Les entreprises quant à elles, ne se lanceront pas si elles n'y sont pas obligées. La CNIL a un rôle de vitrine pour ces technologies de protection et peut même favoriser leur développement.

Les autorités doivent également élargir leur horizon en travaillant avec de nouveaux partenaires. Jérémie Zimmermann, Jean-Marc Manach, Yves Deswarte et Philippe Lemoine pensent par exemple au monde — complexe et protéiforme — du logiciel libre (voir « Vers de nouvelles fractures numériques ? », page 40).

À long terme, la CNIL doit, pour Bernard Stiegler, être repensée pour favoriser voire animer la nécessaire émergence d'une société civile numérique. En fait, par analogie avec la « pharmacologie du numérique » évoquée par Bernard Stiegler, la CNIL doit être un médecin : elle doit établir des diagnostics et « prescrire ». Mais elle doit aussi permettre au patient de gérer lui-même son « état de santé » numérique, comme tout médecin devrait le faire. Philippe Lemoine rappelle qu'à l'origine, la CNIL était envisagée comme une « conscience sociale de la Nation » et qu'elle n'a jamais saisi réellement ce rôle : « La question dont la CNIL est détentrice est une des plus lourdes et importantes qui soit, bien plus que celle des droits de propriété intellectuelle sur les biens d'information. Elle doit faire de la croissance externe en accueillant des nouveaux sujets de débat des libertés et des droits numériques, comme par exemple ceux liés à l'ouverture des données. »

Après tout, comme le rappelle Yann Leroux, quoi qu'il arrive, le rôle d'une autorité est toujours important, ne serait-ce que parce que son existence permet de se plaindre de son action...

« API-SER » LA MAÎTRISE DE SES DONNÉES ?

L'innovation dans la régulation doit s'incarner dans des outils et de nouveaux modes d'action pour les données personnelles.

Pour Arnaud Belleil, les principes de protection des données sont encore robustes. Il convient en revanche de les rendre plus

opérationnels en trouvant des moyens de les adapter aux usages actuels. Ainsi, le véritable enjeu est de permettre un rééquilibrage des asymétries d'informations existant entre les organisations et les individus. Il ne s'agit plus d'appréhender le droit des personnes sur leurs données dans une logique défensive, ou comme un recours en cas de litige, mais bien d'instaurer de nouvelles modalités d'interactions entre les acteurs. Au cœur de ces dernières se trouve le principe d'un accès transparent et symétrique aux données détenues. Dominique Cardon appuie cette rénovation nécessaire où l'utilisateur pourrait décider des données à conserver ou à effacer dans le *CRM* de l'opérateur par exemple, au moyen d'une interface simple qui se présenterait comme un tableau de bord de ses données personnelles.

C'est d'ailleurs ce que Daniel Kaplan souhaite promouvoir au travers du projet « Mes Infos » de la Fing qui vise à rééquilibrer les rapports entre les individus et les organisations (voir « La donnée au cœur des modèles d'affaires : demain, tous traders de données ? », page 15). Partant du principe que les nouvelles données « ouvertes » sont des données personnelles, il s'agit d'étendre la logique de l'*Open Data* à ces données (qui ne sont pas ouvertes au public mais uniquement à l'utilisateur qu'elles concernent). Techniquement, un moyen de faciliter l'accès direct et transparent est de passer par des *API (Application Programing Interface)* — c'est-à-dire des interfaces de programmation — que l'on peut schématiser comme « une prise » que les organisations mettraient à la disposition de leurs utilisateurs, et sur laquelle ils pourraient « se brancher » pour accéder et modifier leurs données. Le recours à une *API* rend ainsi les données plus directement accessibles pour les utilisateurs en même temps qu'il suppose de les délivrer dans un format standardisé, lisible par d'autres machines. En ce sens, militer pour l'ouverture d'*API* ne renvoie pas seulement à une architecture technique mais à un design plus général facilitant la réutilisation des données en les délivrant dans un format qui favorise leur interopérabilité.

VERS DE NOUVELLES RESPONSABILITÉS POUR LES HÉBERGEURS ?

Selon Paul-Olivier Gibert, il faudrait instaurer dans la loi un statut spécifique pour l'hébergeur qui ne serait pas responsable du traitement des données. De cette manière, il n'aurait pas la possibilité de conserver un droit d'utilisation pour son propre compte des données, et aurait alors comme seule obligation la mise à disposition de la plateforme. Il faudrait accompagner le statut d'hébergeur par la mise en place d'une certification de la politique de l'organisme en matière de *privacy*. Il pourrait par exemple être obligé de fournir à un instant T et dans la durée les outils nécessaires à la protection des données personnelles (comme le *privacy by design*, des comptes configurés par défaut au strict minimum...). Et un argument central dans la position de Paul-Olivier Gibert repose sur la labellisation de l'hébergeur, un thème abondamment commenté par les experts.

QUID DES LABELS ?

Le mécanisme de certification par les labels semble être un axe intéressant pour nombre d'experts. Pour Emmanuel Kessous, un marché des labels est susceptible de se développer dans la mesure où ils peuvent constituer un signal de confiance en véhiculant une réputation positive d'une entreprise. Le label représente ainsi une opportunité économique en particulier pour les entreprises qui voudraient se différencier.

Les labels peuvent aussi s'avérer dangereux dans la mesure où ils peuvent être manipulés par les entreprises. Pour Philippe Lemoine, elles sont susceptibles d'adopter des comportements tactiques en vue d'être labellisées. Pour cette raison, Nathalie Mallet-Poujol estime que leur crédibilité est fortement dépendante des contrôles et des amendes associés. Elle ajoute qu'il est nécessaire que le mécanisme de certification par les labels soit opposable. Yves Deswarte estime pour sa part que la labellisation est un dispositif incitatif mais qu'il demande des efforts importants de sensibilisation en direction des utilisateurs. Si l'idée est séduisante, la gouvernance peut s'avérer compliquée et suppose au préalable l'instauration d'un référentiel avec homologation de la CNIL.

Finalement, Emmanuel Kessous ouvre une voie intermédiaire avec l'instauration d'un socle légal minimal complété par plusieurs niveaux de labellisation possibles. Les entreprises pourraient de cette manière être incitées à aller vers le label pour acter de leur transparence et de leur excellence en matière de traitement des données. ■

REPENSER LE DROIT DU NUMÉRIQUE ?

« En matière de Droits de l'Homme, les droits fondamentaux n'ont pas tous le même statut, certains sont plus importants que d'autres. Le droit au respect de la dignité de la personne est le seul droit indérogeable. La dignité doit être protégée comme une valeur absolue. La question des données personnelles pourrait tenir compte de cette hiérarchie implicite entre les droits fondamentaux. La Convention européenne des Droits de l'Homme étant un « catalogue » plus complet quand il s'agit de parler de Droits de l'Homme, il faudrait établir un lien entre les sujets Informatique et Libertés et les droits et libertés énumérés dans la Convention européenne. »

Mireille Delmas-Marty

DROIT À L'OUBLI : UTOPIE POLITIQUE OU ENJEU VÉRITABLE ?

Il y a une mauvaise compréhension du droit à l'oubli, explique Arnaud Belleil : il ne s'agit ni d'un droit à effacer systématiquement toutes ses données, ni d'un droit à falsifier les archives et donc le passé, comme le fait le personnage principal du roman *1984*. Pour Isabelle de Lamberterie, le droit à l'oubli doit se penser dans une société de droit à la conservation et de devoir de mémoire.

En permettant à l'individu d'obtenir l'effacement de certaines données, ce droit vise, en réalité, à lui permettre de ne plus voir sa vie entravée par le rappel de son passé. La place des décisions de justice sur Internet, dont le principe d'anonymisation a été posé par la CNIL, en est un bon exemple. Dominique Cardon va au-delà en jugeant que « le droit au mensonge est essentiel » : les technologies ne doivent pas empêcher les personnes de cacher certaines informations. Pour Olivier Iteanu, il faudrait organiser le droit à l'oubli dans le temps, peut-être en liaison avec le droit à l'information, en prévoyant un droit à l'anonymisation des articles en ligne après un certain délai. D'autres propositions sont faites : Yves Deswarte envisage l'attribution d'une date d'effacement lors de chaque cession de données. Dominique Cardon évoque la mise en place, dans les espaces conversationnels, d'un réel système d'évaporation, d'érosion des données personnelles. Il insiste sur l'intérêt qu'il y aurait à rappeler aux « réseaunautes » ce qu'ils ont indiqué, par exemple, durant l'année précédente pour les mettre en mesure de trier, effacer ou conserver leurs données (voir encadré). Emmanuel Kessous propose, pour sa part, l'inscription d'une date de péremption des données sur les réseaux sociaux, date qui tiendrait compte du type de contenu, ainsi que le développement d'outils destinés à contrôler l'effacement qui a été programmé (même si rien ne permet de garantir techniquement le respect de la règle en cas de copie de la donnée). Il mentionne également la possibilité que les mémoires caches soient systématiquement supprimées tous les 18 mois, même si sa préférence irait à des solutions moins extrêmes. Dans le même sens, Daniel Le Métayer et Claude Casteluccia estiment que, si le droit à l'oubli est un concept qui « est en réalité impossible à imposer à l'échelle d'Internet », cela ne signifie pas pour autant qu'il soit inenvisageable de développer des outils permettant de faciliter l'effacement systématique des données et la vérification après coup que ces mécanismes n'ont pas été contournés (problématique de l'*accountability* évoquée supra).

Pierre-Jean Benghozi aborde la question sous un autre angle, celui du droit à la mémoire, aussi important sur Internet que le droit à l'oubli : peut-on dire que les contenus appartiennent encore à la personne qui les a mis en ligne ? Il prend l'exemple du service de sauvegarde de fichiers en ligne *Dropbox* qui stipule dans ses conditions générales d'utilisation que tout fichier stocké dans le programme lui appartient légalement. Il en résulte que rien n'oblige ces opérateurs de service à en garder la trace. Comment l'internaute pourra-t-il se

SAVOIR GÉRER SA MÉMOIRE DIGITALE

Clive Thompson, éditorialiste de la revue Wired, explique qu'à terme, les utilisateurs vont devoir se comporter comme de vrais archivistes. Jusqu'à présent les individus disposaient de peu d'enregistrements sur leur vie privée. Mais, avec les espaces de publication en ligne, les modalités de conservation se transforment. Les capacités de mémorisation à l'extérieur se développent et cette mémoire change de nature en devenant digitale. Il faudra bientôt gérer des années de courriels, d'énormes amas de souvenirs et donc savoir jeter. Avoir une mentalité d'archiviste consisterait à apprendre à ne pas enregistrer et à éliminer les traces jugées non pertinentes. Cet auteur explique que les individus ont naturellement tendance à être durs avec leurs êtres passés. Le regard de l'archiviste devrait aussi leur permettre de se réconcilier avec eux-mêmes.

retourner contre ce service le jour où il constatera l'effacement des données le concernant ? La question d'un droit à l'archivage des données personnelles lui paraît encore plus problématique que le droit à l'oubli, surtout depuis le développement du *Cloud Computing*. La question de la définition d'un droit à la portabilité des données n'en est que plus essentielle.

LA PORTABILITÉ DES DONNÉES EST UNE EXIGENCE FORTE. QUELS OUTILS ?

La mise en place d'un droit à la portabilité des données personnelles devrait constituer un levier essentiel pour leur protection. Jérémie Zimmermannn le relie à la question du droit d'accès, qui doit être repensé de manière à y associer une exigence d'interopérabilité, le recours à des formats ouverts et le droit de choisir le format de communication de ses données. Dès lors, la portabilité des données devrait conduire à créer, si possible au niveau européen, une véritable « obligation de transmission des données personnelles vous concernant ». Pierre-Jean Benghozi reprend l'idée de standards d'interopérabilité et insiste sur la nécessité de pouvoir créer des sauvegardes de ses données personnelles.

Pour Daniel Le Métayer, l'absence de portabilité est une des causes du déséquilibre entre l'utilisateur et des services comme Facebook, car l'individu y perd la possibilité d'exercer ses droits, en particulier celui de pouvoir renoncer sans contrainte à un service en ligne. Dans son livre *The Intention Economy*, Doc Searls résume cette asymétrie en expliquant que les conditions générales d'utilisation de ces services sont généralement « du velcro » du point de vue du service et « de la glu » du côté de l'utilisateur. Le droit à la portabilité est déjà présent dans le droit à la consommation (portabilité du numéro de mobile, portabilité bancaire). Or, plusieurs de nos experts soulignent que la marchandisation des données personnelles fait émerger de nouvelles problématiques de régulation qui mêlent protection de la vie privée et droit à la consommation.

Daniel Kaplan ne croit pas en la bonne volonté des acteurs économiques pour mettre fin aux barrières à l'entrée qui protègent leurs marchés. Pour lui, il faudra leur imposer la portabilité, ce qui le conduit par ailleurs à militer pour le développement de réseaux sociaux acentrés (type *Diaspora*).

DE NOUVEAUX DROITS SUBJECTIFS POUR RÉPONDRE AUX NOUVEAUX DÉFIS

Un grand nombre d'experts consultés jugent indispensable de reconnaître aux particuliers un rôle plus actif dans le dispositif de régulation qui leur est appliqué. Antoinette Rouvroy propose, pour faire face aux nouveaux risques d'atteinte aux droits et libertés des personnes, la reconnaissance, dans le prolongement du droit d'accès, de nouveaux droits :

- le droit « à un environnement mental non pollué », déjà promu par divers collectifs anti-publicité ;
- le droit de se définir par soi-même, car l'identité n'est pas un phénomène mais un processus et l'on construit son identité en rendant compte de soi (voir les travaux de la philosophe américaine Judith Butler) ;
- le droit de refuser son profilage par des automatismes qui jugent et classifient les personnes à leur insu ;
- le droit d'accéder aux raisons pour lesquelles un profilage particulier vous a été attribué.

Parallèlement, Paul-Olivier Gibert souhaite que les particuliers puissent disposer d'outils personnels, tant juridiques que techniques, de protection des données pour protéger eux-mêmes leurs données et garder un certain contrôle sur leur circulation (par le chiffrement...) et leur effacement.

DROIT DE PROPRIÉTÉ SUR SES DONNÉES : UNE FAUSSE BONNE IDÉE ?

Alain Bensoussan note que certains réseaux sociaux entretiennent d'ores et déjà l'ambiguïté en demandant à leurs usagers de signer un contrat de licence. Pourtant, attribuer aux personnes un droit de propriété sur leurs données personnelles n'aurait rien d'anodin. Cela reviendrait à dire pour Meryem Marzouki, que la protection des données n'est plus un droit fondamental, ni un droit de la personnalité. Elle n'en serait pas facilitée, loin de là. Un « droit de propriété » implique en effet le « droit d'être dépossédé », ajoute Nathalie Mallet-Poujol, alors qu'un droit de la personnalité est inaliénable tout en permettant, s'il y a lieu de le faire, des compensations financières, un contrôle de l'usage... et l'effacement de ce droit devant un intérêt public.

Le risque de renforcer le clivage social est souligné par Francis Jauréguiberry : « Les plus pauvres pourraient être tentés de vendre leurs données, tandis que les données des plus riches seraient plus facilement préservées. » Christine Balagué s'interroge sur la portée du droit qui serait reconnu : « Il y a des chances que le droit de propriété des particuliers ne puisse concerner que leurs données brutes et non les données scorées ou enrichies par une entreprise. » Alain Rallet et Fabrice Rochelandet précisent que, de toute façon, la valeur reconnue à la « propriété » serait nécessairement variable, car fonction de l'usage attendu. Il serait donc impossible de donner une valeur à des données en dehors d'un traitement ou d'un contexte spécifique. Pierre-Jean Benghozi ajoute que le droit exclusif reconnu aux individus sur leurs données rencontrerait les mêmes limites que le droit d'auteur, les mêmes difficultés pour se faire respecter, pour trouver les ayants droit... Il serait donc largement illusoire.

RENFORCER CERTAINS VOLETS DE LA RÉGLEMENTATION EN VIGUEUR

Nathalie Mallet-Poujol insiste sur l'intérêt qu'il y aurait à donner toute sa portée au principe de finalité. Bien que celui-ci ait été conçu comme la pierre angulaire du système juridique en vigueur, il a toujours été sous-employé. Ses violations sont nombreuses. La jurisprudence se contente trop souvent, par commodité, d'invoquer le principe de proportionnalité et ne dit rien de la légitimité ni de l'opportunité de la finalité du traitement. Pourtant, cet examen laisserait moins de place aux appréciations subjectives, estime-t-elle. Antoinette Rouvroy propose un resserrement des critères d'emploi, d'une part, des profils de groupe, notions statistiques qui peuvent être à l'origine de fortes discriminations, d'autre part, du *data-mining*. Enfin, Claude Casteluccia et Daniel Le Métayer souhaitent voir posé le principe que toute utilisation de données doit laisser des traces vérifiables (principe d'*accountability*).

POUR DES DROITS DE L'HOMME NUMÉRIQUE

> **« La dignité numérique correspondrait aux droits et principes fondamentaux, naturels et universels, qui permettent de vivre dans le monde virtuel : le droit à l'anonymat car on a rarement besoin d'utiliser son identité réelle sur Internet ; le droit de changer de vie ; le droit de gérer de multiples identités, de créer des avatars, doubles virtuels spécialisés constitués d'agrégats de données personnelles qui sont des décalques tronqués de notre identité ; le droit d'utiliser un identifiant non signifiant, sans référence à son identité réelle, et un domicile virtuel ; un droit à la remise à zéro, variante du droit à l'oubli ; un droit à la transparence, au sens de « tu ne me feras pas quelque chose que je n'aurai pas compris ». »**
>
> **Alain Bensoussan**

Face à des sociétés privées se comportant comme des quasi-États qui gèrent des identités individuelles et cherchent à les profiler pour mieux les commercialiser, il faut promouvoir les Droits de l'Homme dans le cyberespace. Une telle démarche pourrait s'appuyer sur plusieurs initiatives : la « déclaration d'indépendance du cyberespace », publiée le 8 février 1996 à Davos par John Perry Barlow, co-fondateur de l'*Electronic Frontier Foundation*, qui est à l'origine de la pensée de l'Internet libertaire ; la Charte des droits et principes d'Internet, issue d'un groupe de travail international constitué en 2005 surtout de juristes et en discussion depuis lors ; le projet rédigé par le journaliste blogueur Jeff Jarvis, centré sur les droits numériques. En France, un projet de loi est envisagé et, de façon générale, l'idée est soutenue par la Ligne des Droits de l'Homme, au nom de laquelle Maryse Artiguelong et Jean-Claude Vitran estiment qu'il faut « constitutionnaliser le droit à la protection des données personnelles et aller vers un *habeas corpus* numérique ». ■

COMMENT DIRE LE DROIT FACE AUX ÉVOLUTIONS DES TECHNOLOGIES ET DES PRATIQUES SOCIALES ?

Mireille Delmas-Marty, vous appliquez à la protection des données l'idée de « flou du droit ». Ne craignez-vous pas que ce concept ne remette en cause les principes de clarté et d'opposabilité des règles juridiques ?
Mireille Delmas-Marty : Pas du tout ! Le « flou du droit » n'est pas synonyme d'obscurité ou d'inefficacité, mais de souplesse. Il permet, à certaines conditions, d'articuler l'un et le multiple. C'est le moyen de disposer à la fois de principes communs et de règles techniques et pratiques différentes, adaptées aux situations locales. Cela permet de ménager des marges d'appréciation et d'adaptation dans un droit partagé. La notion de « marge nationale d'appréciation », utilisée par la Cour Européenne des Droits de l'Homme, en est une illustration. Elle vise à conjuguer l'universalité des droits et libertés de la Déclaration universelle des Droits de l'Homme et la diversité des cultures, dont la valeur pour l'humanité a été proclamée en 2005 par l'UNESCO avec la Convention sur la protection de la diversité des expressions culturelles.

Ne faut-il pas encadrer efficacement les marges d'appréciation qui sont ainsi concédées aux différents acteurs ?
Bien sûr, un organe unique doit contrôler la compatibilité avec les principes communs des diverses solutions retenues en droit positif, afin d'éviter tout risque d'arbitraire. Car le flou appelle, non pas l'absence de rigueur, mais un surcroît de rigueur et de transparence. Il doit être assorti d'indicateurs sur la marge de variabilité acceptable, pour que celle-ci soit compréhensible et prédictible. Il faut aussi expliciter les seuils de compatibilité. Ainsi organisé, le droit peut être évolutif et innovant, car il ne sera plus nécessaire de modifier sans cesse la norme de référence.

Cette approche n'est-elle pas particulièrement adaptée au niveau européen ?
C'est vrai. Une marge d'appréciation est d'ailleurs implicitement reconnue chaque fois qu'un texte européen renvoie à l'ordre public national. Pourtant, il est actuellement de moins en moins fait appel à cette technique, car les autorités préfèrent uniformiser le droit, quitte à oublier les particularismes des droits nationaux. C'est ainsi qu'en matière de protection des données, il est prévu de passer d'une directive à un règlement. Or, les atteintes aux données personnelles sont souvent liées à des intérêts économiques nationaux ou à des spécificités culturelles. Si bien que l'uniformisation des systèmes juridiques des pays européens ne me semble pas être un objectif très réaliste.

En quoi l'idée d'un droit flou est-elle une idée d'avenir, en particulier pour la protection des données ?
L'application d'une « logique floue » est devenue indispensable à l'échelle européenne ou mondiale.
Elle est particulièrement nécessaire dans les États démocratiques dans les domaines de la vie privée et, plus généralement, pour chaque liberté assortie de restrictions. Dans le domaine de la protection des données personnelles, un tournant s'est produit avec les attentats du 11 septembre 2001 et la réaction qui s'en est suivie. Des dérives ont eu lieu, permises par des innovations technologiques. L'ambivalence des nouvelles technologies est maintenant éclatante : elles permettent autant le renforcement de la démocratie que la surveillance généralisée de chacun sur tous. Comment préserver les aspects positifs tout en luttant contre les dérives ? On peut répondre aux innovations technologiques par des innovations juridiques, mais il est très difficile de penser un droit évolutif. Les réponses juridiques sont souvent en retard sur les technologies. Or, que l'on parle de bioéthique ou de protection des données, il est nécessaire d'adapter en permanence la construction de la norme juridique pour tenir compte de l'accélération des innovations. Les autorités administratives indépendantes sont sans doute mieux armées pour jouer ce rôle, utilisant à la fois *soft law* et *hard law* et n'hésitant pas à mettre en œuvre une logique de gradation.

Faut-il en conclure qu'il n'y a plus de place pour du « droit dur » ?
Certainement pas. Le droit dur est indispensable, mais il peut être flou (imprécis) dans les conditions évoquées *supra*, alors le droit mou (non obligatoire) et le droit doux (non sanctionné) peuvent être précis. Cette *soft law* a une fonction particulière : exprimer les engagements qui ont été pris au plan éthique. Plus généralement, il ne faut pas faire un éloge inconditionnel du flou. Plus on laisse de marge d'interprétation au juge, plus il faut lui fournir des indicateurs précis et des grilles de pondération de ces indicateurs. Ces éléments pourraient, par exemple, prendre la forme de recommandations de la CNIL comprises comme autant de normes comportementales de référence.

ANNEXE GRILLE D'ENTRETIEN

La vie privée, les libertés et les données personnelles à l'horizon 2020. Quels enjeux de protection et de régulation pour la CNIL ? Représentations, perceptions et attentes des acteurs.

LES ÉVOLUTIONS TECHNOLOGIQUES, ÉCONOMIQUES ET SOCIÉTALES AYANT UN IMPACT SUR LA PROTECTION DE LA VIE PRIVÉE, DES LIBERTÉS ET DES DONNÉES PERSONNELLES

Évolutions et impacts hier et aujourd'hui

- Quels sont parmi les changements majeurs intervenus au cours des dix dernières années, ceux qui vous paraissent avoir eu un impact sur la protection de la vie privée, des libertés et des données personnelles ?

S'agissant plus particulièrement des comportements individuels en matière de vie privée et des libertés, d'exposition de soi ou encore face à la sollicitation de données personnelles :

- Les changements sociaux que l'on constate concernant la relation des individus à leurs données personnelles, à la protection de leur vie privée sont-ils, selon vous, liés essentiellement, aux développements technologiques ou s'agit-il de transformations intrinsèques aux sociétés contemporaines ?
- Finalement, considéreriez-vous que l'édifice Informatique et Libertés (conçu en 1978 et modifié en 2004) a été suffisamment « adapté » face à ces transformations passées et en cours ? Pour quelles raisons ?

Évolutions et impacts dans les 10 prochaines années

- Quels seront, selon vous, les risques (menaces), émergents ou nouveaux, susceptibles de peser sur la vie privée, les libertés ? Faudra-t-il tracer de nouvelles « lignes rouges » ?
- Y aura-t-il de nouvelles données personnelles « sensibles » et d'autres qui ne le seront plus autant ?
- Comment vont se redessiner, selon vous, les frontières entre espace public et espace privé ?
- Comment peuvent évoluer les contours de la notion de vie privée ?

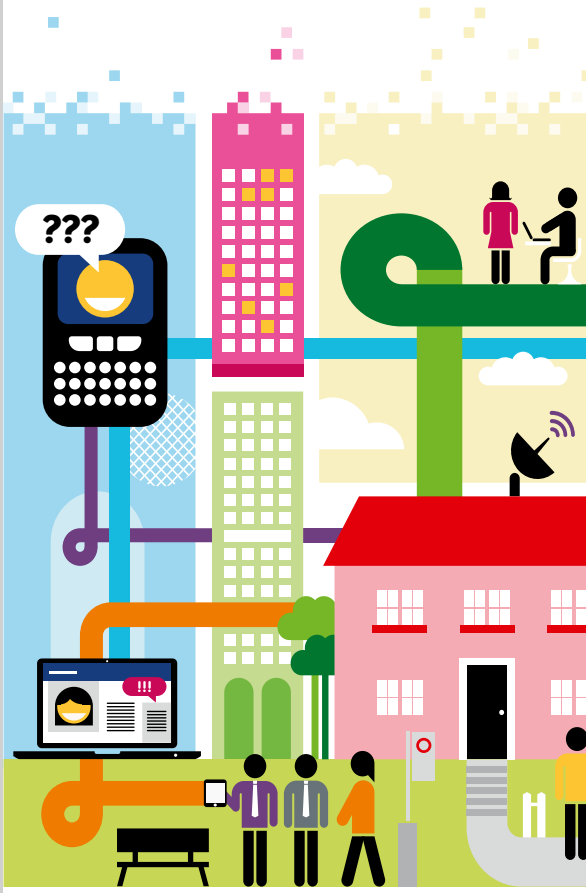
QUELLES PROTECTIONS ET QUELLES RÉGULATIONS DEMAIN ?

- D'ici les 10 prochaines années, quelles sont les principales transformations (celles que vous connaissez déjà et celles que vous percevez comme possibles/vraisemblables, voire celles que vous redoutez) qui vous paraissent porteuses d'enjeux majeurs en matière de protection de la vie privée, des libertés et des données personnelles ?
- Quelle forme de régulation voyez-vous pour demain : autorégulation par les individus, régulation juridique, régulation marchande, régulation par les technologies, corégulation ?
- Les droits consacrés par les lois de protection des données (droit d'accès et de rectification de leurs données personnelles, droit d'information, droit d'opposition et droit au consentement préalable) vous semblent-ils efficaces face aux transformations à venir ? De nouveaux droits sont-ils à définir (ex : droit de propriété sur ses propres données personnelles) ?
- Des « régulations par les technologies », par des outils informatiques permettant aux individus de protéger leurs données (les « technologies de protection de la vie privée » *PETs*, les techniques d'« obfuscation » ou « assombrissement »...) doivent-elles être encouragées ?, comment favoriser le développement d'un marché pour les *PETs* ?
- La certification ou la labellisation peut-elle y concourir ? Par qui ?
- Quels rôles seront amenés à jouer demain les entreprises dans la régulation de la vie privée ? des données personnelles ? Faut-il introduire de nouvelles obligations à leur égard ? Faire intervenir dans la régulation d'autres acteurs ? (opérateurs, concepteurs de technologies...). Quelles sont les formes de régulation par le marché qui pourraient émerger ?
- Quelle implication demain de la société civile en matière de protection de la vie privée et des libertés (degré, formes, nouveaux acteurs) ?

VOTRE LECTURE DES ÉVOLUTIONS (PERÇUES, SOUHAITÉES) DU RÔLE D'AUTORITÉS, COMME LA CNIL, DEMAIN

Concernant notamment les aspects suivants :

- Pouvoirs, modes d'intervention et évaluation de leur efficacité
- Relations avec les parties prenantes, les acteurs
- Statut, composition et moyens financiers
- Rôle au plan européen et international
- Doit-on aller vers une autorité de protection des données européenne ?



CNIL.

Commission Nationale de l'Informatique et des Libertés

Commission Nationale de l'Informatique et des Libertés
Direction des Études, de l'Innovation et de la Prospective

8, rue Vivienne - CS 30223
75083 Paris CEDEX 02
tél. : 01 53 73 22 22
fax : 01 53 73 22 00
deip@cnil.fr

www.cnil.fr

CNIL
Commission Nationale de l'Informatique et des Libertés