

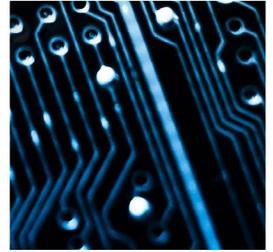


LES **AVIS**
DU CONSEIL
ÉCONOMIQUE,
SOCIAL ET
ENVIRONNEMENTAL



**Les données numériques :
un enjeu d'éducation
et de citoyenneté**

Éric Peres
Janvier 2015



RÉPUBLIQUE FRANÇAISE
LIBERTÉ - ÉGALITÉ - FRATERNITÉ



CONSEIL ÉCONOMIQUE
SOCIAL ET ENVIRONNEMENTAL


Les éditions des
Journaux officiels

2015-01
NOR : CESL1500001X
Lundi 19 janvier 2015

JOURNAL OFFICIEL DE LA RÉPUBLIQUE FRANÇAISE

Mandature 2010-2015 – Séance du 13 janvier 2015

LES DONNÉES NUMÉRIQUES : UN ENJEU D'ÉDUCATION ET DE CITOYENNETÉ

Avis du Conseil économique, social et environnemental
présenté par

M. Éric Peres, rapporteur

au nom de la
section de l'éducation, de la culture et de la communication

Question dont le Conseil économique, social et environnemental a été saisi par décision de son bureau en date du 13 mai 2014 en application de l'article 3 de l'ordonnance n° 58-1360 du 29 décembre 1958 modifiée portant loi organique relative au Conseil économique, social et environnemental. Le bureau a confié à la section de l'éducation, de la culture et de la communication la préparation d'un avis intitulé : *Les données numériques : un enjeu d'éducation et de citoyenneté*. La section de l'éducation, de la culture et de la communication, présidée par M. Philippe Da Costa, a désigné M. Eric Peres comme rapporteur.

Sommaire

■ Avis	6
■ Introduction	6
■ Constats et enjeux	9
■ Enjeux et usages du Big Data : le traitement des données numériques au cœur des transformations économiques et sociales	9
■ Big Data : Origine et définition	9
↳ Caractéristiques de la donnée	9
↳ Explosion, massification et stockage des données	11
↳ Production et traitement des données : les caractéristiques du Big Data	14
↳ Des données numériques aux métadonnées	15
↳ Le Big Data et la règle des 3V : volume, variété, vitesse	16
↳ <i>Big Data</i> et système décisionnel	16
■ La donnée numérique : valorisations sociales, économiques et environnementales	17
↳ La donnée numérique, nouvelle ressource économique	17
↳ Opportunités du Big Data : de la santé à la maîtrise énergétique	19
↳ Le domaine de la recherche en général et médicale en particulier	20
↳ Transition numérique et développement durable	22
↳ De la ville intelligente (<i>smart city</i>) à la mobilité connectée	23
■ La citoyenneté à l'ère du numérique, un nouveau pouvoir d'agir	24
↳ Culture, éducation et nouveaux accès aux savoirs à l'ère du numérique	24
↳ Nouveaux pouvoirs de création et d'échanges : des <i>FabLabs</i> à l'économie collaborative	30
↳ Accès aux données publiques : un nouveau regard citoyen	31
↳ Les nouveaux enjeux sociaux et culturels de la fracture numérique	35
■ L'enjeu de la « souveraineté numérique »	37
↳ La valeur économique captée par les GAFA (Google, Apple, Facebook, Amazon)	38
↳ L'illusion du tout gratuit	39

■ Les libertés à l'ère du numérique:	
■ une relation sous tension	40
■ La collecte exponentielle des données face aux risques de l'hypersurveillance	41
↳ De la collecte de données au fichage généralisé : de l'affaire Safari à l'affaire Snowden	41
↳ Big Data ou Big Brother ?	42
■ Vie privée et protection des données personnelles	45
↳ La protection de la vie privée : risques et inquiétudes	46
↳ <i>Open Data</i> et données personnelles	48
↳ Objets connectés et algorithmes : nouveaux enjeux et nouveaux risques	51
↳ Puissance des plateformes et pouvoir des algorithmes	55
■ Protection et maîtrise des données : nouveaux enjeux et nouvelles approches	58
■ La protection des données à caractère personnel : un impératif démocratique	59
↳ La loi « Informatique et Libertés »	59
↳ Les différents textes et accords-cadres : de la Convention 108 à la Directive 1995	63
↳ Le projet de règlement européen	65
■ La protection des données personnelles : entre régulation et autorégulation	65
↳ Complémentarités de la loi et de la technologie	66
↳ La maîtrise des données personnelles : entre confiance et réciprocité	67
■ Préconisations	71
■ Promouvoir l'éducation au numérique	71
■ Accompagner et soutenir le rôle éducatif de la famille dans la transition numérique	72
↳ Promouvoir des campagnes publiques de sensibilisation à la protection des données personnelles	72
↳ Renforcer la protection des mineurs	73
■ Soutenir le déploiement d'une éducation au numérique de la maternelle à l'enseignement supérieur	74

↳ Favoriser l'acquisition d'une éducation à l'esprit critique du développement et de la maîtrise des techniques numériques	75
↳ Renforcer l'Éducation au numérique dans les programmes scolaires	75
↳ Promouvoir la certification renforcée via le brevet informatique et internet B2i	76
↳ Renforcer la formation au numérique au sein de l'Education nationale et de l'enseignement supérieur	77
↳ Établissements scolaires et le déploiement des outils numériques	79
■ Lutter contre les nouvelles fractures numériques	80
↳ Redynamiser les politiques publiques sur les territoires	81
↳ Revitaliser les Espaces publics numériques (EPN)	81
↳ Repenser un « service universel » dédié aux actions d'accompagnement des citoyens vers la maîtrise des données numériques	84
↳ Soutenir les initiatives des « tiers-lieux » pour renforcer les réseaux d'accompagnement à la maîtrise du numérique	85
↳ Lutter contre l'enfermement de l'internet en renforçant le lien intergénérationnel.	86
■ Entreprises, administrations : quelle éducation au numérique ?	87
■ Promouvoir une politique de sécurité et de protection des données au sein des entreprises et des administrations	87
↳ Faire de la protection des données personnelles un nouvel avantage compétitif de l'entreprise.	88
↳ Développer le <i>Privacy by design</i> comme facteur de différenciation compétitive	90
↳ Promouvoir une éthique numérique au sein des entreprises et des administrations	91
■ Bâtir une politique publique du numérique et construire une stratégie industrielle	93
↳ Développer une stratégie numérique pour les données et les technologies de l'État	93
↳ Etablir de nouveaux principes « <i>Design</i> et ergonomie » pour la démocratie à l'ère numérique	94
↳ Développer une politique publique du numérique articulée à une politique industrielle en faveur notamment des jeunes « pousses ».	95
↳ Maîtriser les impacts énergétiques pour une meilleure protection des données	97
■ Bâtir un cadre réaliste et exigeant de protection des données à l'ère du numérique	99

■ Créer un cadre de protection des données au niveau international	100
✎ Promouvoir un cadre protecteur au niveau international	100
✎ Favoriser une culture européenne du numérique garante de l'architecture du net	101
✎ Améliorer et soutenir le projet de règlement européen sur la protection des données	103
✎ Sécuriser les transferts de données à l'international	104
■ Renforcer les pouvoirs de régulation et promouvoir la co-régulation	105
✎ Renforcer les pouvoirs de régulation de la CNIL	105
✎ Promouvoir la prospection et la labellisation	109
✎ Revoir l'encadrement des nouvelles données sensibles	109
✎ Protéger les données personnelles au sein de l' <i>open data</i>	110
■ Rechercher les voies et moyens pour une maîtrise par les individus de leurs données personnelles	111
✎ Revoir les Conditions générales de vente (CGV) et les Conditions générales d'utilisation (CGU)	113
✎ De la récupération au partage des données, le rôle des tiers de confiance	115

■ Déclaration des groupes _____ 116

■ Scrutin _____ 133

Annexes _____ 135

Annexe n° 1 : composition de la section de l'éducation,
de la culture et de la communication _____ 135

Annexe n° 2 : liste des personnes auditionnées _____ 137

Annexe n° 3 : glossaire _____ 138

Annexe n° 4 : table des sigles _____ 141

Annexe n° 5 : bibliographie _____ 142

LES DONNÉES NUMÉRIQUES : UN ENJEU D'ÉDUCATION ET DE CITOYENNETÉ¹

Avis

Introduction

Data-driven management, *data marketing*, désintermédiation, prescription algorithmique... pour qui veut s'immerger dans l'univers du *Big Data*, le passage obligé par une explication de texte est requis. Dans les années quatre-vingt-dix, l'internet était encore un outil à taille humaine et les résultats qui apparaissaient à la suite d'une requête étaient le résultat d'avis d'experts humains « identifiables ». Près d'un quart de siècle plus tard, une requête sur un moteur de recherche peut générer l'analyse des données de 200 millions de sites web. Face à cet imposant volume de données en circulation, seule une poignée d'entreprises ont su déployer une infrastructure de type *Big Data* capable de servir des bases d'utilisateurs supérieures à 500 millions de personnes (plus d'un milliard pour Google et Facebook, plus de 900 millions pour Microsoft ou plus de 600 millions pour Apple...). La désintermédiation est un des risques les plus importants du *Big Data*, en ce sens que d'ores et déjà, ces entreprises et autres plateformes du numérique proposent, comme Google à la suite d'une requête et de manière quasiment instantanée, leur propre « panneau de réponses ». Se mouvoir dans cet espace numérique requiert alors une capacité à gérer et maîtriser les données qui nous entourent.

La production des données a pour l'essentiel de notre histoire été le fruit de travaux complexes auxquels participaient de nombreux acteurs administratifs, culturels ou économiques. Le recueil des données à l'échelle d'une population entière nécessite des compétences multiples et souvent des moyens considérables. L'archivage des données constitue aussi un élément délicat et coûteux du processus de transmission des savoirs. Les plus grandes bibliothèques du monde peuvent au mieux conserver quelques millions d'ouvrages² et la pérennisation de ces lieux nécessite d'importants moyens humains et techniques. Les processus ainsi mis en œuvre induisent une rareté des lieux de savoirs et une obligation de ne conserver de manière durable que les savoirs jugés indispensables. Qu'il s'agisse des administrations, des entreprises ou des individus, pendant l'essentiel de l'histoire de nos sociétés, l'oubli était la règle et la mémoire était l'exception. Or, les technologies numériques ont transformé ce rapport à l'information en réduisant drastiquement les coûts de stockage et de traitement des informations. Cette conservation massive des données

- 1 **L'ensemble du projet d'avis a été adopté au scrutin public à l'unanimité des votants** (voir le résultat du scrutin en annexe).
- 2 La bibliothèque du Congrès des États-Unis considérée comme la plus importante au monde rassemble 23 millions d'ouvrages. L'équivalent numérique des ouvrages stockés dans cette bibliothèque pourrait aujourd'hui être stockée sur 20 terabits (soit l'équivalent de quelques disques durs de haute capacité). Source Library of Congress, 25 avril 2012 « *A "Library of Congress" Worth of Data : It's All In How You Define It* ». <http://blogs.loc.gov/digitalpreservation/2012/04/a-library-of-congress-worth-of-data-its-all-in-how-you-define-it/>

est devenue un vecteur de changement pour l'ensemble des organisations, mais elle induit aussi des changements dans nos modes de vie à mesure que les informations personnelles sont traitées et stockées. Face à l'essor du *Big data*, les révélations d'Edward Snowden sur les pratiques mises en place par la NSA ont permis à l'opinion publique mondiale de prendre conscience de la vulnérabilité des individus face aux dispositifs qui étaient mis en place sur Internet pour leur apporter des services nouveaux et qui pouvaient dans une logique inversée devenir un risque pour eux-mêmes et pour leurs libertés. Ces révélations sont ainsi apparues comme un nécessaire rappel à la lucidité pour les citoyens et les organisations dans la gestion des données personnelles et dans la protection des données sensibles des entreprises. Suivant les études du CREDOC³, avant même l'affaire Snowden, le premier sujet d'inquiétude des internautes reste le risque d'atteinte aux données personnelles. 86 % des mobinautes français souhaitent pouvoir interdire la transmission de leur géolocalisation à des entreprises commerciales.

La maîtrise des données numériques est désormais devenue un élément crucial de la participation à la vie sociale, culturelle et politique. Dans un premier temps, les usagers des technologies ont bénéficié de la décentralisation de la puissance de traitement en passant d'ordinateurs centraux connectés à des terminaux, puis à des micros ; nous assistons désormais à la recentralisation d'importantes masses de données via les technologies de l'informatique en « nuage » (*Cloud*) et bientôt la montée en puissance de services associés aux capteurs et aux objets. Avec ces changements de dispositifs technologiques, c'est la nature des données (en plus du volume des informations échangées) qui est amenée à évoluer. En effet, si pour l'essentiel, les données qui transitent sur internet sont aujourd'hui créées par les humains, dans un avenir proche ce sont les objets connectés, leurs capteurs et autres robots qui généreront la majorité du trafic sur les réseaux⁴. La capacité qui sera donnée aux citoyens de maîtriser ces nouveaux flux de données pourrait devenir l'une des caractéristiques les plus cruciales de l'architecture informationnelle de nos sociétés.

Dans le même temps, l'enjeu des données numériques est plus que jamais au cœur des questions économiques et des modèles qui les sous-tendent. Pour certains d'entre eux, il s'agit de valoriser les données des utilisateurs à des fins publicitaires, et pour d'autres d'analyser ces données afin d'établir de nouveaux services à valeur ajoutée. Ces services concernent des domaines aussi divers que la santé, la maîtrise de l'énergie, les transports, le tourisme ou la culture. À terme, de nouveaux services se mettront en place en lien avec de nouvelles générations d'objets connectés. L'intérêt pour les acteurs de l'économie numérique d'intervenir dans la fabrication des objets de grande consommation sera d'autant plus important que ces technologies permettront à leur tour de créer des services nouveaux dans la quasi-totalité des secteurs industriels.

3 http://www.arcep.fr/uploads/tx_gspublication/rapport-credoc-diffusion-tic-2012.pdf

4 « La croissance combinée du nombre d'utilisateurs d'Internet et des débits de connexion a conduit à une explosion du volume des données transitant sur les réseaux. En 2012, le trafic mensuel a été de 43 exaoctets par mois, c'est-à-dire 43 milliards de milliards d'octets (1018) ; c'est 20 000 fois plus qu'en 1996. Le taux de croissance du trafic est encore de 40 % par an, ce qui équivaut à un quasi-doublement tous les deux ans. La montée en puissance de "l'Internet des objets" pourrait en outre donner un essor accru à cette expansion, les données transmises par les objets connectés s'ajoutant à celles issues des activités des internautes humains. » Étude annuelle 2014 du Conseil d'État : « Le numérique et les droits fondamentaux » <http://www.ladocumentationfrancaise.fr/rapports-publics/144000541-etude-annuelle-2014-du-conseil-d-État-le-numerique-et-les-droits-fondamentaux>

L'économie mondiale des produits et services numériques représente déjà plus d'un sixième de l'économie des biens et produits traditionnels (estimées respectivement à 15 000 et 100 000 milliards d'euros)⁵. Cette part devrait bientôt rattraper celles des industries et services traditionnels et le cœur de métier de l'ensemble des entreprises industrielles pourrait ainsi évoluer vers des services informationnels.

Ces mutations des usages liés aux données numériques correspondent aussi à des changements importants dans les formes culturelles, sociales et politiques que prennent nos sociétés. Ces mutations de nos sociétés ne peuvent (et ne doivent) pas être induites « mécaniquement » par la capacité des technologies ou la volonté de quelques acteurs industriels. Les personnes doivent en effet participer non pas en tant qu'utilisateurs mais bien en tant que « co-architectes » de cette nouvelle société numérique. En plus de leur impact économique, les mesures qui permettront de rendre intelligibles et maîtrisables les données et les services de l'internet, revêtent un caractère politique et stratégique pour l'ensemble de nos sociétés. Autant dire que cette transition numérique pose la question des enjeux démocratiques dans une société où la relation entre la surveillance et l'Etat de droit est réinterrogée à la lumière des moyens mis en œuvre pour assurer un contrôle et une surveillance légitime de ces flux de données.

5 Source *Oxford Economics* et *Citybank*, 2011.
http://www.citibank.com/transactionservices/home/docs/the_new_digital_economy.pdf

Constats et enjeux

Enjeux et usages du *Big Data* : le traitement des données numériques au cœur des transformations économiques et sociales

Pas un jour, et ce depuis plusieurs années, sans qu'un quotidien, une émission radio, un ouvrage, une conférence ne relate une discussion, une analyse autour du *Big Data*. Si la traduction littérale française du *Big Data* (la « grosse donnée ») est moins séduisante, son pouvoir de transformation révèle une force d'attraction que l'on pourrait croire sans limite.

Mais d'où vient cette donnée ? De quoi parle-t-on quand d'aucun évoque le « nouvel or noir » de l'économie que nous manipulons chaque jour ?

Big Data : Origine et définition

Si l'expression « *Big Data* », que l'on peut traduire par « exploitation de très grands volumes de données », n'est apparue qu'en 2010, le concept est plus ancien et remonte à plus d'une dizaine d'années, lorsque les données sont devenues trop volumineuses pour être stockées et manipulées à l'aide des techniques classiques. Dans tous les cas, lorsqu'on évoque le *Big Data*, le cœur du sujet demeure celui de la donnée et de son traitement.

Caractéristiques de la donnée

La donnée n'est qu'un matériau brut de base. Pourtant sa collecte et son traitement peuvent conduire au savoir entendu comme une information établie au rang de « vérité provisoire scientifiquement acceptée » et à la connaissance entendue comme ce que chacun de nous construit à partir des interactions avec son environnement. Parler de « data » évoque alors une information numérique ou alphanumérique, codée, lisible par la seule machine, en vue de son enregistrement, traitement, conservation et communication. Les processus n'ont pas contemporain. La codification, la fixation et la transmission d'informations sont une série d'opérations anciennes, qui est à l'origine du développement de l'écriture, des échanges marchands, de la comptabilité, de l'imposition, de la monnaie, des transports, des sciences et, en conséquence, de la richesse des Nations. L'observation de la structure des révolutions scientifiques⁶ suggère qu'elles suivent souvent un même déroulement : la collecte de données met à mal la théorie scientifique dominante, qui entre en crise avant d'être remplacée par une nouvelle théorie, cadre qui est mieux à même d'expliquer les données problématiques. Le meilleur exemple reste l'œuvre de l'astronome danois Tycho Brahe⁷ qui, prônant un retour à l'observation, a collecté le premier une masse étendue de données qui

6 Thomas Khun, *La structure des révolutions scientifiques*, Ed. Flammarion, coll. Champs, 1962..

7 Tycho Brahe, né Tyge Ottesen Brahe (1546-1601), est un astronome danois. Il prend grand soin de la fabrication et de la mise au point de ses instruments qui lui permettent de recueillir un nombre considérable de données.

a permis d'établir une cartographie fiable du ciel et de formuler des prévisions correctes sur les mouvements des astres. Dans ce travail du XVI^e siècle, la problématique de la donnée est déjà présente : la collecte massive de données et le traitement de celles-ci permettent des prédictions fiables. En ce sens, même si la donnée est une notion ancienne, c'est au début de l'époque moderne que les sciences entament un mouvement de datafication dont l'œuvre de Brahe est un exemple.

□ *Datafication : une donnée codée, figée et transmissible*

La datafication est plus que la simple mesure ou transformation du réel en datas qui peuvent être recueillies et analysées. C'est la perception qu'il y a, dans les grands volumes de données, plus de valeur que dans les petits volumes de datas. Cela étant, même si Brahe et d'autres peuvent être présentés comme des exemples de ce mouvement, la datafication reste jusqu'au XX^e siècle quelque chose de rare. Le développement récent de l'informatique change cela, en permettant de simplifier, d'accélérer et de massifier la collecte et le traitement des données.

Une donnée est, par définition, une information codée, figée et transmissible. La donnée nécessite une codification, ce qui permet à la fois sa collecte et son rapprochement avec d'autres données formulées dans le même référentiel. Par exemple, une date de naissance possède un format, et peut être comparée à une autre date de naissance. La donnée est figée : la donnée doit être égale à elle-même, sinon sa collecte et son traitement deviennent impossibles. Deux dates de naissances distinctes ne peuvent être une donnée qui change : ce sont deux données. Enfin, la donnée est transmissible : cela signifie qu'elle peut être mémorisée, confiée à un système d'enregistrement, pour traitement immédiat ou ultérieur.

La donnée numérique est quant à elle la donnée dont la mémorisation a été confiée à un système informatique (et non à un papier, par exemple). Cette définition, en raison de sa simplicité, est d'une grande extension et permet de désigner des réalités très différentes : une donnée numérique peut être créée et non collectée – même si, le plus souvent, on entend désigner par « donnée numérique » des données qui ont été collectées.

□ *La donnée personnelle*

À cet égard, le terme français de « donnée » est trompeur : il sous-entend que cette information est donnée volontairement. Or, une part importante des données ne sont pas perçues par leurs propres utilisateurs comme des données. Par exemple, nos données de navigation sur Internet sont des données économiques précieuses, que nous ne percevons souvent pas comme telles. Enfin, certaines données qui nous paraissent anodines, peuvent si elles sont rapprochées fournir des informations personnelles, que nous ne désirons pas partager. Bien que ces informations ne soient pas des données numériques élémentaires, elles peuvent par différents procédés de traitement devenir des données à part entière. En ce sens, la donnée ne procède pas toujours du don : elle peut être absorbée et construite. Afin de ne pas entretenir de confusion sur le caractère volontaire ou involontaire de la donnée, on peut lui préférer le terme de « data ».

Il faut noter que la donnée personnelle est à la fois une information déclarative sur la personne et un ensemble d'informations non déclarées, mais recueillies automatiquement notamment lors de la navigation sur les sites web. Concrètement, quand un individu s'inscrit sur un site pour accéder à un produit ou un service, il donne son adresse électronique et, accessoirement, son nom, son prénom et parfois quelques autres informations. Elles contiennent ainsi l'ensemble des coordonnées, traces que nous laissons sur les sites,

moteurs de recherche, réseaux sociaux mais également dans le monde physique (musées, hôtels...). « Elles nous définissent et reflètent, parfois à notre insu, notre personnalité, nos goûts, nos aspirations, nos préoccupations, notre vie privée », pour reprendre les propos de Laure Kaltenbach du Forum d'Avignon.

L'exploitation des données personnelles⁸ n'est pas récente. En revanche, la capacité exponentielle d'outils de collecte, de stockage et la puissance des algorithmes de traitement ont pour caractéristique de circonscrire la vie privée, de prédire nos comportements et motivations – notamment d'achat.

La question du stockage et indirectement celle de la protection des données numériques concerne directement trois types d'acteurs : le citoyen, l'entreprise, l'État. Pour le citoyen se pose la question de l'hébergement de ses données personnelles hors du territoire, chez des acteurs qui ne relèvent pas forcément d'une juridiction nationale, dans des conditions de sécurité non garanties. Pour l'entreprise, cette question se pose également et est couplée à une sorte de dilemme : externaliser le stockage des données ou le gérer en interne avec les risques inhérents à cette activité. Enfin, pour l'État, s'ajoute aux enjeux précédents la question du besoin énergétique et celle du développement durable : les infrastructures de stockage des données nécessitent, entre autres, des équipements de distribution électrique.

Explosion, massification et stockage des données

Depuis les origines de l'humanité et jusqu'en 2003, l'humanité avait produit 5 exaoctets de données numériques, soit 5 milliards de milliards d'octets⁹. En 2010, il suffisait de 2 jours pour produire le même volume et depuis six ans, le poids de la data dans les communications électroniques augmente de 5 points par an¹⁰. Les sociétés Internet ont ainsi été submergées. Pour exemple, Google traite quotidiennement plus de 24 pétaoctets de données, ce qui correspond en volume à des milliers de fois la quantité de tous les documents imprimés de la Bibliothèque du Congrès américain.¹¹

Chaque minute, 350 000 tweets, 15 millions de SMS et 200 millions de courriels sont envoyés au niveau mondial. À l'horizon 2018, le trafic généré par les téléphones mobiles devrait être douze fois plus important que celui qui est constaté aujourd'hui. La société française *Criteo*¹² avance ainsi que 90% de la data qui est disponible aujourd'hui dans le monde a été créée depuis deux ans. En août 2012, Facebook fait savoir que, chaque jour, étaient enregistrés sur ses réseaux 70 000 requêtes, 300 millions de photographies et 2,5 milliards d'objets documentaires échangés. Si l'on tient compte de toutes les sources de données, il faut, en 2013, dix minutes pour produire 5 exaoctets d'informations. Il fallait deux jours en 2011 pour générer une volumétrie comparable, selon Eric Schmidt, l'ancien PDG de *Google*.¹³

8 « Nominatives » à l'exclusion des données « sensibles » que sont notamment les données relatives à l'état de santé, aux orientations sexuelles, aux origines ethnique et à l'appartenance politique, syndicale ou religieuse.

9 Stéphanou Lupieri, journalistes, Les Echos :

<http://archives.lesechos.fr/archives/2012/Enjeux/00294-036-ENJ.htm#>

10 *Op.cit.*

11 Viktor Mayer-Schonberger, Kenneth Cukier. *Big Data*. Editions Robert Laffont, Paris 2013, p.17.

12 Criteo est une entreprise française de recilage publicitaire personnalisé sur Internet, fondée à Paris en 2005. Elle est cotée au NASDAQ depuis 2013. Source Wikipédia 2014.

13 Google Inc. est une société fondée le 4 septembre 1998 dans le garage Google dans la Silicon Valley, en Californie, par Larry Page et Sergueï Brin, créateurs du moteur de recherche Google.

Les raisons de cette explosion de données tiennent à la montée en puissance des microprocesseurs et de la mémoire informatique, à la généralisation du haut débit, à la réduction des coûts de collecte, de stockage et de traitement des informations qui s'en est suivie, aux réseaux sociaux, au Web 2.0, aux smartphones, aux appareils photos numériques, à l'Internet des objets, aux nouvelles règles d'utilisation des moyens informatiques avec le *cloudcomputing*. Parallèlement, le coût de la mémoire numérique s'est effondré : le prix du mégaoctet¹⁴ était évalué en 1980 à 300 dollars. Il vaut aujourd'hui 0,00022 dollar.

□ Nouvelles sources de données : Open Data et objets connectés

Depuis l'émergence de la statistique publique, c'était l'acteur public qui se trouvait en charge et qui représentait l'expert des données. Il avait ses services et ses experts de données. Manipuler les données, c'est faire émerger du sens, et faire émerger des actions, cela avait un rapport très étroit avec le pouvoir. Or aujourd'hui les données numériques ne sont pas seulement produites dans le cadre d'un service public mais par toutes nos applications et nos machines intelligentes (ordinateur, tablette, smartphone, GPS, puces RFID -Radio Frequency Identification-, texte, photo, traces numériques laissées par un objet). La variété correspond donc à la multitude de sources qui produisent ces données. Cela change la source de production de la donnée, cela change également les sources potentielles d'analyse et d'exploitation de celles-ci et cela change enfin les capacités d'expertise. Car ces données ne sont pas structurées et sont donc difficilement stockables et analysables avec des outils informatiques traditionnels.

□ Les objets connectés

Pour l'heure, une grande partie des données transmises par les individus aux machines passent par des terminaux fixes ou mobiles dont les individus soupçonnent la propension à collecter des données, même si les usages ne mesurent pas le volume et la valeur des données qu'ils transmettent. Le développement d'interfaces naturelles, comme les objets connectés dont on estime le nombre d'ici à 2020 à 50 milliards, laisse penser que le volume, la variété et la vélocité de la collecte et du traitement vont encore augmenter, notamment pour bénéficier non plus seulement à l'activité professionnelle, mais aux activités personnelles des individus. Ce mouvement est déjà à l'œuvre dans le *life-hacking*, littéralement, « la prise de contrôle de l'existence », un mouvement qui encourage l'usage des applications, non pas pour se divertir du quotidien, mais, au contraire, pour enrichir et contrôler le quotidien. Les activités les plus touchées sont donc celles de tous les jours : la santé, l'alimentation, l'économie domestique, les déplacements, les transports, les loisirs, l'éducation, la culture. Ainsi, même si la révolution des objets connectés est distincte de celle du *Big Data*, ces deux innovations se soutiennent : les bénéfices apportés par le *Big Data* poussent à l'adoption des objets connectés, avec cette promesse que les grands nombres pourront nous aider à mieux vivre, plus longtemps.

□ L'Open Data ou la libération des données publiques

L'*Open Data* est un mouvement visant à généraliser la mise à disposition des internautes des informations détenues par le secteur public ; un mouvement qui considère que l'ouverture et le partage des données publiques est un bien commun. Il s'agit alors de

14 1 mégaoctet = 10⁶ octets. L'octet est l'unité de mesure qui est utilisée pour indiquer une quantité de données, quantifier la mémoire d'un disque dur ou la taille d'un fichier. Un octet est composé de 8 bits, le bit étant l'unité de base en informatique (un 0 ou un 1).

rendre ces données, qu'elles aient été créées par des États ou des entreprises qui opèrent des délégations de service public, accessibles à tous, facilement et gratuitement, afin de favoriser une meilleure information des citoyens et de susciter des innovations économiques sur la base de ces informations.

En France, ce mouvement s'amorce à la fin des années 70 avec le droit d'accès aux documents administratifs (loi du 17 juillet 1978, loi dite CADA), érigé en liberté publique par le Conseil d'État en 2002. Cette loi s'inscrit dans la suite de la loi relative à l'informatique, aux fichiers et aux libertés (dite loi Informatique et libertés du 6 janvier 1978) qui dispose que l'utilisation de l'informatique ne doit pas porter atteinte aux droits de l'homme et aux libertés individuelles et publiques et de la directive européenne de 2003 sur la réutilisation des informations du secteur public. En 2008 l'État définit, dans le plan « France numérique 2012 », une stratégie pour diffuser les données publiques et favoriser leur réutilisation. Cette stratégie est mise en œuvre par l'Agence du patrimoine immatériel de l'État (APIE) qui est, entre autres, chargée de rédiger les licences fixant les conditions de diffusion et d'utilisation des données publiques. La mission Etalab, créée en 2011 auprès du Secrétariat général du gouvernement (placée maintenant auprès du Secrétariat général pour la modernisation de l'action publique) succède à l'APIE pour mettre en œuvre concrètement l'ouverture et le partage des données publiques.

Récemment mises à disposition de tous - via le portail data.gouv.fr qui les héberge et qui est administré par Etalab - pour information et traitement, l'usage a fini par réserver ce terme d'*Open Data* aux seules données produites et rendues disponibles par la puissance publique, ce qui désigne, à terme, une partie limitée des données disponibles en ligne. Ces données diffusées uniquement après autorisation et anonymisation¹⁵ sont réutilisées dans un cadre précis qui peut être défini par une licence. Actuellement deux licences principales en France, la Licence Ouverte (inspiré de celui des *Creative Commons - CC -*) et l'*Open Database Licence*, encadrent cette source de données et permet la reproduction, la diffusion, la transformation et l'exploitation des données.

□ Le stockage des données : les *data centers* (DC)

En matière de numérique, le processus de dématérialisation renvoie couramment pour le sens commun à celui d'immatérialité. Le *cloud* en est le parfait exemple. Or, il est bon de rappeler que les données numériques sont physiquement stockées. Et les *data centers* sont ces lieux de stockage. En 2011, on en compte 2087 dans le monde.¹⁶

L'étude globale *Datacenter Dynamics 2012* indique que l'investissement dans les *data centers*, majoritairement situé dans les régions Asie-Pacifique¹⁷, a augmenté de 22 % dans le monde par rapport à 2011. Malgré les progrès technologiques en termes de compression et de virtualisation, il sera nécessaire de multiplier par 10 le nombre de serveurs physiques d'ici 10 ans.¹⁸ Le *data center* (DC)¹⁹ est un emplacement de quelques centaines à quelques dizaines de milliers de mètres carrés. Il comporte des serveurs pour le traitement des

15 Ces données susceptibles d'être rendues publiques par l'État ou les collectivités territoriales sont d'abord d'ordres démographique, territorial ou financier mais, selon chaque administration, elles peuvent être très différentes

16 Fabrice Coquio in <http://pro.01net.com/editorial/605472/>

17 <http://www.globalsecuritymag.fr>

18 Christophe Brasseur, *Enjeux et usages du Big Data, technologies, méthodes et mise en œuvre*, Lavoisier, Hermès Science, 2013.

19 Présentation détaillée dans *Data center et Développement Durable*, juin 2011, Syntec Numérique.

données, des équipements de stockage, de transmission et de communication permettant les échanges internes et externes, des systèmes de refroidissement, des équipements pour fournir l'électricité.

La consommation énergétique de la donnée

La consommation électrique des *data centers* a fortement augmenté du fait de la densification des sites, environ 1500W/m²²⁰ aujourd'hui; ainsi un *data center* de 10 000 m² peut avoir une consommation équivalente à celle d'une ville de 50 000 habitants ; ceux de Google aux USA²¹ représentent une puissance de 300 MW ; dans le monde on considère qu'il y a quelques dizaines de milliers de lieux de stockage pour une puissance électrique équivalente à la production de 30 centrales nucléaires ; ils représentent environ 2% de la consommation d'électricité mondiale, avec un taux de progression annuelle de plus de 10%²². Une étude de l'université de Stanford estime qu'entre 2005 et 2010, la consommation électrique de ces usines a représenté 1,5 % de la consommation mondiale des installations de refroidissement.

b) *Data center* et développement durable

Pour les opérateurs de *data center*, l'impératif est de garantir une disponibilité maximale à leurs clients, ce qui nécessite la redondance des équipements critiques. Il s'agit de tout ce qui assure un approvisionnement électrique suffisant et de qualité, ainsi que les systèmes de refroidissement du *data center*. Ce qui fait que les *data centers* sont suréquipés et que l'efficacité énergétique n'est pas souvent au rendez-vous. Selon le cabinet Mc Kinsey ²³, la plupart des serveurs utilisent en moyenne moins de 10% de l'énergie qu'ils consomment pour traiter les données, le reste est utilisé pour maintenir les systèmes prêts ou se dissipe en chaleur ! Même chose pour le stockage ou pour les autres équipements. Cela est aussi en lien avec les possibilités « sans limite » qui ont été données aux utilisateurs/consommateurs, à savoir d'avoir tout, tout de suite, n'importe où et indéfiniment !

Production et traitement des données : les caractéristiques du Big Data

Il serait erroné de croire que le phénomène *Big Data* ne se réfère qu'aux « nouvelles données », notamment celles issues des blogs, des réseaux sociaux. Une grande part de la croissance exponentielle constatée concerne les données traditionnellement traitées par les entreprises, qu'elles soient issues des secteurs bancaires, média, ou réseaux publics tels que l'énergie ou les transports. Pour exemple, pas moins de 165 millions de transactions bancaires sont réalisées quotidiennement dans la zone euro ; le nombre moyen de contacts clients d'une banque française a été multiplié par 10 en moins de dix ans, les 2/3 d'entre eux concernant le canal Internet et plus de 1/3 provenant des smartphones.

Mais pour Christophe Brasseur²⁴, si jusqu'à présent on avait tendance à ne stocker que les données a priori utiles et à oublier les autres, avec les nouvelles capacités de stockage et d'analyse, il n'est plus nécessaire d'échantillonner pour exploiter les données. Toutes les données peuvent être prises en considération.

20 *Idem.*

21 James Glanz, *New York Times*, 22/09/2012.

22 *How dirty is your data*, Greenpeace, 2011.

23 James Glanz, *op. cit.*

24 C. Brasseur, *op.cit.*

Le *Big Data* peut être défini comme l'ensemble des technologies, des infrastructures et des services qui permettent la transformation des données numériques en information, et la transformation de cette information en connaissance.²⁵ L'origine du *Big Data* se trouve de fait dans l'explosion même du volume de ces données numériques. Mais il est aussi et avant tout un moment de l'histoire de la collecte et du traitement des données qui est marqué par la possibilité conjointe de la collecte massive de données et de leur traitement rapide.

Des données numériques aux métadonnées²⁶

Les données numériques sont désormais « enchâssées » dans des architectures logicielles qui leur permettent de devenir intelligibles à l'ensemble des usagers de l'Internet. Ainsi, des données qui n'étaient accessibles qu'à un petit nombre de professionnels peuvent « prendre sens » auprès du grand public.

Ces architectures, ces « cathédrales logicielles », reposent aussi sur des données de description des données (ou métadonnées) qui sont essentielles au traitement des informations et peuvent parfois représenter une valeur économique plus importante encore que la donnée dont elles sont issues. Les métadonnées sont ainsi des informations structurées qui décrivent, expliquent, localisent ou encore facilitent la découverte, l'utilisation ou la gestion d'une ressource informationnelle (exemple des fichiers vidéos, musicaux, etc.). Dès lors, devient un enjeu capital la définition d'un ensemble de métadonnées communes à diverses communautés, suffisamment simple pour que des non-spécialistes puissent les créer à n'importe quel point du cycle de vie de la ressource, mais suffisamment structurées pour qu'elles puissent rendre les moteurs de recherche plus performants et donc faciliter la recherche et la récupération des ressources.

Ainsi, Kenneth Cukier²⁷ décrivait en ces termes l'importance du traitement des métadonnées pour l'ensemble des organisations : « *L'innovation et la création de valeur proviennent désormais de nouvelles formes de "re-structuration" des informations, liées au développement de "l'information sur les informations" ou "métadonnées". Celles-ci permettent aux organisations de réorganiser leurs réseaux plus facilement afin d'effectuer de nouvelles tâches, et cela signifie pour ces organisations accroître leur capacité d'apprendre en permanence et ainsi de s'adapter aux changements.* »

En d'autres termes, les métadonnées organisent et suivent l'ensemble du cycle de vie numérique des informations importantes, y compris les procédures, les processus et les utilisateurs à qui les tâches sont affectées. Elles offrent ainsi une traçabilité précise dans le cadre de la protection et l'organisation des données mais permettent également de générer à leur tour les données relatives aux goûts et préférences des utilisateurs qui deviennent la base de systèmes de recommandation en ligne. Là encore, des données issues du recueil des données individuellement introduites ou collectées auprès des utilisateurs peuvent générer des informations liées à des tendances générales dans une population.

25 Commissariat général à la stratégie et à la prospective, Internet : *prospective 2030*, note d'analyse n°2, juin 2013.

26 Ne dites plus « Big Data », mais « mégadonnées » (Le Point, 22/08/2014)
http://www.lepoint.fr/high-tech-Internet/ni-dites-plus-big-data-mais-megadonnees-22-08-2014-1855721_47.php

27 Report of the 2007 Rueschlikon Conference on Information Policy,
<http://www.cukier.com/writings/Rueschlikon2007-infogov-cukier.pdf>. Kenneth Cukier est aussi le co-auteur avec Viktor Mayer-Schonberger de *Big Data, la révolution des données est en marche* (Lafont, février 2014).

Le Big Data et la règle des 3V : volume, variété, vitesse

Le *Big Data* est avant tout le point de rencontre entre la multiplication des données non structurées, les besoins d'analyse de ces données et les progrès de la technologie. On le définit souvent à partir de 3 V (volume, variété, vélocité), auxquels Christophe Brasseur adjoint un quatrième pour « valeur » (ou « valorisation »).

Selon Wikipédia, le Big Data se caractérise de la façon suivante:

- les données n'y sont pas organisées sous forme de tables et leurs structures peuvent varier (textes, vidéos, photos, sons...); elles sont souvent non structurées;
- elles sont produites en temps réel;
- elles arrivent en flot continu et doivent pouvoir être intégrées quasiment instantanément;
- elles sont méta-taguées, mais de façon disparate (localisation, heure, date...);
- elles proviennent de sources très diversifiées (PC fixes ou portables, smartphones, tablettes, capteurs numériques, téléviseurs connectés, puces RFID, GPS, caméras, sites, blogs, réseaux sociaux, données publiques de l'*Open Data*...), de façon désordonnée et non prédictible.

Cette nécessité du volume a toutefois un revers. Elle peut inciter les agents collecteurs à vouloir acquérir beaucoup d'informations, notamment des informations personnelles. Il en va de même pour la variété des données collectées car le *Big Data* repose sur la mise en rapport entre données de natures différentes issues notamment de l'historique de navigation, des données personnelles déclarées, ou issues de procédés de géolocalisation. Comme dans le besoin de volume, il y a là un danger dans cette nécessité d'acquisition de données. Ce premier danger se double d'un deuxième écueil : il n'est pas aisé de savoir à l'avance quelles seront les données significatives.

Il serait cependant erroné de caractériser une situation de type *Big Data* à partir du seul critère de la volumétrie. Les outils et les volumes de données gérées ne sont pas identiques d'un secteur économique à l'autre. Il est vraisemblable que, sous l'effet de l'évolution technologique, les *Big Data* de 2020 n'auront pas la même définition qu'en 2013. On peut ainsi penser que, pour les années à venir, les *Big Data* devraient correspondre à des volumétries allant de plusieurs dizaines de téraoctets à plusieurs pétaoctets selon les secteurs. Dès lors, un cinquième élément, la véracité, s'impose comme une caractéristique majeure et stratégique pour le *Big Data*, tant il est vrai qu'une information erronée peut avoir des conséquences préjudiciables à tous points de vue.

Big Data et système décisionnel

Face à ce déluge de données, les entreprises sont conduites à développer sans cesse des technologies qui permettent de stocker et de traiter en temps réel toutes ces informations disponibles, structurées ou non, provenant de multiples sources²⁸. L'enjeu est alors de les croiser et de les enrichir très rapidement, « avec un seul but : mieux connaître et comprendre la réalité et anticiper les besoins futurs » en validant des intuitions. « On parle désormais de modèles prédictifs, dans lesquels des variables connues, dites explicatives, vont être utilisées pour déterminer des variables inconnues, dites à expliquer. »

28 Christophe Brasseur, *Enjeux et usages du Big Data, technologies, méthodes et mise en œuvre*, Lavoisier, Hermès Science, 2013.

Le Web sémantique, qui propose de poser des métadonnées sur l'ensemble des ressources du Web, est un allié de taille pour les *Big Data*, dès lors que les deux mouvements poursuivent le même objectif : faire parler les masses de données.

Le changement se manifeste dans une inversion des critères qui guident habituellement nos actions. Traditionnellement, nous agissons en nous appuyant sur la connaissance causale de phénomènes. Nous savons que la concomitance de deux phénomènes ne signifie pas leur liaison logique : leur concomitance peut être une coïncidence. Donc, nous cherchons à savoir pourquoi ou comment les choses arrivent. Le *Big Data*, en un sens, nous fait revenir à un stade antérieur : il est un retour à la concomitance. Le *Big Data* permet de relever des corrélations statistiques et donc de faire une prédiction probabiliste. Concrètement, avec le *Big Data*, on ne sait pas toujours pourquoi telle chose va se produire, mais on peut la prévoir avec une forte probabilité. Par exemple, on peut, en temps réel, et avec une géographie précise, savoir où se trouvent les personnes qui, dans un moteur de recherche, se renseignent sur les symptômes de la grippe. Et l'on peut établir, en quelques minutes, la cartographie de l'épidémie de grippe. Les données peuvent être comparées dans le temps, dans l'espace. Les séries statistiques peuvent être rapprochées. Le *Big Data* ne peut pas tout prédire, mais il est un outil nouveau, d'une puissance incomparable, qui change notre manière d'agir.

Ceci étant sans vouloir mettre un coup d'arrêt à ce qui relève d'une révolution technologique dont la portée et la puissance sont fonctions du nouvel entrant économique que représente la multitude, nous avons besoin d'une culture, d'une éducation qui fasse bien comprendre qu'une donnée n'est pas quelque chose de naturel, mais de construit. Les données sont construites, produites, et le processus de fabrication est aussi important que la donnée en elle-même.

La donnée numérique : valorisations sociales, économiques et environnementales

La donnée numérique est ainsi une ressource qui devient de plus en plus déterminante du point de vue économique, et le succès de Google démontre l'efficacité d'une valorisation systématique des données collectées. Au-delà des questions liées aux capacités de stockage et des types d'applications pour exploiter ce flux ininterrompu d'octets, les questions clefs pour les entreprises seront de savoir comment intégrer et valoriser leurs données pour en faire leur modèle économique.

La donnée numérique, nouvelle ressource économique

Si l'objectif de la production de cette masse de données extrêmement variées et non structurées est leur exploitation, l'analyse des données numériques, en vue de leur valorisation, est devenue un enjeu de compétitivité tout particulièrement pour les entreprises. Plus que les caractéristiques du *Big Data*, ce sont les possibilités d'analyse des informations que recouvrent les données numériques, qui deviennent dès à présent et plus encore à l'avenir l'enjeu stratégique de l'économie de la data.

Christophe Brasseur explique qu'en matière de marketing, « nous sommes en train de passer d'un modèle classique de segmentation à un modèle de caractérisation comportementale. [...] Le profiling des clients apporte sans aucun doute une valeur ajoutée à l'entreprise qui peut alors affiner et personnaliser ses produits et ses offres. » Ainsi, dans la publicité, le *Big Data*

permet d'offrir de nouveaux outils à disposition des PME et TPE, leur donnant la possibilité de développer leur activité d'une manière inédite.

□ *Données et valorisation capitalistique*

La donnée - et plus encore la donnée personnelle - est devenue en quinze ans le critère principal de valorisation des entreprises de la nouvelle économie. La valorisation capitalistique de certaines entreprises n'est d'ailleurs pas liée à leur chiffre d'affaire actuel, ou leur rentabilité, mais aux profits qui sont escomptés par leur croisement entre leur capacité à générer du trafic sur leur plateforme (traction) et leur capacité à recueillir des données personnelles.

Les premières informations données par les clients et les usagers des sites s'assimilent aux informations nécessaires pour constituer une base clients, qui est une première source de valeur pour une entreprise. C'est l'exemple d'Amazon pour la vente de livres en ligne qui, en 1997, employait une quarantaine de personnes pour faire de la recommandation personnalisée à ses acheteurs. Un jeune chercheur leur indique que le véritable actif de cette entreprise ne réside pas dans ces quarante « libraires », mais dans les données récoltées sur les clients de cette librairie. Il postule l'homogénéité des pratiques d'achats entre utilisateurs similaires et suggère de demander aux clients de noter, en aveugles, la qualité de la recommandation humaine et celle de la machine. Massivement, les clients plébiscitent les recommandations de la machine et l'entreprise finit par licencier ces quarante personnes.

Les premières expérimentations de *Big Data* en 2012 concernent entre 2 et 5 % des grandes et moyennes entreprises, entre 17 et 30 % des très grandes entreprises et plus de 90 % chez les 500 premières entreprises américaines²⁹. Pour information, le chiffre d'affaires du marché mondial du *Big Data* est estimé à 6,3 milliards de dollars en 2012 et devrait atteindre 8,9 milliards de dollars en 2014 et 24,6 milliards de dollars en 2016.³⁰ Quant à la croissance des revenus du marché, elle est estimée à plus de 40 % par an en moyenne, représentant 100 millions de dollars en 2009 et pourraient approcher les 50 milliards de dollars à l'horizon 2018.³¹

Ce sont ces données d'un second type qui permettent d'affiner le profil de l'individu. Cet affinement permet deux premières valorisations économiques.

D'une part aux yeux de la publicité, cela permet de cibler avec, en théorie, une grande précision, les individus : au lieu d'engager des moyens étendus pour toucher une cible limitée, les campagnes publicitaires peuvent être ajustées à leur cible réelle, ce qui peut à la fois rendre plus efficaces les grandes campagnes, et ouvrir l'accès au marché publicitaire à des TPE et des PME, qui peuvent désormais, avec des budgets moindres, atteindre leur public.

D'autre part, cette « datafication » des usagers semble exaucer un vieux rêve du marketing : la possibilité d'ajuster l'offre à la demande, en déterminant avec exactitude la taille de la cible. Cette évolution est à la fois au bénéfice des grandes entreprises, qui peuvent optimiser leur investissement, et au bénéfice des TPE et PME qui peuvent employer des outils ou ressources qui leur étaient interdites dans le passé. Deux des entreprises les

29 Source : Talend, Gartner Group et Deloitte.

30 Source : Transparency Market Research « Big Data Market – Global Scenario, Trends, Industry Analysis, Size, Share and Forecast 2012-2018 »

31 Source : Deloitte 2013

plus exemplaires de la nouvelle économie ont tiré leur croissance de leur capacité à mettre le *Big Data* au service de la publicité et du marketing : Google et Facebook.

Dans cette perspective, le *Big Data* est une étape nouvelle dans l'automatisation et la robotisation du monde. C'est une manière de confier à la machine ce qui était auparavant aux mains d'agents humains.

□ Le caractère « disruptif » de la révolution numérique

Lorsqu'on évoque Internet, on parle souvent - notamment pour le champ économique - d'une « technologie de rupture » (*disruptive technology*) selon le sens qu'en donne Clayton Christensen dans son ouvrage *The Innovator's Dilemma* publié en 1997 et dont le concept est aujourd'hui repris et développé par de nombreux acteurs du numérique comme Henri Verdier et Nicolas Colin, auteurs de *L'âge de la multitude*³². Pour ces deux auteurs, évoquer le caractère disruptif renvoie à la dimension innovante du numérique dont les effets sur le paysage économique peuvent être radicaux. Lorsque Joseph Schumpeter³³ parlait de « destruction créatrice », on peut ici parler de rupture avec certains modèles existants. La dématérialisation des données, l'accroissement vertigineux des capacités de stockage, tout comme l'augmentation de la vitesse de transmission instantanée, rompant avec l'unité de lieu et de temps, remettent en question les modèles classiques.

Tous les secteurs de l'action, qu'elle soit publique ou privée, peuvent être « datafiés » et, en ce sens, tirer des bénéfices du *Big Data*. Ces bénéfices peuvent prendre la forme d'innovations incrémentales, qui permettent d'affiner des outils, ou d'innovations radicales, que l'on nommera aussi « innovations disruptives », qui vont restructurer le secteur auquel elles s'appliquent. Et ces innovations peuvent être soit aux mains des acteurs qui interviennent dans ces secteurs, comme l'État ou des sociétés déjà existantes, ou aux mains de sociétés intermédiaires qui peuvent se spécialiser soit dans la collecte, soit dans le traitement des données. Concrètement, quel que soit le secteur concerné, le *Big Data* peut permettre un affinement de l'action, grâce à une détection et une prédiction plus justes. L'effet disruptif majeur du *Big Data* est la possibilité d'automatisation qu'il apporte, en transmettant à la machine des fonctions qui étaient auparavant confiées à des personnes. Pour les grands acteurs de l'informatique, comme par exemple Bill Gates, c'est le propre du progrès informatique : « automatiser ce qui peut l'être, de manière à ce que l'être humain puisse se concentrer sur ce qui lui est propre – et qui ne peut être automatisé ». Cette évolution est parfois décrite comme une évolution d'une société *people-based* (dont la majeure partie des opérations est traitée par des humains) à une société *software-based* (dont la majeure partie des opérations est traitée par des automates). D'un point de vue social, le *Big Data* allonge la liste des fonctions qui deviennent automatisables.

Opportunités du Big Data : de la santé à la maîtrise énergétique

Les opportunités les plus grandes du *Big Data* sont probablement à découvrir. Cela étant, cette nouvelle façon d'appréhender la donnée a déjà ouvert des perspectives, à la fois au secteur public et au secteur privé. En un sens, le *Big Data* est un grand révélateur

32 Henri Verdier, Nicolas Colin, *L'âge de la multitude, Entreprendre et gouverner après la révolution numérique*, Editions A. Colin, 2012.

33 Joseph Alois Schumpeter (1883 – 1950) est un économiste autrichien du milieu XXe siècle, connu pour ses théories sur les fluctuations économiques, la destruction créatrice et l'innovation.

de réel : l'action, qu'elle soit publique ou privée, ne repose plus sur l'expérience des agents, sur leurs intuitions, sur leurs croyances rationnelles, mais sur des faits statistiques. Il existe de nombreuses perspectives de réutilisations innovantes à partir des données publiques de santé. L'analyse de ces *Big Data* santé repose sur plusieurs bénéfices majeurs : une meilleure prise en charge du patient (passer d'une logique curative à préventive), assurer l'efficacité des dépenses publiques (doublement de la population senior d'ici 2030) et offrir de nouveaux terrains d'analyses et expérimentations à la communauté de recherche scientifique (épidémiologie, maladies chroniques, pharmacovigilance...).

De même dans le milieu sportif où les capteurs biométriques permettent d'évaluer les performances des joueurs en quantifiant les données liées aux distances parcourues, aux différentes phases d'accélération et de décélération, ou encore celles liées au rythme cardiaque afin notamment de pouvoir anticiper des risques de blessures et également de vérifier l'impact de la fatigue sur le jeu pour l'adapter en conséquence. Dans un autre domaine où l'affrontement n'est plus synonyme de compétition mais de conflit armé, le *Big Data* offre aux organisations civiles ou militaires l'opportunité de fonder leurs décisions sur une représentation fidèle de leur environnement tout en créant il est vrai une forme de dépendance essentielle à l'égard de ces systèmes d'information et de commandement. Il en résulte que les sources de vulnérabilité qui affectent ces systèmes – mauvais traitements, paramétrage des algorithmes, sécurité - crée un nouveau champ de conflictualité qui n'obéit pas nécessairement aux principes stratégiques établis dans d'autres espaces stratégiques, qu'ils soient conventionnels ou nucléaires.

Autant dire que rares sont les domaines qui échappent aux applications liées aux capacités d'analyses offertes par le *Big Data*. Toutefois les domaines de la santé et de l'énergie que nous avons délibérément retenus ici sont certainement les plus significatifs des transformations opérées par le *Big Data*.

Le domaine de la recherche en général et médicale en particulier

Grâce au numérique, la médecine progresse à pas de géant. Les techniques biomédicales permettent de vivre mieux et plus longtemps, et les problématiques de santé prennent aussi en compte des dimensions de confort, de bien-être et de longévité notamment par l'activité sportive.

Prévention, prédiction, participation, personnalisation : tels sont les enjeux de la médecine, qui tire parti des progrès de la science pour mieux comprendre la complexité du corps humain, prévenir les maladies mais aussi améliorer l'accompagnement des patients par une personnalisation des soins et un meilleur partage entre médecins, patients et médecins-patients. Avec le numérique et l'imagerie médicale, notamment, de nouveaux outils sont apparus qui permettent d'aller encore plus loin dans la compréhension du vivant, l'analyse des cas et les interventions ; on sait aujourd'hui modéliser des organes sur ordinateur, étudier des systèmes biologiques complexes, détecter des maladies, et même optimiser des gestes chirurgicaux avec la réalité augmentée et des robots spécialisés.

En même temps, le stockage et la puissance de calcul ont rendu le génome complet d'un être humain plus facile à analyser et à stocker et ce à un coût dérisoire. Le coût de

séquençage du génome humain approche les 100 dollars³⁴ et le temps pour l'analyser a chuté de 13 ans à moins de 3 jours. Les données de plusieurs millions de personnes peuvent ainsi être gérées et traitées dans des bases de données à plusieurs niveaux de stockage. Le véritable défi est alors de combiner ces ensembles de données dans différentes archives et de les croiser avec les dossiers de patients, les traitements et les résultats pour permettre de guérir de nombreuses maladies, dont le cancer.

De nombreux défis restent à relever mais, dans les pays développés, où l'espérance et la qualité de vie se sont nettement améliorées, la recherche de confort et de bien-être prend aussi de plus en plus d'importance. Là également, l'apport du numérique est stratégique, avec le développement de la santé à domicile ou le *quantified self*, par exemple, qui améliorent l'accès à des soins plus personnalisés³⁵.

Dans le secteur médical, la détection des pathologies et la prévention peuvent être réalisées avec plus de réussite par l'observation des corrélations statistiques entre facteurs en apparence sans lien, que par l'action concertée des médecins. Ainsi, une étude récente de *Microsoft Research* a permis de montrer à partir de données récupérées sur la base de 25 000 lits en hôpital comment, en matière de lutte contre les maladies nosocomiales, on pouvait à l'aide d'une cartographie gérer les emplacements différenciés des patients pour limiter les risques.

À cet égard, le *Big Data* ouvre la possibilité d'automatiser une partie du secteur médical - tout comme les recommandations de lectures fournies par l'automate d'Amazon sont considérées par les utilisateurs d'Amazon comme plus efficaces que des recommandations humaines. Deux acteurs majeurs Apple et Samsung viennent de créer des bases de données sur la santé. Aux États-Unis, plusieurs hôpitaux sont partenaires d'Apple pour accéder aux données des futurs patients. Il est toutefois prévu un accord préalable de l'utilisateur. Automne 2012, en encourageant l'ouverture et l'exploitation des données publiques, le gouvernement américain a permis à IBM de créer un logiciel de médecine prédictive : *Patient Care and Insights*. Le logiciel puise dans l'historique du système de santé en analysant et en recoupant des centaines de milliers de données - traitement, résultats, procédures, morphologies, géographies, climats, etc. - pour permettre aux médecins d'anticiper les futures pathologies de leurs patients en détectant certaines similitudes, et ainsi assurer une prise en charge préventive.

Si la recherche ne doit pas être entravée, sa conduite et les finalités doivent être particulièrement encadrées, notamment en ce qui concerne la donnée médicale et la sécurisation de celle-ci. Ces traitements massifs de données doivent concourir à renforcer de véritables politiques de santé et de prévention. La détention de ces données par des entreprises privées impose un encadrement rigoureux au-delà des règles éthiques et qui ne puisse souffrir d'aucune remise en cause pour des raisons de profitabilités financières. Car les risques ne sont pas loin de voir des dispositifs échapper à tout contrôle et porter par là même atteinte tant à la vie privée et au respect de la dignité humaine qu'à l'exigence d'un accès au soin pour tous. En France, Axa a annoncé que les assurés qui accepteraient de porter des capteurs pourraient se voir appliquer des tarifs dégressifs. Aux États-Unis, les assureurs n'hésitent pas à différencier les tarifs de leur complémentaire santé en fonction du profil de l'assuré avec un risque non négligeable de non-couverture pour les profils les

34 <http://investor.illumina.com/phoenix.zhtml?c=121127&p=irol-newsArticle&ID=1890696>

35 Source : INRIA, rapport 2012.

plus à risque. En outre, si le partage de l'information médicale est aujourd'hui reconnu par tous comme la garantie d'une meilleure prise en charge des malades, comme un moyen de remédier aux déséquilibres croissants de la démographie médicale et d'optimiser les dépenses de santé, tout en offrant au patient une meilleure maîtrise de ses données de santé, le déploiement de solutions de sécurité efficaces et de haut niveau est une condition impérative. Mais le développement du *cloud computing*, c'est-à-dire d'offres de service, consistant à héberger des données dans des serveurs dont on ignore où ils sont installés, et qui deviennent difficilement contrôlables, peut à défaut d'une réponse législative adaptée être une menace pour la protection de données personnelles.

Transition numérique et développement durable

Aucun domaine n'échappe au *Big Data*, pas même le domaine de l'agriculture, lui aussi concerné par cette évolution du numérique. Loin des seules approches productivistes, la collecte et le traitement de données autour de capteurs, de pulvérisateurs automatiques, de drones et de satellites, métamorphosent le travail de l'agriculteur.

Le numérique devient ainsi un outil au service de l'agriculteur pour assurer une meilleure irrigation, limitant les gaspillages, appliquant une juste dose d'engrais et en assurant une gestion écologique des eaux douces d'un territoire. Aux États-Unis, le projet de l'organisation américaine de protection de l'environnement The Nature Conservancy, s'est appuyé sur un système d'irrigation assistée par ordinateur, pour réduire la consommation en eau et récupérer l'eau des champs afin de moins puiser dans les rivières. En deux ans, c'est ainsi plus d'un milliard de litres d'eau qui a été économisé.

Lors d'une conférence à l'Unesco en mars 2012 intitulée « Le mariage du numérique et de l'énergétique : vers un Internet de l'énergie »,³⁶ Joël de Rosnay déclarait « *l'avenir de l'énergétique repose sur un mariage avec le numérique. Un partage de l'électricité en P2P devient possible, grâce à des smart grids, réseaux de distribution intelligents capables de s'adapter à l'offre de production d'énergies renouvelables et à la demande des entreprises et des consommateurs. Une voie nouvelle s'ouvre vers la démocratie énergétique et l'écomobilité* ».

Jeremy Rifkin³⁷ ne dit pas autre chose lorsqu'il présente les 5 piliers de ce qu'il appelle la troisième révolution industrielle :

- « *le passage aux énergies renouvelables ;*
- *la transformation du parc immobilier en ensemble de microcentrales énergétiques qui collectent sur site des énergies renouvelables ;*
- *le déploiement de la technique de l'hydrogène et d'autres techniques de stockage des énergies intermittentes ;*
- *la transformation des réseaux électriques actuels en réseaux électriques intelligents ou smart grids ;*
- *le passage des moyens de transport aux véhicules électriques » et il conclut : « Au XXI^e siècle, des centaines de millions d'êtres humains vont produire leur propre énergie verte dans leurs maisons, leurs bureaux et leurs usines et la partager entre eux sur des réseaux*

36 Le mariage du numérique et de l'énergétique : vers un Internet de l'énergie <http://www.scenarios2020.com/2012/05/le-mariage-du-num%C3%A9rique-et-de-l%C3%A9nerg%C3%A9tique-vers-un-Internet-de-l%C3%A9nergie.html>

37 *Smart grid*, Interview intégrale de Jeremy Rifkin, « Futuremag », ARTE <http://www.youtube.com/watch?v=OhWNUUKHahc>

intelligents d'électricité distribuée, exactement comme ils créent aujourd'hui leur propre information et la partagent sur Internet. »

Cette transformation numérique de la production et de la gestion de l'énergie au cœur des réseaux électriques de demain peut apparaître comme une douce lubie, voire un horizon lointain. Pourtant, l'arrivée des compteurs *Linky* est déjà une réalité pour de nombreux foyers qui ouvrent un compte auprès d'un fournisseur d'électricité. Et dans un avenir proche, chacun pourra s'abonner à l'énergie numérique qui lui est nécessaire et modifier son abonnement en fonction de l'évolution de ses besoins. Ces besoins, essentiellement de « consommation » aujourd'hui, évolueront progressivement, au fur et à mesure de l'équipement des foyers.

Un mouvement qui doit cependant s'accompagner d'une exigence en matière de protection des données et notamment de données personnelles. La capacité de ces compteurs *Linky* d'analyser finement la consommation électrique ouvre une voie d'accès au domicile privé et à l'ensemble des activités domestiques du foyer. La présence ou non de personnes au sein du domicile peut alors être constatée, des dispositifs en lien avec les distributeurs d'énergie peuvent aussi permettre dans certains cas de couper à distance tel ou tel appareil électrique. On peut alors aisément imaginer que sans une réglementation adaptée à cette évolution de la gestion numérique de l'énergie et aux attentes des citoyens dans leur accès à l'énergie, des offres commerciales permettent à des ménages aux revenus élevés de disposer d'un accès énergétique illimité, réservant aux ménages les plus modestes des forfaits limités ou « adaptés » à leurs besoins minimaux. La sobriété énergétique serait dès lors supportée par les seuls ménages les plus fragilisés.

De la ville intelligente (*smart city*) à la mobilité connectée

Autre exemple, la *smart city*. L'équipement d'une ville, comme Santander en Espagne, de plusieurs dizaines de milliers de capteurs permet de recueillir des informations de différentes sources (parking disponible, bruit, température) sur les comportements des usagers. Ces données sont transmises aux opérateurs publics et privés de la ville en Open Data pour optimiser les services. Leur analyse permet d'avoir une meilleure compréhension de la structure sociale d'une ville et de favoriser les initiatives publiques et privées. L'originalité de la *smart city* est donc d'impliquer autour d'un projet commun les acteurs sociaux, techniques, politiques et économiques de la ville.

Avec le développement des objets connectés, c'est la mobilité elle-même qui est revisitée. Il est alors possible de piloter au mieux ses déplacements chez soi et ailleurs. Trouver le meilleur mode de déplacement, devient dès lors possible avec une application consacrée au transport connecté qui gère la mobilité avant, pendant et après un trajet. L'application centralise toute une série d'informations sur le réseau de transports (voiture, bus, velib, taxi) et répond à des questions comme combien de places assises reste-t-il dans le bus, quelle station d'essence est la moins chère. Orienter, guider le piéton ou le conducteur à l'aide d'un GPS intégré dans la semelle comme chez *E-sole* ou dans la bague d'*Igoobook*, facilite les déplacements sans manipulation, ni *checking* à faire sur le smartphone. Le propriétaire est comme « pris en charge » par l'objet.

Quelle que soit la technique retenue, ces dispositifs peuvent également permettre de dresser une cartographie des relations familiales, professionnelles, amicales, des centres d'intérêts et types de comportement (sédentaire, mobile), en retraçant les déplacements des intéressés.

L'intégration croissante de dispositifs de traçage dans les usages du quotidien peut alors conduire à une modification importante des comportements et remettre en question le principe de la liberté d'aller et venir anonymement. L'atteinte aux droits et libertés induit par la géolocalisation varie toutefois en fonction de la catégorie de personne concernée (salariés, transports routiers, client d'une compagnie d'assurance, enfants, etc.) et du secteur impliqué.

La citoyenneté à l'ère du numérique, un nouveau pouvoir d'agir

Le numérique change incontestablement, pour ne pas dire radicalement, les relations entre individus en matière de citoyenneté. Cela interroge immanquablement notre vie en démocratie. Avec la production des données dont on ne sait pas toujours qui en sont les pourvoyeurs, l'expertise est beaucoup plus largement partagée. Dans le même temps, Google ou d'autres prennent des postures de domination avec la mainmise sur un nombre immense de données leur donnant un pouvoir d'analyse sur la société.

La captation de l'expertise collective constitue une difficulté démocratique majeure à laquelle nous sommes confrontés et que l'absence d'éducation au numérique ne fera qu'accroître. Parallèlement, la transformation numérique offre à l'acteur public les moyens de donner du pouvoir d'agir, de captation de l'expertise collective afin d'accompagner une « encapacitation », un *empowerment* des individus³⁸.

Culture, éducation et nouveaux accès aux savoirs à l'ère du numérique

L'histoire a permis le développement d'une multiplicité de lieux de savoirs. Les musées, les bibliothèques, les universités, les écoles sont les plus illustres des représentants de ces lieux de savoirs. Le développement du numérique au cours des 15 dernières années, qui ont vu l'émergence de la mise en réseau à l'échelle mondiale comme une norme possible d'échanger des informations, est en train de remettre en cause non seulement les lieux, mais aussi les modalités d'accès aux informations, aux savoirs, et aussi à la connaissance.

Internet est incontestablement un facteur de diffusion du savoir. Grâce aux milliers de bases de données connectées, les étudiants peuvent par exemple, consulter des millions de documents dans leur bibliothèque mais aussi celles d'autres universités, lire des revues dans une autre langue éditées dans un autre pays et les compléter par des conférences en ligne (type Ted). Citons également Gallica, la bibliothèque numérique de la Bibliothèque nationale de France qui propose à ce jour à la consultation en ligne plus de plus de 3 millions de documents dont 550 390 livres, 1 347 078 fascicules de presse et revues, 981 659 images, 44 358 manuscrits, 72 291 cartes, 24 015 partitions, et 3 513 documents sonores.³⁹

En bouleversant l'accès à l'information et les modes de communication, la révolution numérique a développé une culture de l'échange et de la liberté d'expression qui est en

38 Audition de Mme Amandine Brugière, Fondation Internet Nouvelle Génération (FING), devant la section de l'éducation, de la culture et de la communication du Conseil économique, social et environnemental le 1er juillet 2014.

39 Source : Wikipedia. Site Gallica accessible via <http://gallica.bnf.fr>

elle-même un acte de résistance dans beaucoup de pays. L'actualité récente a démontré la puissance des réseaux sociaux dans le domaine de la propagation des idées. Pour certains pays, l'accès au monde numérique démocratise indéniablement l'accès au savoir : les livres sont rares et chers, les bibliothèques désertes, les cinémas sinistrés, les télévisions navrantes. Avec Internet, il est alors possible de combler d'un clic le décalage culturel et entrer de plain-pied dans les modes, les musiques et les façons de penser d'une génération.

□ *Éducation au numérique et accès à la connaissance*

Si les technologies numériques démultiplient les accès à la connaissance, avec le risque non négligeable d'une uniformisation de ces derniers, décloisonnent certains espaces jusque-là réservés à une certaine élite, pour accéder en temps réel, partout dans le monde, à la connaissance (collections de musée, photos, presse, livres, films, etc.), il reste que cet accès instantané à la connaissance n'est pas synonyme de savoir. Car en plus de la nécessité de comprendre l'information qui s'ouvre à nous, nous devons garder à l'esprit qu'elle n'est pas proposée de façon aléatoire mais de façon conditionnée par les fonctionnalités des moteurs de recherche.

En proposant un ordre préférentiel de réponses, voire en en écartant certaines, les moteurs de recherche et autres plateformes numériques imposent leurs modèles de pensée ou dans le pire des cas modèlent notre pensée et nos perceptions du monde. Si l'accès instantané à la connaissance donne, en quelque sorte, un moyen d'agir pour le citoyen, encore faut-il que ce dernier soit capable de décrypter cette connaissance. De la donnée brute à la donnée traitée, il convient de déconstruire le processus ou le traitement qui œuvre à cette transformation. Aux côtés des acteurs de la société civile plus que jamais le rôle de l'école et celui des enseignants est capital pour assurer ce passage. Car c'est l'un des lieux essentiels pour acquérir les fondamentaux d'une vie en société et bâtir l'édifice de la citoyenneté.

□ *Numérique et pédagogie : de la classe inversée aux cours ouverts massifs en ligne (MOOCs)*

Qu'est-ce que l'éducation numérique ? Est-ce informer ou donner des compétences sur l'exploitation qui est faite des données qu'on produit ? Il faut sans doute aller beaucoup plus loin car le numérique change tout. Cela bouleverse la théorie mathématique. Le mathématicien Giuseppe Longo, spécialiste de Turing⁴⁰, montre ainsi comment le support numérique transforme les conditions mêmes du savoir mathématique. En astrophysique, le *Big Data* produit par les observatoires dans l'espace modifie totalement les conditions de la production d'une planétologie. Idem pour la biotechnologie ou même la langue. Le numérique avec Google transforme toutes les langues. Notre compréhension de tout cela est faible, essentiellement pour des raisons de vitesse.

Les cours ouverts en ligne (MOOCs) transforment les modes d'enseignement en s'adressant à un effectif d'apprenants beaucoup plus important qu'une classe d'étudiants et en leur permettant d'interagir entre eux et l'enseignant sur le contenu de cette connaissance (Cf. sur ce sujet l'avant-projet d'avis *La pédagogie numérique : un défi pour l'enseignement supérieur* préparé par Mme Danièle Dubrac et M. Azwaw Djebara).

40 Alan Mathison Turing, (23 juin 1912 - 7 juin 1954), est un mathématicien, cryptologue et informaticien britannique. Il est l'auteur, en 1936, d'un article de logique mathématique qui est devenu plus tard un texte fondateur de la science informatique. Il donnera en 1950 son nom au fameux test d'intelligence artificielle fondée sur la faculté d'imiter la conversation humaine.

La « classe inversée » - ou *flipped classroom* en anglais – est un modèle d'organisation scolaire qui tend à se populariser depuis quelques années. Le principe : les élèves regardent chez eux des vidéos de leurs cours enseignés par le professeur et consacrent leur temps en classe aux exercices et aux travaux de groupe encadrés par l'enseignant. Le rôle de l'enseignant change assez radicalement : il accompagne les élèves de manière plus personnalisée et devient un « pilote » dans une classe autonome. Il intervient donc pour donner des explications et s'adapter à chaque élève.

Si la classe inversée bouleverse les fondamentaux du système scolaire, les enseignants qui ont décidé d'adopter le modèle sont unanimes : les élèves sont beaucoup plus engagés dans les cours et leur apprentissage d'une manière plus générale. Sans doute y a-t-il là une opportunité qui doit être laissée à la discrétion de l'enseignant pour favoriser autour de projets pédagogiques une éducation à la collecte et au traitement des données numériques.

Toutefois, ce type d'organisation nécessite de disposer des outils et des supports d'enseignement adaptés. Outre les vidéos des enseignants que les élèves doivent regarder chez eux – à supposer qu'ils aient tous accès à un ordinateur –, la forme des exercices en classe change également : les élèves peuvent donc être amenés à choisir entre des exercices traditionnels, l'apprentissage sur des jeux vidéo ou encore des travaux de groupe. Cette innovation se présente comme une remise en question de méthodes pédagogiques fondées sur le retrait du transmissif et la promotion de l'activité de l'élève, le tout dans un contexte numérique sans lequel cette innovation ne serait pas possible. Nous devons y voir de plus près à partir des exemples pour savoir quels sont les enjeux et les limites d'une telle approche.

Le numérique à l'école : bref état des lieux

S'il est possible de remonter à 1970 pour trouver trace d'une première réflexion sur le numérique à l'école avec une circulaire de mai de cette année, et au plan « Informatique pour tous » en 1985 qui a permis de commencer à doter l'ensemble des écoles, collèges et lycées, il faut attendre 2011 pour que la plupart des écoles, y compris rurales, en soient dotées. Les dernières annonces d'un plan numérique par le président de la République devraient permettre de finir d'équiper toutes les écoles d'un accès à Internet.

Les compétences numériques font partie intégrante du socle commun de compétences et de connaissances actuel en attendant la refonte de ce socle.

Selon les programmes officiels, les élèves sont censés développer les consignes et connaissances suivantes :

- à l'école maternelle, les enfants découvrent les ordinateurs et comprennent leur usage et leur fonctionnement.
- à l'école élémentaire, les enfants apprennent l'écriture au clavier et l'utilisation d'un dictionnaire. Ils commencent à acquérir les compétences constitutives du brevet informatique et Internet (B2i) en utilisant les fonctions de base de l'ordinateur. Ils sont sensibilisés aux usages d'Internet et aux risques y afférent. L'usage raisonné de l'informatique, du multimédia et de l'internet est de règle. 5 domaines définissent le B2i : s'approprier un environnement informatique de travail ; adopter une attitude responsable ; créer, produire, traiter, exploiter les données ; s'informer, se documenter ; et enfin communiquer et échanger.

Les élèves devraient étudier le respect de l'intégrité des personnes et l'interdiction des atteintes à autrui y compris liés à l'usage d'Internet.

À la fin du CM2, l'élève serait capable de :

- utiliser l'outil informatique pour s'informer, se documenter, présenter un travail ;
- utiliser l'informatique pour communiquer ;
- faire preuve d'esprit critique face à l'information et son traitement.

Au collège, la maîtrise des outils informatiques serait mise en œuvre dans l'ensemble des disciplines. L'analyse critique serait essentielle avec le tri des informations et en matière d'utilisation des outils informatiques. Des principes de base sont censés être enseignés sur l'algorithmique élémentaire, la manipulation d'images, couleurs, textes et sons, la compréhension des principes et des bons usages d'Internet, des messageries...

Un rapport de 2013 sur *La standardisation de la filière numérique éducative : un enjeu pédagogique et industriel* rappelle que l'utilisation des outils numériques reste trop faible dans l'école primaire car elle remet en cause des pratiques pédagogiques ; de ce fait l'apprentissage au numérique reste très marqué par l'éducation aux outils. Dans le cadre de la formation tout au long de la vie, au niveau européen, il faut noter que la compétence numérique fait partie des compétences clés (recommandation du Parlement européen et du Conseil européen du 18/12/2006). Cette compétence met l'accent sur l'apprentissage de l'utilisation et de la critique des utilisateurs des Technologies de l'information et de la communication (TIC) comme sources d'échanges, de créativité, et d'innovation.

La loi d'orientation et de programmation pour la refondation de l'école de la république a instauré un service public du numérique avec la création d'une direction du numérique éducatif et la nomination d'un délégué académique du numérique dans chaque académie. Cela doit permettre de mettre à disposition des ressources numériques pour la réussite des élèves, de renouveler les programmes d'évaluation au numérique et de mettre en place une véritable formation des enseignants au numérique au sein des écoles supérieures du professorat et de l'éducation (ESPE).

Ces ESPE proposent quelques heures d'apprentissage du numérique centrées sur la pratique de supports. Mais l'essentiel de l'enseignement doit amener à l'obtention du C2i2e qui permet la maîtrise de l'environnement numérique professionnel (identification des ressources, utilisation des ressources de l'espace numérique de travail, organiser ses propres ressources) ; le développement de compétences pour la formation tout au long de la vie (utilisation de formation à distance, veille pédagogique à travers des réseaux d'échanges) et la responsabilité professionnelle dans le cadre du système éducatif (sécurité informatique, protection des libertés individuelles et publiques, protection des mineurs, confidentialité des données, propriété intellectuelle).

Il s'agit également d'acquérir les compétences nécessaires à l'utilisation du numérique dans la pratique d'enseignement (travail en réseau, préparation de contenus d'enseignement et de situation d'apprentissage, mise en œuvre pédagogique et démarches d'évaluation). Cette formation des maîtres reste souvent trop abstraite au regard de l'utilisation pédagogique des ressources numériques et de la transversalité des usages au sein des différentes disciplines et les heures d'enseignement spécifique sont insuffisantes (9 heures seulement).

Les recherches sur les usages pédagogiques des TIC sont aujourd'hui insuffisantes. La faiblesse de la formation continue ne permet pas de s'adapter à de nouveaux enjeux tels que l'utilisation du numérique.

L'avis du CESE sur *Les inégalités à l'école*⁴¹ rappelait le poids des disciplines dans la formation continue des enseignants.

▣ *Les tiers-lieux, nouveaux espaces de transmission des savoirs*

L'évolution, dans le monde entier, des lieux de savoirs, accompagnée par le très rapide développement des usages du numérique, met sur le devant de la scène le questionnement sur l'apprentissage et sur les modèles qui traditionnellement les portent : désormais dans un musée, on trouve des librairies, des dispositifs pédagogiques, dans une bibliothèque on trouve des expositions, des agoras, des spectacles de jazz, etc. Et dans les collèges les lycées, nombre de personnel éducatif dont notamment les professeurs documentalistes ont pris en charge cette ouverture. Mais dans les faits, la reconnaissance explicite de cette évolution est encore faible.

▣ *Les Espaces publics numériques (EPN)*

Parmi ces espaces novateurs d'accès aux nouvelles technologies numériques, on notera l'exemple des EPN issus en 1998 du programme Pacsi⁴².

Les EPN témoignent de cet engagement de la puissance publique en faveur d'une diffusion très large des accès et pratiques numériques. Initialement organisés et soutenus plus étroitement par le ministère de la Culture et par celui de la Jeunesse et des sports, les EPN se sont développés à partir de la fin des années 1990 de multiples façons : certains grâce à un programme national, impulsé par un ministère ou un organisme public, d'autres dans le cadre de programmes régionaux, départementaux, de villes ou de syndicats de communes qui s'associent parfois à d'autres programmes plus axés sur la formation professionnelle et l'autoformation. D'autres enfin sont issus d'initiatives associatives locales. L'ensemble forme une carte diversifiée de lieux d'accès, d'accompagnement et de formation aux services numériques, souvent regroupés en réseaux autour de centres de ressources.

Il arrive que les EPN soient intégrés à d'autres espaces ressources comme les médiathèques qui sont par ailleurs les plus grands espaces fournisseurs de ressources numériques. Or certaines d'entre elles ont limité l'ouverture de leurs ressources numériques aux strictes applications documentaires. On observe également la présence des EPN dans les centres sociaux. Dans certains cas le lieu d'accueil peut être mis à disposition par une école, ou encore par la mairie. Les formateurs sont mis à disposition par la ville ou par une association.

Plus de 4 500 lieux publics d'accès à Internet sont ouverts en France. En leur sein un ou plusieurs animateurs multimédia (appelés aussi médiateurs numériques) accompagnent, initient, aident chacun à maîtriser et bien utiliser ces outils et services offerts par Internet et plus largement par les Technologies de l'information et de la communication (TIC). Trois labels nationaux : les ECM (espaces culture multimédia) les cyber-bases (label de la Caisse des dépôts et de consignations en 2000), et les Points Cyb, sont venus compléter les nombreux labels des collectivités locales qui ont su avant l'État prendre des initiatives dans le cadre du développement de la culture numérique.

41 Conseil économique, social et environnemental, *Les inégalités à l'école*, avis présenté par M. Xavier Nau au nom de la section de l'éducation, de la culture et de la communication, septembre 2011.

42 Programme d'action gouvernementale pour la société de l'information fut annoncé par Lionel Jospin en août 1997, au cours des rencontres à Hourtin.

L'absence d'une véritable politique publique de mise en cohérence des actions multiples des EPN n'a pas toujours permis à ces espaces de saisir les opportunités de l'animation du numérique local. Dans ce domaine, très peu de projets de formation au numérique sont arrivés à maturité. Une difficulté due à l'absence d'initiatives pour faire émerger des projets innovants et pertinents. À cette difficulté s'ajoute un véritable souci de formation des personnels aux enjeux du numérique pour toutes les instances déconcentrées de l'État et tout particulièrement dans les DRAC.

En 2008, les financements publics consacrés au numérique que ce soit à travers le programme Pacsi ou ceux alloués par la Caisse des dépôts et consignation (CDC) en direction des EPN ont été supprimés. Bien que les structures soient demeurées, l'absence de fonds publics s'est avérée beaucoup plus préjudiciable pour le maintien des postes d'animateurs et des actions déployées par ces espaces. Les difficultés de financement des actions ont renforcé les difficultés de recrutement ou de maintien des postes initiaux. A cela s'ajoute un défaut de hiérarchisation des compétences et des niveaux de formation insuffisants.

Ces manques sont préjudiciables à la revitalisation des EPN dont les missions sont amenées à changer au regard de la vitesse à laquelle le numérique transforme les pans entiers de nos activités sociales et économique. Sans stratégie de changement il sera difficile d'accompagner la revitalisation des EPN comme nouveaux espaces d'innovation et de production d'information et de données numériques. Dans cette revitalisation, les associations ont sans aucun doute un rôle spécifique à jouer.

Un nouveau rapport aux œuvres

La culture numérique se réfère à la production d'une œuvre culturelle grâce aux technologies de l'information et de la communication. Elle renvoie à la maîtrise des outils alors que la culture à l'ère du numérique renvoie à l'impact des outils sur la manière de créer.

Un univers qui renvoie notamment à la numérisation des œuvres et aux relations entre le public et les artistes et qui désigne aussi la production et la diffusion de nouvelles formes d'expression culturelle. L'utilisation d'Internet et des appareils mobiles (smartphones, tablettes...) accélère de ce point de vue la métamorphose des pratiques culturelles, bouleverse le modèle économique des industries culturelles et les politiques publiques de soutien à la création. L'avis *Pour un renouveau des politiques publiques de la culture*⁴³ a décrit ce mouvement en proposant des pistes de réforme pour adapter nos normes traditionnelles à la culture numérique.

Plus généralement, la culture numérique renvoie au partage de l'information, à son décloisonnement et à la démarche collaborative des réseaux. Le développement, dans les années 1990, du Web 2.0 et des *wikis* est une illustration de la progression de cette culture : les *wikis* sont des sites Internet dont les pages sont modifiables par les internautes sous l'égide d'un modérateur (l'exemple du site *Wikipedia* en est le plus abouti). Les utilisateurs peuvent ainsi collaborer à l'écriture et modifier, de façon anonyme pour le public, les informations que le site contient. Lorsqu'ils sont anonymes, le site les identifie par leur adresse IP (*Internet Protocol*)⁴⁴. Les modifications jugées indésirables sont repérées et annulées par

43 Conseil économique, social et environnemental, *Pour un renouveau des politiques publiques de la culture*, avis présenté par M. Claude Michel au nom de la section de l'éducation, de la culture et de la communication, avril 2014.

44 Numéro d'identification qui est attribué de façon permanente ou provisoire à chaque appareil connecté à un réseau informatique.

des procédures sociales et techniques propres au site. La culture numérique de création collaborative à l'image des *wikis* met la multitude des regards et des échanges possibles au cœur même du projet. Le Web 3.0, permet à un logiciel d'analyser le comportement de l'internaute et d'en déduire ses besoins. Aujourd'hui, l'immersion du citoyen dans un environnement où le Web est très prégnant caractérise la culture numérique (Web 4.0 où l'homme peut travailler avec des outils uniquement en ligne).

La culture à l'ère du numérique, c'est donc un accès privilégié à la connaissance, grâce à la facilité d'accès pour le plus grand nombre aux moyens de communication nationaux et internationaux et aux bases de données qui y sont connectées. Internet et tous les outils numériques qu'il développe ouvre ainsi par le partage et la création collaborative les voies et moyens d'une expression de la liberté et de la confrontation des points de vue. La mise en place de centres de ressource dédiés à la mémoire et à la création, notamment audiovisuelle, deviennent alors une évidence et militent pour un « Droit à la mémoire », ils valorisent ainsi de nombreux territoires comme lieux d'une culture en devenir au profit du respect des différences comme source de richesse.

Nouveaux pouvoirs de création et d'échanges : des *FabLabs* à l'économie collaborative

Depuis quinze ans, il est apparu qu'Internet n'est pas seulement un moyen de diffusion, mais aussi un moyen de production, un lieu d'acquisition de compétences rédactionnelles collaboratives pour les contributeurs qui, dans l'exemple de *Wikipedia*, seraient cinquante mille en France⁴⁵. Sur ce mouvement de production virtuelle, qui reste un des plus grands moteurs de l'Internet actuel, s'est ajouté un mouvement de rematérialisation du virtuel, qui peut prendre toute sorte de forme.

L'étape suivante de cette évolution devrait correspondre à la capacité donnée aux usagers de participer à l'élaboration tangible de leur environnement, en particulier via les technologies d'impression 3D. Les données échangées sur le réseau participeront alors littéralement à la création physique de l'environnement des usagers.

□ *Des tiers-lieux aux FabLabs*

Cette rematérialisation prend principalement deux formes : la création de lieux où les usagers se réunissent pour un travail virtuel, et la création de lieux où une valeur créée en ligne est rematérialisée. Ces deux formes peuvent être combinées : l'utilisateur vient à la fois se rapprocher du virtuel, et rapprocher le virtuel du réel.

Les *FabLabs* sont souvent des lieux de production et d'innovation, au regard des lieux classiques et traditionnels de la production industrielle par exemple. En effet, si l'on regarde l'histoire des deux cents dernières années, on voit qu'ont succédé à des méthodes traditionnelles des techniques industrielles fondées sur le travail individuel. Cette phase industrielle laisse la place à une nouvelle phase : les moyens de production industrielle sont mis à la portée des individus et non plus seulement des entreprises. En encourageant une organisation sociale de plus en plus *software-based* ou automatisée, le numérique accélère cette mise à disposition des individus d'outils traditionnellement réservés aux entreprises et donne un pouvoir de production inédit aux particuliers. Mais une partie de ce pouvoir nouveau est un pouvoir qui est en fait retiré au monde du travail, et notamment aux PME et

45 Source : Wikipédia

TPE, qui peuvent se trouver parfois fragilisées par l'émergence d'un secteur de production informel qui ne s'embarrasse pas des contraintes habituelles du monde de l'entreprise.

Ainsi, Internet n'est donc pas seulement un lieu de diffusion, mais aussi un lieu de production.

□ *Le développement de l'économie collaborative*

L'économie collaborative concerne aussi bien l'échange de biens physiques, que la finance (*crowdfunding*, financement participatif), ou encore la production (*FabLabs*, *makerspaces*, lieux ouverts à tous où sont mis à disposition des machines pour fabriquer). Elle repose sur l'échange en pair-à-pair⁴⁶ via une plateforme.

Cette possibilité de produire propre à l'Internet est liée au phénomène dit de la « richesse des réseaux ». On trouve aussi des formes de collaborations qui ne sont pas massives et ouvertes, mais qui n'auraient pas pu se développer dans l'ère industrielle qui s'achève : par exemple, il existe des produits culturels qui sont issus de collaborations purement virtuelles entre artistes, qui seront rémunérés à la hauteur exacte de leur contribution. C'est ainsi que des agences de design ou de communication créent de nouvelles polices de caractères, ou des contenus rédactionnels. Enfin, il existe toute une économie collaborative qui n'est pas directement liée au secteur marchand et qui peut reposer sur des choses aussi diverses que l'échange de services, que ce soit entre particuliers ou entre entreprises, ou l'échange d'objets, ou la production de biens, services ou événements qui ne sont pas destinés au secteur marchand.

Accès aux données publiques : un nouveau regard citoyen

Les différents outils mis désormais à la disposition des citoyens ouvrent de nouvelles opportunités d'implication des citoyens dans les processus de décision des pouvoirs publics et des collectivités territoriales. Tout d'abord, le développement d'une société qui s'oriente davantage en fonction des faits statistiques (*data-driven*) peut avoir un effet positif sur la compréhension que les citoyens ont de ce qu'est l'État et de ce qu'il fait. Or, mettre à disposition des citoyens, que ce soit en ligne, dans des administrations, ou dans des tiers-lieux, des données publiques et d'outils, présente différentes limites. D'une part, l'appropriation de ces moyens est inégale, si bien que certains citoyens peuvent être exclus ou certains peuvent être plus ou moins écartés de ces processus. D'autre part, les administrations peuvent être rétives à partager des données, à confier des outils, et à accompagner ces expériences, qui peuvent être perçues comme inutiles, ou porteuses de dysfonctionnements ou de ralentissements.

□ *L'Open Data et transparence de la décision publique*

Du partage des résultats de recherche scientifique, *l'Open Data* renvoie aujourd'hui plus largement à la publication des données des administrations pour les rendre accessibles à la société. Ce mouvement dont nous avons vu précédemment qu'il se diffuse dès les années 70, participe de la construction de la transparence de la décision publique et favorise la participation citoyenne. Les Etats-Unis, le Canada, le Royaume-Uni et les Pays-Bas font notamment office de figures de proue de ce mouvement né en Europe de libération des informations du secteur public. Une littérature spécialisée se constitue d'ores et déjà

46 Pair-à-pair (*peer to peer*), c'est-à-dire échanger des fichiers sans passer par un serveur extérieur.

(réflexions philosophiques et perspectives espérées par les acteurs concernés, relayées par la presse) et les premières modifications des cadres juridiques afférents interviennent depuis le début des années 2000⁴⁷. En France, ce concept a été initié depuis 2010 par les collectivités locales, avant que le gouvernement ne rejoigne le mouvement⁴⁸. En effet, la mission Etalab a été créée en 2011 avec pour objectif la mise en place du portail gouvernemental data.gouv.fr⁴⁹, pour réunir les différentes données produites par les départements ministériels et autres institutions publiques, et désormais destinées à une mise à disposition gratuite sur Internet. Résultat de la mobilisation de la puissance publique, la France vient de se hisser de la 16^{ième} place en 2013 à la 3^{ième} place de l'*Open Data Index* pour l'année 2014.

De ce point de vue, l'*Open Data* est donc un mouvement distinct du *Big Data*. Leurs origines historiques et intellectuelles sont différentes. On considère généralement que la source de l'*Open Data* est à chercher dans l'article 15 de la Déclaration des droits de l'Homme et du citoyen de 1789 comme le rappelle Henri Verdier⁵⁰ qui stipule que la société a droit de demander compte à tout agent public de son administration. En un premier sens, l'*Open Data* est d'abord une aspiration démocratique à la transparence. En un second sens, ce mouvement s'est trouvé accéléré depuis une vingtaine d'années, sous le double effet du désir de participation des citoyens à l'administration et à la gestion quotidienne de leurs territoires, et de la possibilité de développer des projets collaboratifs en ligne. Enfin, en un dernier sens, l'*Open Data* peut se relier au *Big Data* car les données rendues publiques par l'*Open Data* peuvent nourrir des dispositifs *Big Data*.

L'*Open Data* permet aux services publics de publier des données publiques et à la société civile de les enrichir, modifier, interpréter, en vue de coproduire des informations d'intérêt général. L'histoire du mouvement multi-factoriel de l'*Open Data* montre qu'il est à la fois un signe de vitalité démocratique, un champ d'innovation économique et social et un outil pour affiner l'action publique.

A titre d'illustration, il est possible de récupérer des statistiques judiciaires sur une ou plusieurs fourchettes annuelles, les horaires de bus parcourant un territoire, la cartographie des forêts domaniales ou de toute autre zone protégée. Toutes ces données sont rendues accessibles, par accès direct depuis le portail *Open Data* ou par des liens pointant vers d'autres sites.

Les opérateurs privés comme publics ont déjà pris la mesure du potentiel économique lié aux exploitations innovantes des informations publiques, notamment sous l'impact de l'explosion du marché des applications pour smartphones. D'autres exemples comme les défricheurs que sont les réseaux citoyens ou les journalistes d'investigation permettent de mesurer la portée de la libération des données. Les développements de projets issus de l'*Open Data* séduisent par leur modernité, les capacités d'innovation qu'ils recèlent, et les promesses de croissance qui en découlent.

47 Par exemple : modification du *Freedom of Information Act* de 1996 pour les Etats-Unis, révision en cours de la directive européenne 2003/98/CE « Public Sector Information » dite PSI.

48 La mission interministerielle « Etalab » a été créée par décret n°2001-194 du 21 février 2011 du Premier ministre, François Fillon. Cette mission désormais présidée par Henri Verdier, est actuellement intégrée au Secrétariat général à la modernisation de l'action publique (SGMAP).

49 Le portail « data.gouv.fr », a été créé par circulaire en date du 26 mai 2011 et a été mis en ligne le 4 décembre 2011.

50 Audition de M. Henri Verdier, Directeur d'EtaLab, devant la section de l'éducation, de la culture et de la communication du Conseil économique social et environnemental, le 28 mai 2014.

Connaître la qualité de l'eau dans sa ville, découvrir les sites d'écotourisme dans sa région, consulter la réglementation en vigueur sur l'énergie solaire. Autant d'informations vertes disponibles sur le portail toutsurlenvironnement.fr. Créé dans le sillage du Grenelle de l'environnement, en juillet 2009, ce site du ministère de l'Écologie rassemble près de 44 000 ressources sur l'environnement, mises à disposition par environ 170 administrations. On y trouve aussi bien des cartes que des rapports, des bases de données ou encore des documents multimédias. « *L'objectif est de rendre l'information publique environnementale accessible au plus grand nombre de citoyens, comme l'impose la convention d'Aarhus, ratifiée par la France en 2002* », explique Éric Bonmati, responsable du portail. Le site, qui est passé de 20 000 à 36 000 visites par mois, mène en outre depuis octobre une campagne pour inciter les collectivités à collaborer en ouvrant leurs bases de données. Une initiative qui s'inscrit dans la tendance à l'ouverture des données publiques, l'*Open Data*, lancée par l'État avec data.gouv.fr.

Malgré les progrès accomplis par l'administration en termes de transparence, la mission commune d'information du Sénat sur l'accès aux documents administratifs constate « l'inertie persistante » des administrations sur l'ouverture des données publiques et la qualité inégale des informations publiées⁵¹. Les pratiques actuelles des principaux acteurs de l'*Open Data* ne permettent néanmoins pas de satisfaire pleinement les objectifs initiaux de ce mouvement de libération des données publiques. En effet, la multiplicité actuelle des portails *Open Data* ne facilite pas l'accès direct à l'information par les citoyens. Compte tenu du format brut des données mises à dispositions, l'intervention d'un intermédiaire semble en outre inévitable. Cette médiation, source d'activités économiques, tempère dès lors l'objectif de transparence « directe » à l'égard des administrés.

De même, la diversité des formats⁵² utilisés pour mettre à disposition les données et la nécessité induite par certains d'utiliser des logiciels spécifiques, voire payants, complexifient l'accessibilité aux données et tendent à faire perdre le caractère gratuit de cet accès. Enfin, la qualité des données mises à disposition peut-être altérée par l'absence d'explication sur les méthodes de production de la donnée (par exemple, en matière de statistiques, sur les sources utilisées, etc.). Ces déficits dans la cohérence des débuts de l'*Open Data* s'érigent en obstacles à l'accessibilité des informations du secteur public.

Par ailleurs, il convient d'intégrer dans la réflexion portée sur l'*Open Data*, l'accès aux données des entreprises mises à disposition des représentants des salariés dans le cadre des « bases de données uniques ». Si ces données ne sont pas à considérer comme « ouvertes », elles contribuent cependant à donner aux représentants des salariés, des éléments d'analyses pour mieux connaître la situation de l'entreprise, et ainsi conforter le dialogue social, ainsi que la démocratie sociale.

51 Rapport au nom de la mission commune d'information sur l'accès aux documents administratifs et aux données publiques présidé par M. Jean-Jacques Hysté, sénateur, présenté par Mme Corinne Bouchoux, sénatrice, juin 2014.

52 Sur le site data.gouv.fr, 15 formats de données différents sont utilisés pour diffuser en *Open Data*. Parmi ces formats, la plupart nécessitent l'utilisation d'un logiciel pour consulter les données. La plupart des formats sont difficilement compréhensibles en l'état. C'est le cas notamment du format [XML].

La création d'un administrateur général des données (équivalent du *chief data officer* anglo-saxon) laisse espérer la définition d'une politique nationale de la donnée au-delà de la seule dimension de l'*Open Data*.

Cependant il convient de rester prudent : le croisement des fichiers d'*Open Data* peut permettre d'accéder à des données individuelles qui menaceraient la vie privée des citoyens. Une transparence absolue ne peut être atteinte et n'est pas forcément toujours souhaitable ; notamment de la part des Etats, à condition que ce soit pour des raisons légitimes de protection des libertés individuelles (par exemple : secret défense, secret de l'instruction...). Dès lors le dogme politique de l'*Open Data* avec l'ouverture des données risque fort bien de déplacer la médiation et l'expertise vers les détenteurs d'un capital technologique.

Si l'ouverture des données doit être encouragée, elle doit s'accompagner dans le même temps de toutes les garanties de respect de l'anonymat. Doivent également être exclues de ce mouvement d'*Open Data* les données relevant du secret industriel et commercial et de la sécurité publique.-

□ *La révolution numérique et l'administration électronique*

La France a été désignée, par l'ONU, première en Europe et quatrième dans le monde pour l'administration numérique. La transformation numérique permet aux Français de simplifier leurs démarches administratives. À titre d'exemple, 53% des Français paient leur impôt sur Internet. 86% des agriculteurs effectuent des demandes d'aide au titre de la politique agricole commune. Le site *Legifrance* a reçu 100 millions de visites et service-public.fr plus de 200 millions en 2013⁵³.

Les technologies numériques permettent aux citoyens de faciliter leurs démarches quotidiennes. Les relations administration-citoyens sont de plus en plus dématérialisées grâce aux sites Internet ou aux applications mobiles des administrations. Un des enjeux du développement de l'administration numérique est de rendre ces services ergonomiques pour être utilisables par tous. En effet, une étude de l'Agence nationale des solidarités actives (ANSA) montre que l'ergonomie de ces services participe à la réduction de la fracture numérique qui concerne particulièrement les jeunes en difficulté, les personnes en recherche d'emploi et les seniors⁵⁴.

Mais le défi de la transformation numérique de l'État réside aussi en la capacité des pouvoirs publics à permettre à tous de pouvoir être connecté, ce qui n'est pas le cas actuellement au vu du coût d'un abonnement ou d'une connexion ponctuelle. L'ANSA recommande ainsi de développer le *WiFi*⁵⁵ public dans les lieux fréquentés par ces populations : foyers de jeunes travailleurs, missions locales, centres d'hébergement, centres sociaux...

53 Compte-rendu du Conseil des ministres du mercredi 17 septembre 2014.

54 Agence nationale des solidarités actives, *L'accès aux télécommunications pour tous, la parole aux personnes en situation de précarité*, avril 2012.

55 Le *WiFi* est un ensemble de règles de communication permettant de relier sans fil plusieurs appareils informatiques.

Les nouveaux enjeux sociaux et culturels de la fracture numérique

Alors que l'illettrisme a été déclarée Grande Cause nationale 2013⁵⁶, son avatar numérique l'illectronisme toucherait 15% de la population. L'illectronisme est « *une difficulté qui peut se traduire autant par la manipulation de ces nouveaux outils - computer illiteracy - que par une incapacité à accéder aux contenus de l'information numérique et à les comprendre - information illiteracy* ». ⁵⁷ Un obstacle technique et intellectuel, en somme.

Les recherches menées sur le sujet démontrent une corrélation entre la variété de l'usage du numérique et le niveau d'éducation ; et le fait de se trouver en marge des circuits sociaux, éducatifs, et professionnels est un facteur d'exclusion numérique considérable. En 2013, selon le CREDOC, 82% des français de plus de 10 ans étaient internautes au moins occasionnellement. 81% des foyers sont équipés à domicile. En ce qui concerne l'internet mobile le CREDOC décompte 39 % d'utilitaires. Les inégalités d'accès sont fondées sur l'âge (au-delà de 65 ans), le niveau de diplôme, et l'existence d'enfants d'âge scolaire au sein des foyers qui induit un plus fort équipement.

Le CREDOC identifiait 4 populations dont le taux d'accès à internet restait inférieur ou égal à 60 % : les plus de 70 ans, les retraités, les membres des ménages dont le revenu était inférieur à 900 euros par mois et les non diplômés,

Parmi les internautes, 91 % des 18-24 ans et 87 % des diplômés du supérieur utilisent internet tous les jours, contre la moitié des plus de 70 ans et des non diplômés. Les trois quart des moins de 24 ans et les deux tiers des diplômés du supérieur utilisent internet hors de chez eux contre 6 % des plus de 70 ans et 13 % des non diplômés.

En matière d'utilisation d'internet, les réseaux sociaux sont fréquentés majoritairement parmi les 12-39 ans et très minoritairement par les plus de 60 ans ; les services administratifs, de même que les achats sur internet sont utilisés par les diplômés (83 %) et les jeunes de 25 à 39 ans (78 %). Internet est un média pour les jeunes diplômés alors que le reste de la population continue à écouter la radio et à regarder la télévision. Enfin, la pratique du numérique est corrélée avec la taille de population du lieu de résidence et l'utilisation est maximale dans les très grandes agglomérations de plus de 100 000 habitants.

On rappellera que les avis du CESE *Pour une politique de développement du spectacle vivant : l'éducation artistique et culturelle tout au long de la vie* et *Pour un renouveau des politiques publiques de la culture* ont démontré que l'usage intensif d'internet est fortement corrélé avec l'intensité des pratiques culturelles. On n'omettra pas d'ajouter les zones géographiques qui restent non couvertes par internet notamment les zones rurales et de montagne. Le gouvernement s'est engagé dans un plan numérique permettant la connexion à terme de la totalité de la population.

S'il existe « *un lien entre public en difficulté avec les acquis simples, les savoirs de base et l'illectronisme* » - Internet est constitué de 90 % d'écrit -, comme le relève Frédéric Rampion, chargé de projet au sein de l'association rouennaise « Éducation & Formation », qui vise à former les publics peu ou pas qualifiés à l'acquisition des compétences clés, les individus en

56 Selon une étude de l'Insee parue en décembre dernier, la France compte 2,5 millions de personnes illettrées. 7% des adultes de 18 à 65 ans ayant été scolarisés en France, mais ayant perdu les acquis de base, souffrent de ce handicap.

57 Elisabeth Noël, Ecole nationale supérieure des sciences de l'information et des bibliothèques

situation de précarité sociale ou économique, les seniors, les non-diplômés ou encore les grands ruraux font aussi partie des populations touchées.

Toujours selon une étude du CREDOC sur « la diffusion des technologies de l'information et de la communication dans la société française », 42 % des Français non connectés invoquent comme frein principal le coût de l'abonnement et de l'ordinateur, ainsi que la complexité de l'outil. *« Il s'agit d'une machine qui change de configuration en permanence. Contrairement à un toaster ou un fer à repasser, où un bouton est égal à une fonction, sur Internet un bouton correspond à une multitude de fonctions »*, détaille ainsi Bernard Benhamou.

Le numérique est souvent présenté et perçu comme la solution à toutes les difficultés, en somme une baguette magique. Le numérique ne peut pas gommer à lui seul la barrière de l'accès au savoir qu'est le milieu social ? L'accès aux savoirs et plus encore aux savoirs numérique et par le numérique nécessite un effort de médiation et de partage sur l'ensemble du territoire. Ce qui pour notre assemblée oblige de construire autour de ces nouveaux outils de recherche et d'exploration des projets dont l'ambition doit demeurer la mise en relation citoyenne et l'émancipation des personnes.

À mesure que ces technologies sont devenues accessibles à un plus grand nombre de foyers⁵⁸, le besoin d'accompagnement, loin de s'éteindre, s'est au contraire amplifié tout en se diversifiant. La pensée qui prévalait alors était qu'à mesure que les foyers français seraient équipés en micro-ordinateurs connectés, les citoyens se formeraient progressivement et les besoins d'accompagnement diminueraient « mécaniquement ». Force est de constater que cette prévision s'est révélée fautive et cela pour plusieurs raisons parmi lesquelles on pourra citer :

- l'explosion en volume des services mis à disposition des citoyens sur Internet ainsi que leur importance croissante dans l'ensemble des démarches sociales, culturelles et professionnelles a nécessité un accompagnement pour permettre aux citoyens d'effectuer en ligne certaines démarches qui pour les plus importantes d'entre elles (comme la recherche d'emploi) nécessitent la maîtrise des usages de l'Internet.
- dans le même temps, la « numérisation » de l'ensemble des métiers et des filières a rendu plus indispensable la maîtrise de ces technologies au-delà des seuls métiers liés à l'informatique. Les risques sociaux liés à l'absence de maîtrise des technologies et des usages de l'Internet sont devenus d'autant plus importants que ces compétences ne sont pas toujours quantifiables.
- la montée en puissance des réseaux sociaux a pu donner en particulier aux plus jeunes utilisateurs une fautive sensation de maîtrise de ces technologies qui devenaient pour beaucoup un substitut à la consultation des médias audiovisuels traditionnels sans qu'elle s'accompagne nécessairement de bénéfices sociaux ou professionnels.
- l'essor des terminaux mobiles qui permettent de simplifier l'accès aux ressources de l'Internet (en particulier pour les primo ou néo-utilisateurs) pose aussi des questions nouvelles sur la maîtrise des démarches administratives ou sociales

58 La France se situe au 8^e rang européen, avec 82 % des ménages connectés à l'Internet à domicile en 2013, contre 74 % en 2010 et 62 % en 2008. Elle est précédée notamment par l'Allemagne et le Royaume-Uni (88 % pour chacun) (Observatoire du Numérique – DGCS)
<http://www.observatoire-du-numerique.fr/u+6sages-2/grand-public/equipement>

en particulier lorsque le terminal mobile constitue, comme c'est le cas pour de nombreux foyers défavorisés, l'unique moyen de connexion à l'Internet.

- la complexité et le manque d'ergonomie des premiers outils, notamment les micro-ordinateurs ont rebuté les utilisateurs néophytes.

La fracture numérique n'est alors plus seulement une affaire entre ceux qui ont accès à l'informatique et ceux qui ne l'ont pas. Le matériel informatique est aujourd'hui devenu un produit de consommation de masse, même dans les pays pauvres. La nouvelle fracture se fait et se fera plus encore à l'avenir entre ceux qui sauront trier l'information, la vérifier, l'organiser, bref l'utiliser pour en faire un véritable outil de savoir, et ceux qui faute d'une éducation au numérique n'auront pas les moyens de le faire. Comme le rappelle le CESE, c'est l'ambition du socle commun.

L'appropriation des techniques d'utilisation du numérique et du mode d'usage d'Internet est aujourd'hui une dimension tout aussi discriminante au regard des répercussions dans le monde du travail, le développement professionnel, la consommation, la communication et l'exercice de la démocratie.

L'utilisation des logiciels, la compréhension de l'information pour s'en servir, la compréhension de la structure d'un fichier ou du fonctionnement d'un site Web nécessitent des connaissances et des compétences. Tout cela, le CESE le rappelle dans ses avis récents sur l'éducation, renvoie notamment à la maîtrise du socle commun de connaissances, de compétences et de culture.

L'enjeu de la « souveraineté numérique »

Pour être utilisables par le plus grand nombre, les vastes ressources numériques accessibles sur Internet nécessitent que soient mis en place des services de différentes natures ; des moteurs de recherche, des réseaux sociaux, des services de géolocalisation, des plateformes d'échanges d'images ou de vidéos. Ces plateformes qui centralisent et organisent l'information représentent des intermédiaires « obligés » pour la quasi-totalité des utilisateurs de l'Internet. À ce titre, ces plateformes disposent d'un pouvoir d'influence considérable sur les citoyens. Face à la montée en puissance des grandes plateformes qui agrègent et organisent l'information sous ses différentes formes, des questions nouvelles sont désormais posées quant à la capacité des citoyens à en tirer parti et aussi d'en bénéficier de manière transparente.

Ces plateformes sont en particulier la face visible par les citoyens des technologies de *Big Data*. Par leur importance dans la vie quotidienne de l'immense majorité des usagers de l'Internet, ces plateformes ont à la fois un pouvoir économique sur l'ensemble des secteurs d'activité mais elles représentent aussi un vecteur d'influence politique dans le cadre de la formation des opinions publiques. En effet, le cadre d'utilisation des données issues de ces plateformes devrait aussi s'élargir à mesure qu'elles accompagneront les démarches de santé, les dispositifs de maîtrise de l'énergie ainsi que la culture ou les transports. Même si la maîtrise des technologies en ce domaine correspond à des métiers à part entière, il est chaque jour plus important que les citoyens et les entreprises aient une forme de maîtrise des technologies qui sous-tendent ces plateformes, pour permettre tant leur contrôle que la transparence en ce domaine.

Face à la domination des acteurs économiques américains et à la captation de la valeur produite en France qui en découle (faute de réponses économiques et fiscales adaptées), la question de l'indépendance économique et politique est posée. Sans offre de notre part, c'est à la fois des pans entiers de nos industries qui en souffriront et une approche de la gestion des données à l'opposé de nos exigences éthiques qui l'emportera, avec les risques que nous connaissons en matière de protection de la vie privée et des données sensibles à caractère personnel ou pas.

Il faut réaffirmer l'exigence d'une réponse politique, à même d'accompagner les transformations en cours en adaptant à la fois nos comportements, et en encourageant l'innovation et l'audace. Sous-estimer les enjeux du numérique, c'est prendre le risque de perdre une vision globale des atouts de notre pays et une capacité de redéployer les efforts indispensables.

La valeur économique captée par les GAFA (Google, Apple, Facebook, Amazon)

Cette valeur économique présente actuellement trois difficultés. Tout d'abord, elle est très inéquitable, au sens où la richesse apportée par les particuliers n'étant pas rémunérée, elle n'est pas valorisée à sa juste valeur et permet une grande marge aux sociétés qui savent, notamment dans le cadre du *Big Data*, exploiter ces données. Cet écart entre valeur réelle et valeur perçue explique que ces sociétés attirent massivement de l'investissement car leur modèle économique permet, en théorie, un « passage grande échelle », renforçant la capacité d'adaptation et de croissance des performances, ce que les investisseurs en capital nomment parfois une « scalabilité ». Concrètement, si une application ou un service sont bien conçus et génèrent une forte attraction, les coûts fixes de leur fonctionnement, bien qu'augmentant avec l'usage, augmentent beaucoup plus faiblement que leurs résultats, permettant une très forte marge d'exploitation. Sans cette forte marge d'exploitation, ces entreprises, et notamment les *startups*, ne pourraient que difficilement attirer de l'investissement. Ensuite, cette valeur économique est captée par un très petit nombre d'acteurs qu'un essayiste comme Jaron Lannier, dans son ouvrage *Who Owns the Future*, nomme des *siren servers*, des sirènes, qui attirent les particuliers et leurs données. Par exemple, le fait que nombre de services emploient pour identifier leurs usages une application comme Facebook Connect tend à renforcer la centralité de Facebook dans l'économie générale des usages en ligne : Facebook finit par être le passeport nécessaire pour un nombre signifiant d'activités en ligne. Donc, non seulement nos données personnelles ne sont pas rémunérées, mais, en outre, nous ne percevons pas que ces données sont aux mains d'un nombre limité d'entreprises concentrées sur une aire géographique, qui n'est pas tant les États-Unis que la stricte Silicon Valley ; ce qui n'est pas sans poser une série de problèmes, économiques, stratégiques et politiques.

- Économiques : la valeur économique captée se retrouve captée par la Silicon Valley.
- Stratégiques : les autres écosystèmes de startups lorgnent vers la Silicon Valley, que leur objectif soit seulement de l'émuler, ou d'y transférer leur direction, notamment pour devenir des entreprises globales.
- Politiques : les solutions émanant de la Silicon Valley sont dotées, en creux, d'un outillage mental spécifique, qui, en raison de la domination de ces solutions dans les usages des internautes, tendent à pénétrer l'imaginaire des usages.

Créer un discours critique de ces pratiques est possible, l'imposer devient difficile. Pourtant nous devons poursuivre ce combat car nous sommes au commencement de la métamorphose numérique du monde, où la souveraineté forme un tout : souveraineté des données privées ; souveraineté des données d'entreprise ; souveraineté des données économiques : le pouvoir d'influence sur les marchés des opérateurs en position dominante (Google, Apple, Amazon, etc.) ; souveraineté fiscale : le secteur du numérique échappe aux règles fiscales usuelles ; souveraineté politique : vis-à-vis des États-Unis, le pouvoir d'influence politique de l'Europe est déterminé par sa position de force ou de faiblesse dans les domaines économique, fiscal ou privé.

Aussi pour promouvoir un écosystème numérique régulé, il est nécessaire de maintenir l'outil de la fiscalité en rendant opérant les principes sur lesquels elle repose comme par exemple la capacité à faire de la redistribution.

L'illusion du tout gratuit

La question de la gratuité est récurrente sur Internet. Les internautes ont adopté la gratuité comme règle. L'esprit de partage et de mise à disposition gracieuse, par des particuliers, de ressources et de documents, est une des raisons du déploiement massif de l'Internet dans les vingt-cinq dernières années. Cette habitude de la gratuité provoque, depuis longtemps, des usages problématiques, comme par exemple le piratage massif de certains produits. Ce piratage est souvent lié au fait que la valeur de l'objet piraté n'est pas perçue, et que l'action de piratage n'est pas perçue comme potentiellement nuisible. Dans le cadre du *Big Data*, cette habitude de la gratuité joue potentiellement contre les particuliers qui souscrivent un très grand nombre de services gratuits en ligne. Ils devinent bien que ces services sont produits par des sociétés commerciales et que la possession de leur adresse de messagerie est une richesse potentielle. Toutefois, ils sous-estiment l'étendue et la valeur des données personnelles qu'ils confient à ces sociétés en échange de la possibilité de jouir gratuitement du service qui les intéresse. Même en limitant les données déclaratives qu'ils confient à l'entreprise, ils finissent, à l'usage, par confier des informations nombreuses et précises sur ce qu'ils sont, ce qu'ils font, ce qu'ils apprécient. Ces données personnelles ont une grande valeur économique pour ces entreprises, qui peuvent valoriser chaque utilisateur de leur service entre cinquante et cent euros par an⁵⁹, voire davantage. En un sens, là où certaines entreprises, liées à des économies traditionnelles, devaient déployer des ressources pour lutter contre l'impression de gratuité afin de maintenir des modèles économiques classiques comme l'achat de produits et services, la majeure partie des acteurs du Web s'appuient sur cette impression de gratuité et finissent par masquer aux internautes la valeur réelle de leurs données personnelles : par exemple, le slogan de Facebook est, depuis ses débuts : « Facebook est gratuit et le restera toujours ».

Cette ouverture et cette liberté ont évidemment leurs revers et leurs dangers. La découverte de l'étendue des données collectées par la National Security Agency (NSA) auprès des géants de l'Internet via le programme PRISM a constitué un « séisme » pour les opinions publiques et aussi pour l'ensemble des acteurs de l'Internet. Ceux-ci ont en effet découvert que leurs infrastructures étaient devenues « transparentes » pour les agences gouvernementales.

59 Il y a plusieurs méthodes pour estimer la valeur des données, on peut prendre la capitalisation de Facebook et diviser par le nombre d'abonnés, ce qui fait de 40 à 50 dollars par personne selon la valeur de l'action.

Les libertés à l'ère du numérique: une relation sous tension

Pour la première fois depuis la création de l'Internet, les révélations d'Edward Snowden ont créé les conditions d'un « schisme » entre les industriels de l'Internet et le gouvernement américain. En effet, si elles posent, à juste titre, des questions liées aux risques démocratiques issus de la surveillance de masse, c'est la remise en cause de la confidentialité des données des entreprises qui a constitué le volet le plus inquiétant pour l'ensemble des acteurs économiques. Ainsi, les géants de la Silicon Valley ont fait savoir à Barack Obama à quel point la NSA pouvait remettre en cause la clef de voûte de l'Internet : la confiance de ses usagers⁶⁰. Mark Zuckerberg, PDG de Facebook, déclarait même récemment : « *Le gouvernement américain est devenu une menace pour l'Internet...*⁶¹ »

La notion de surveillance de masse est devenue une réalité pour l'ensemble des opinions publiques mondiales. Au-delà de l'appropriation individuelle du fonctionnement des services et des technologies à des fins sociales, culturelles ou professionnelles, c'est aussi l'appropriation collective de ces technologies et donc la capacité de nos sociétés à édifier une architecture numérique conforme à leurs principes et à leurs valeurs qui sera déterminante pour l'évolution de nos sociétés ; or c'est précisément cette capacité d'appropriation collective qui est remise en cause par l'affaire Snowden. Les révélations de l'ancien contractant de la NSA ont en effet démontré à l'ensemble des opinions publiques que certains de leurs préjugés avaient gravement été ébranlés :

- la volonté des acteurs technologiques de protéger les données de leurs usagers serait un invariant économique ;
- la surveillance ne concernerait que des enquêtes et des individus isolés et pas l'ensemble des citoyens d'un État ;
- seuls les contenus directement issus des usagers devraient être protégés (les métadonnées issues de la navigation des internautes sont « moins sensibles » que le contenu des échanges eux-mêmes) ;
- les entreprises auraient les moyens de protéger leurs données sensibles face à des intrusions ;
- aucun État ne prendrait le risque de fragiliser l'ensemble de l'internet.

Les conséquences sociales et politiques à long terme de l'affaire Snowden commencent à peine à être mesurées. Déjà, certains préjugés sur la nature des échanges sur les réseaux sociaux commencent à être remis en cause. Ainsi, contrairement à la perception commune, les médias sociaux semblent être moins à même de permettre l'échange d'opinions, surtout lorsque ces opinions paraissent être en désaccord avec celles des personnes pour lesquelles il peut être établi un lien de proximité notamment dans les sphères sociale ou professionnelle.

60 *Tech executives to Obama : NSA spying revelations are hurting business* (Washington Post, 17/12/2013)
<http://wapo.st/1kfMSAZ>

61 Éditorial de Mark Zuckerberg posté sur Facebook le 13/03/2014
<http://on.fb.me/1nVf2Cc>

La collecte exponentielle des données face aux risques de l'hypersurveillance

Le coût du stockage de données, la certitude que la valeur est dans la donnée, et les bénéfices apparents que l'individu peut tirer du partage de ses informations sont de nature à encourager une collecte maximale et indifférenciée des données, à partir de deux sources : les données que nous fournissons en employant des applications ou en navigant sur le Web, et les données qui sont collectées à travers les objets connectés que nous portons ou sommes appelés à porter. Même si, dans chaque interface, les données sont collectées à des fins précises et légitimes, deux problèmes demeurent. D'une part, il est tentant, pour chaque entreprise, de changer l'usage de ces données, car cet usage, et donc la valeur des données, peut ne pas apparaître lors de leur collecte initiale. D'autre part, même si les données que je transmets sont initialement anonymisées, le grand nombre d'applications et d'interfaces collectrices de données permettent à terme la réidentification des utilisateurs – une réidentification qu'ils ne désirent pas, mais rendent possible en confiant à des entreprises distinctes des informations qui, recoupées, dessinent un profil si précis qu'il finit par désigner un seul individu.

De la collecte de données au fichage généralisé : de l'affaire Safari à l'affaire Snowden

La consécration de la vie privée des individus a entraîné le développement de nombreux moyens destinés à protéger les données personnelles recueillies par les professionnels. Tout professionnel, au gré de l'expansion de son entreprise, se constitue un fichier-clients via un outil informatique qui aura la particularité de regrouper de nombreuses informations confidentielles devant faire l'objet d'une protection maximale.

En 1973, le projet gouvernemental de Système automatisé pour les fichiers administratifs et le répertoire des individus connu sous le nom de SAFARI envisageait de réunir tous les fichiers nominatifs de l'administration française. En mars 1974, la révélation de cette information par le journal *Le Monde* a contraint le gouvernement à créer une Commission nationale d'informatique et des libertés (CNIL) dans le but de veiller à ce que cet archivage de données personnelles ne porte pas atteinte à la vie privée des administrés. La loi Informatique et libertés de 1978 est ainsi née.

Depuis cette époque, l'idée d'une utilisation massive des données par l'État et les services de renseignement revient régulièrement dans l'actualité. C'est ainsi que les récentes révélations d'Edward Snowden sur PRISM ont démontré que la collecte d'informations des services de renseignement américains était effectuée à grande échelle sur les infrastructures comme la fibre optique et les câbles sous-marins, dans les centres de commutation des données mais aussi sur les réseaux et en exploitant les failles des protocoles comme la faille Heartland dans le protocole Open SSL⁶².

62 Une importante faille de sécurité qui a été découverte en avril 2014 dans OpenSSL, la bibliothèque open-source qui configure la sécurité dans certains systèmes d'exploitation comme Linux, OS X ou encore iOS et Android. Présente depuis 2012 elle aurait permis de subtiliser des données personnelles censées être chiffrées. Ce système de chiffrement est utilisé par la plupart des sites web pour les connexions HTTPS.

Selon Edward Snowden, les services de renseignement s'attaquent également aux technologies de chiffrement. Le programme PRISM a permis à l'Agence nationale de sécurité des États-Unis (NSA) de répertorier toutes les données détenues par les géants du net (Facebook, Microsoft, Yahoo et Google) au nom de la loi antiterroriste (*Patriot Act*) et ce, en contradiction du *safe harbor*⁶³ négocié avec l'Union européenne qui encadre le transfert international de données. Par ailleurs, M. Antonio CASILLI, lors de son audition au CESE, nous indiquait que le gouvernement britannique pratiquait une surveillance à grande échelle de toutes les personnes présentes sur le territoire du Royaume-Uni.

Mais ces révélations montrent aussi très clairement l'ambivalence de la surveillance opérée qui tient à la fois de la lutte contre la criminalité organisée et de la lutte économique. Elle montre aussi un changement radical dans l'approche de la surveillance liée à la capacité de calcul disponible. On passe d'une surveillance ciblée en fonction de suspicions (à l'ancienne) à une surveillance globale sans motif. Cette logique est celle du *Big Data*. On amasse et on voit ce qui peut servir ultérieurement.

Big Data ou Big Brother ?

À proprement parler, la problématique des fichiers n'est pas née avec le *Big Data*, mais, là encore, les innovations apportées par le *Big Data* ouvrent des perspectives de contrôle et de surveillance nouvelles pour les institutions en charge de la sécurité intérieure ou extérieure. Le *Big Data* pousse à une collecte indifférenciée et massive afin d'opérer des traitements automatisés à des fins de prédiction et de profilage. Il pousse à recueillir des données en volume, et à recueillir des données variées, de manière indistincte, dont la finalité n'apparaît souvent pas au moment de la collecte. Parallèlement, les particuliers peuvent être amenés à contribuer à cette collecte, pour profiter eux-mêmes des bénéfices du *Big Data*, par exemple, en renvoyant à des applications de remise en forme des données médicales les concernant qui, comparées aux données d'autres utilisateurs, permettront une personnalisation des recommandations dispensées par l'automate. Les particuliers, en un sens, collectent des volumes de données qui attirent la convoitise des entreprises privées comme des institutions de sécurité.

L'interception et la surveillance des télécommunications, qu'elles soient réalisées dans un cadre administratif, dans un cadre judiciaire, ou hors de tout cadre clair, n'est pas une nouveauté. Mais, là encore, le *Big Data* apporte une innovation incrémentale double qui encourage certaines institutions, américaines comme européennes, à amplifier leurs efforts de surveillance, voire d'espionnage. Cette innovation est double et est liée aux possibilités de prédiction et de profilage que permet le *Big Data*. Concrètement, il est devenu possible voire souhaitable, aux yeux de certaines institutions, de se livrer à un espionnage massif et sans distinction, et d'automatiser le traitement de ces données, afin, par exemple, de repérer des corrélations qui pourraient être significatives dans le cadre d'une mission de surveillance ou de prévention d'attaques terroristes.

Cette tentation de devenir *Big Brother*, grâce au *Big Data*, se heurte heureusement à deux difficultés. Tout d'abord, cette collecte et ce traitement peuvent être en contradiction avec les principes qui fondent nos démocraties. Ensuite, l'efficacité de cette collecte n'est

63 Le *Safe Harbor* est un cadre juridique où sont réunis les principes de la Sphère de sécurité (*Safe Harbor*) permettant à une entreprise américaine de certifier qu'elle respecte la législation de l'Espace économique européen (EEE) afin d'obtenir l'autorisation de transférer des données personnelles de l'Union européenne vers les États-Unis.

pas assurée car, dans le cadre d'une mission de prévention d'actes terroristes, le *Big Data* conserve un défaut : il est utile pour prédire la reproduction ou les répétitions d'événements, mais il demeure mal armé pour détecter les événements inédits. Cela étant, les partisans d'une surveillance accrue pourraient répondre à cet argument « conséquentialiste » que l'automatisation partielle de la veille permet de libérer des ressources pour un travail plus classique de surveillance. Mais, quelle que soit l'efficacité pratique de cette « datafication » de la sécurité, elle demeure une infraction aux législations des pays démocratiques, et une entorse à leurs principes. Toutefois, il faut noter deux points importants : la double promesse de prédiction et de profilage exerce logiquement une forte séduction sur les agences chargées de missions de surveillance – et la concentration des principales ressources de *Big Data* dans les mains d'un petit nombre d'acteurs tous situés aux États-Unis présente un danger, dans la mesure où ces acteurs sont soumis à une forte pression de la part d'agences comme la NSA.

□ *L'essor de la biométrie*

Dans le même temps, on voit se développer depuis quelques années des techniques biométriques en vue de la reconnaissance, de l'authentification ou de l'identification des personnes. Les principales pratiques automatisées sont liées aux empreintes digitales ou à l'iris et des reconnaissances du visage. D'autres modes de reconnaissance sont liés aux dynamiques de frappe sur le clavier d'un ordinateur, la reconnaissance vocale et la dynamique des signatures.

Cette évolution technologique qui s'inscrit dans le prolongement de la rationalisation des techniques policières d'identification prend forme bien avant la Troisième République et s'accélère à partir du dernier tiers du XIX^e siècle⁶⁴. C'est alors qu'Alphonse Bertillon commence à identifier les récidivistes ou présumés récidivistes à partir de leurs corps : relevé des tatouages et des marques particulières, mensuration du crâne, de la coudée, etc. Il tente aussi de recourir à l'identification par l'iris. Il y a une certaine continuité, mais il y a aussi une rupture dans les pratiques du fait de l'évolution des technologies. La biométrie (que l'on pourrait aussi appeler anthropométrie), c'est en réalité du bertillonnage ou de la dactyloscopie, mais couplé aux capacités considérables qu'autorise désormais l'outil informatique en matière de traitement des données.

Les conséquences doivent être appréhendées au regard de ce que les pouvoirs publics font de ces « marqueurs ». Avec l'empreinte digitale se pose la question de la trace, car nous laissons tous nos empreintes partout et à tout moment. D'où la possibilité de croiser ces traces laissées à un endroit avec les empreintes des demandeurs de cartes d'identité qui seraient centralisées dans un fichier unique.

Se pose aussi la question de la propension et de la capacité des services de l'État à croiser ces marqueurs. On peut ici évoquer la tentative des institutions de police américaines de recourir à l'identification faciale lors du Superbowl de Tampa en Floride pour détecter, grâce à des caméras, des individus potentiellement dangereux déjà fichés. Ce que permet ici éventuellement le recours à la vidéo à des fins de surveillance ou de contrôle grâce à l'identification faciale (et à l'insu des individus) serait inimaginable avec les empreintes digitales. On voit les avantages qu'une telle possibilité offre dans la logique qui est celle notamment de l'État. On perçoit aussi les risques qu'elle est toujours susceptible de faire

64 Cf. notamment sur ce point les différents travaux de Vincent Denis in *L'identification biométrique* sous la direction d' Ayse Ceyhan et de Pierre Piazza. Éditions de la Maison des sciences de l'homme. Paris 2011

encourir aux individus : il suffit pour s'en convaincre de discuter avec d'anciens résistants ayant été amenés à recourir aux faux papiers durant l'Occupation.

D'aucuns considèrent que cette technologie amène plus de garanties en matière d'authentification et davantage de possibilités de repérer les tentatives de fraudes en cas de perte de carte, notamment bancaire. C'est aussi pour d'autres un moyen de rendre plus fluides les contrôles d'identité, dans les aéroports par exemple, en recourant à des machines scannant le corps humain. A contrario, les risques inhérents à ces dispositifs de contrôle *high tech* accordant la primauté à la biométrie sont élevés. En plus du risque de réification de l'individu, ramené à la simple dimension d'une donnée, transmissible, qui peut dire actuellement si une base de données contenant des millions d'individus autorisera des contrôles biométriques fiables ? Que se passera-t-il pour les individus en cas de « faux rejets » ? Le « plus de garanties » ne risquerait-il pas alors rapidement de se transformer « en plus de suspicions » ? Quelles procédures sont prévues dans un tel cas, quels recours ? Plus généralement, il faudrait peut-être aussi engager, avant de décider de les mettre en œuvre, une profonde réflexion sur l'impact (positif ou négatif) de ces dispositifs sur les rapports sociaux.

Les récentes applications en matière d'accès à la cantine scolaire, de contrôle des horaires de salariés et en matière de sécurité démontrent un déséquilibre préjudiciable à l'exercice des droits et libertés fondamentaux. Pour citer quelques exemples de dérives, la CNIL a sanctionné des responsables de traitements qui filmaient des employés sur leur lieu de travail ou des établissements scolaires filmant en permanence des enseignants et des élèves, des caméras visualisant l'intérieur d'immeubles.

Le CESE rappelle que dans le domaine de la biométrie, la collecte, la transcription ou la reconnaissance de la donnée pose problème. Les données biométriques permettent un traçage des individus et ces données inhérentes à l'individu ne sont pas révocables.

□ *L'essor de la vidéosurveillance et de la géolocalisation*

Dans la rue, dans les magasins, les transports en commun, les bureaux, les immeubles d'habitation, difficile d'échapper aux caméras installés en France. Bien moins nombreuses qu'au Royaume-Uni où les CCTV (Closed-circuit télévision ou caméra de surveillance) sont légion⁶⁵, la France compte en 2011 935 000 caméras.

Dans un communiqué de presse publié le 21 juin 2012, la CNIL illustre parfaitement l'empreinte dans notre vie quotidienne de la vidéosurveillance : *« Dès que l'on sort de chez soi, on peut être filmé dans le hall de son immeuble, puis sur le chemin du bus pour se rendre au travail. Des caméras peuvent également être présentes dans les transports en commun. À son arrivée sur son lieu de travail, on peut aussi être filmé par les caméras installées par l'employeur. Lors de la pause déjeuner, le magasin où l'on achète sa salade, ou celui où l'on fait ses courses, possède également des caméras pour éviter les vols. Retour au travail pour l'après-midi où une caméra est située dans le hall d'entrée de la société. Le soir, même chemin pour rentrer chez soi, avec des arrêts au distributeur automatique pour retirer de l'argent, sous l'œil d'une caméra, et à la boulangerie pour acheter son pain avec une caméra surveillant la caisse. »*

65 On compte près de 4,200,000 caméras de surveillance dans tous le Royaume-Uni et près de 500,000 rien qu'à Londres. Même si il est prouvé que seulement 3% des crimes sont résolus grâce aux caméras de surveillance (d'après la police britannique), le nombre de ces caméras ne fait qu'augmenter d'années en années, faisant de du Royaume Unis, le pays le plus filmé au monde. On compte une caméra pour 14 personnes.

La vidéosurveillance relève directement des dispositions de la loi dite Informatique et libertés, et concerne la mise sous surveillance de lieux non accessibles par définition au public (bureau de travail par exemple). La vidéoprotection relève quant à elle de l'article 10 de la loi du 21 janvier 1995 d'Orientation et de programmation relative à la sécurité, et concerne les lieux accessibles au public (hall d'entrée d'un immeuble, portail d'une école, d'un établissement public ou d'une entreprise).

La CNIL a reçu en 2011 plus de 360 plaintes relatives à la vidéoprotection et à la vidéosurveillance, ce qui représente une augmentation de 32 % par rapport à 2010. 60 % de ces plaintes concernaient la vidéosurveillance au travail, soit une augmentation de 13 %. La vidéosurveillance ou vidéoprotection, pour reprendre un euphémisme qui a pour fin d'atténuer l'aspect intrusif de ce genre de dispositif, a suscité, au sein même des institutions chargées de la sécurité publique, des débats. Est-ce un dispositif de prévention ? Ou une aide à la résolution des affaires ? Est-ce qu'il n'encourage pas un simple déplacement géographique des actes délictueux, hors de la zone couverte ? Est-ce que ce dispositif n'est pas trop coûteux ? Car le coût réel de ce dispositif ne tient pas seulement à son installation matérielle, mais surtout aux moyens humains qu'il requiert pour fonctionner : il faut mobiliser des personnels pour regarder les flux captés par ce dispositif sans oublier les équipes de maintenance.

Le développement rapide de la vidéosurveillance dans des lieux quotidiennement fréquentés par chacun d'entre nous induit de nombreuses données conservées par des entreprises, des collectivités publiques ou des établissements publics comme les collèges, les lycées mais aussi les écoles et les crèches.

Quant à la géolocalisation, il s'agit d'un outil majeur de contrôle des individus et la sensibilité de ce type d'informations n'est souvent pas perçue par les utilisateurs. Son importance peut, à l'inverse, être perçue par des institutions. Par exemple, lors des émeutes de Londres de 2011, les forces de police britanniques, débordées lors des émeutes par l'usage des émeutiers des réseaux sociaux, ont su utiliser, après les événements, l'oubli par les émeutiers de leur géolocalisation dans diverses applications, comme Four Square, qui les plaçaient sur les lieux d'un délit, à l'heure dudit délit. À l'inverse, la géolocalisation d'une personne peut être employée pour déterminer qu'elle n'est pas chez elle et que son domicile peut être cambriolé. Cela étant, ces usages ne relèvent pas du *Big Data*. Là où le *Big Data* a un rapport direct avec cette problématique réside dans la valeur que représente la géolocalisation comme information, permettant par exemple de repérer des phénomènes et des corrélations dans les transports urbains, et de piloter de manière plus fine la gestion de ces transports, en termes d'horaires, de moyens matériels et de moyens humains. Même anonymisée, cette information reste sensible et elle demeure, par recoupement, un outil aisé de réidentification de l'individu.

Vie privée et protection des données personnelles

72% des Français pensent que le numérique a un effet négatif sur la vie privée (Sondage TNS-Sofres 2^{ème} édition mars 2014). Ce constat révélé par la deuxième édition du Baromètre Inria pose la question de la responsabilité des Français face au numérique. Mais qui est responsable de la protection et du respect de nos vies privées ?

Ce constat est surtout lié à l'augmentation des usages. Auparavant les Français utilisaient peu le numérique et ce qu'ils voyaient essentiellement dans les outils numériques c'était la complexité. Aujourd'hui ils utilisent le numérique au quotidien, ils n'en comprennent pas tout, mais ils se considèrent comme définitivement impliqués dans ce monde-là et donc s'interrogent sur ce qui se passe « vraiment ».

La protection de la vie privée : risques et inquiétudes

Dans le domaine de la protection des données personnelles, tout porte à croire que notre société devient schizophrène. Elle garantit, au moins formellement, pour chaque citoyen la liberté de s'exprimer et de communiquer, en particulier sur les réseaux électroniques et le respect, dans le cadre de la loi, de sa vie privée. Chacun veut surfer en toute liberté sur le Net, envoyer des mails à qui bon lui semble et souhaite rarement la transparence complète sur sa vie personnelle et ses affaires. Mais il veut également accéder à toute l'information en ligne, remplir les dossiers administratifs en quelques clics - ce qui évidemment sous-entend que les informations indispensables à la connaissance de sa situation personnelle dispersées entre diverses administrations soient interconnectées - et profiter des avantages de l'achat en ligne auprès de sociétés qui lui font des offres en fonction de son profil - donc des informations qu'elles possèdent sur lui. L'homme politique, devant la complexité de la législation et de la « paperasserie administrative » prêche pour l'administration électronique, le guichet unique et veut connaître les demandes de la société pour y répondre plus efficacement, d'où la multiplication des fichiers « sociaux » et l'accumulation de données sur les personnes en difficulté. De même, devant le sentiment de la montée de l'insécurité et la poursuite de la rationalisation des forces de police, la solution de facilité est de fichier tout suspect, tout comportement « déviant » et de généraliser l'accès à ces informations à tous les policiers assermentés. C'est également la tentation de la surveillance du courrier électronique, l'enregistrement des internautes accédant à certains sites, la chasse aux « pirates » et aux « hackers » et aux groupes criminels. Les entreprises ne sont pas en reste. Elles veulent dresser des profils de leurs clients, les fidéliser par des offres personnalisées, et agrandir leur terrain de prospection en achetant et en échangeant des fichiers avec des officines spécialisées dans ce travail. Une tendance lourde traverse donc toute la société et le citoyen bien que méfiant au départ, est en partie consentant car quelque part, il espère bénéficier des retombées de ce quadrillage « virtuel ». Une régulation s'impose, sinon un jour prochain nous serons suivis en permanence grâce à un implant enfoui au plus profond de notre corps, comme dans le film de Steven Spielberg, *Minority report*.

□ Données personnelles et interopérabilité des réseaux

La révolution numérique s'est accompagnée d'une irréversibilité croissante des interactions et des échanges avec des dispositifs technologiques de plus en plus sophistiquées. L'interopérabilité croissante de ces dispositifs, l'interconnexion plus grande des fichiers de données et la confusion des temps sociaux et intimes avec les temps liés à la sphère professionnelle et celle des loisirs que l'importance du travail en réseau, amplifie contribuent à remettre en cause la notion même de sphère privée.

Même si celle-ci ne se définit plus aussi aisément en opposition avec la sphère publique, il n'en demeure pas moins que l'exigence de transparence qu'exige la société du numérique invite à la plus grande prudence sur le dévoilement de soi. 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 sont telles qu'elles ont vite fait de remettre en cause

cet équilibre en s'immisçant dans notre sphère intime via le prélèvement et la collecte des données personnelles. Le traçage par les réseaux, la biométrie, la géolocalisation, les nanotechnologies, la vidéosurveillance participent d'une mise en visibilité publique d'informations qui relèvent du domaine privé.

Cette évolution technologique conduit à replacer la protection de la vie privée au cœur des réflexions de la défense des libertés à l'ère du numérique.

□ *Privacy paradox*

Face à l'irruption des réseaux sociaux, l'individu serait inquiet de l'utilisation de ses données mais parallèlement divulguerait de plus en plus de données personnelles volontairement ou non. On parle alors de paradoxe de la vie privée. En fait il s'agit plus d'un double sentiment parallèle d'envie d'utilisation et de perte de contrôle. Plus les Français utilisent le numérique, plus ils se demandent comment ça fonctionne et veulent être rassurés, et cette tendance ne peut que se poursuivre. La durée de conservation des données et le droit à l'oubli sont alors au cœur de leur réflexion. Pourquoi des lors cette apparente incohérence est-elle devenue en quelques années un élément incontournable du débat sur la vie privée ?

Pour les grands acteurs du net, et notamment Google, les débats à propos de la vie privée seraient révolus et la vie publique devenue la norme sociale. « L'évangéliste » en chef de Google, Vint Cerf, parle même de « publitude », en opposition à la vie privée source de solitude. La vie privée n'aurait donc été qu'une anomalie de l'histoire liée à la société industrielle du XIX^e siècle. Or le concept de vie privée est lié consubstantiellement à l'affirmation des droits de l'Homme et du citoyen et à la démocratie.

Si la vie privée telle que nous la connaissons historiquement est destinée à disparaître dans un contexte de communication connectée, les révélations d'Edward Snowden n'ont pas signé pour autant sa disparition mais ont placé la société face à un besoin impérieux de protéger la vie privée du citoyen.

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 de concept américain de *right to be left alone* (le droit d'être laissé tranquille). Cette vision demeure la plupart du temps alors qu'en fait la tendance est à confondre secret et privé. Yves Pouillet et Cécile de Terwang ont insisté sur ce changement dans la notion de « zone personnelle » en citant l'arrêt Rotaru de la CEDH de 2000 : « *Ce que vous faisiez chez vous, montrer des photos, des vidéos, gérer l'agenda... se retrouve dans le cloud. Cela reste personnel mais nécessite des acteurs techniques intermédiaires.* » En d'autres termes, le développement technique opère une gestion fonctionnelle de notre vie privée. Le droit s'immisce donc chez les individus via des outils impliquant des intervenants. Pour préserver totalement la vie privée au sens d'un cœur isolé, la solution de la déconnexion de tout réseau apparaît la solution la plus efficace sauf à considérer l'obsolescence des données numériques comme une voie possible pour une meilleure protection. Mais elle a un coût : celui de se retirer du réseau. Ou alors l'ouverture sur les données numérique conduit à ouvrir notre notion de sphère personnelle et créer dans la foulée des responsabilités pour ces tiers. 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.

□ *La vie privée, un problème de contextualisation*

Les utilisateurs des réseaux sociaux, notamment les plus jeunes, savent changer d'identité par l'utilisation des pseudonymes et apprennent à restreindre l'accès à leurs profils. Quant aux géants du web, ils changent de discours en abandonnant la rhétorique de la fin de la vie privée qui avait été leur cheval de bataille depuis des années. La vie privée - ce que je veux publier sur moi et ce que j'autorise les autres à publier sur moi - cesse d'être un droit individuel pour devenir une négociation collective.

La vie privée devient alors un problème de contextualisation dont la valeur principale réside dans la capacité d'arbitrage entre l'intime et le secret. La formule de la Fondation Internet Nouvelle Génération (FING) résume assez bien ce constat : « *La vie privée serait définie comme la possibilité de pouvoir choisir sa vie publique sans renoncer à l'intime et au secret.* » Le refus du partage de certaines données (secret), le droit à être laissé seul (la tranquillité) et l'autonomie individuelle (garder la maîtrise de certaines données) apparaissent comme essentiels mais ces droits effectifs ne peuvent que s'appuyer sur des complémentarités entre la loi et la technologie.

Aussi il est nécessaire pour assurer cette maîtrise de rétablir ce pouvoir de négociation collective entre les groupes de citoyens et les acteurs du numérique pour assurer une maîtrise de cette vie privée. Il est essentiel que les lois redonnent un nouveau pouvoir de négociation collective face à l'État et aux acteurs commerciaux

Cela passe notamment par le renouvellement de l'encadrement légal de ces négociations où l'on passe d'un web de publication à un web d'émission et de production de données. Dans tous les cas, le respect du droit à la vie privée comme un droit constitutionnel doit être maintenu.

Open Data et données personnelles

Depuis la loi n°78-753 du 17 juillet 1978, toute personne peut avoir accès aux documents détenus par une administration dans le cadre de sa mission de service public. Modifiée en 2005 pour transposer en droit français une directive de 2003, cette loi permet également depuis cette date la réutilisation des informations publiques à d'autres fins que celles pour lesquelles elles sont élaborées ou recueillies.

A titre général, l'*Open Data* ne concerne pas directement la protection des données à caractère personnel : la majorité des informations du secteur public mises à disposition des internautes ne comportent aucune donnée personnelle (exemples de la localisation et horaires d'ouverture des services publics, des événements culturels et sportifs, des mesures sur la qualité de l'air, sur la pollution des eaux, etc., des informations touristiques ; etc.). Néanmoins, les organismes publics détiennent une très grande variété de données pour constituer des informations du secteur public (données administratives, données médicales, état civil, adresses, etc.). Ces informations ont toutes vocation, dans le cadre de l'*Open Data*, à être mises à disposition sur Internet.

Dans ce cadre, il existe deux hypothèses dans lesquelles l'*Open Data* implique, directement ou indirectement, le traitement de données à caractère personnel.

□ *Le traitement de données personnelles et l'Open Data : deux hypothèses*

La première hypothèse est liée à la situation où les informations du secteur public se composent elles-mêmes de données à caractère personnel.

Les acteurs publics en charge de réaliser une mission de service public disposent de très nombreuses informations, dont certaines comprennent évidemment des données à caractère personnel relatives aux administrés. Il peut s'agir en premier lieu de données à caractère personnel publiées pour répondre à une obligation explicite du législateur, notamment pour assurer la publicité légale d'une information publique et produire ainsi les effets juridiques liés à l'acte administratif. Exemples : arrêté de nomination d'un agent public, arrêté d'attribution d'une médaille du travail ; permis de construire ; annuaires des agents des administrations ; résultats d'examen ; etc.

Il peut également s'agir de données à caractère personnel dont la communication et la réutilisation sont encadrées (les destinataires bénéficiant de ce droit d'accès à l'information complète sont alors qualifiés de « tiers autorisés »), ou au contraire interdites. Exemples : relevés de propriété ; salaires des hauts fonctionnaires ; avis d'imposition ; liste électorale ; actes de l'état civil ; archives publiques ; données cadastrales ; etc.

Enfin, les administrations disposent de très nombreuses informations contenant d'autres données à caractère personnel identifiantes, directement ou indirectement, dont la mise à disposition sur Internet ou la communication à des tiers non autorisés ne peut être opérée sans avoir été préalablement anonymisées. Néanmoins, il est envisageable que certaines de ces données à caractère personnel soient mises à disposition, non de façon intentionnelle, mais à cause d'une anonymisation insuffisante. Exemples : statistiques judiciaires avec unités trop faibles ; statistiques fiscales avec une attache géographique trop étroite ; « base géographique de référence » [cf. cadastre.gouv.fr] ; etc.

La seconde hypothèse concerne la réutilisation des informations publiques qui peut permettre, par recoupement, l'identification ou la réidentification de personnes.

Sans même contenir initialement de données identifiantes, les informations publiques peuvent, par recoupement, soit avec d'autres informations publiques mises à disposition, soit avec d'autres données disponibles sur Internet, permettre l'identification ou la réidentification de personnes physiques. Cette identification pourrait ainsi intervenir par le biais du recoupement d'informations en *Open Data* ou du recoupement entre informations *Open Data* et informations *Big Data*. Le caractère « personnel » de la donnée est alors attribué aux informations publiques mises à disposition, non par nature, mais par destination. Plus que sa qualité intrinsèque, c'est bien l'usage fait de la donnée initiale qui lui confère son caractère personnel.

Prenons l'exemple des parcelles cadastrales. Le site cadastre.gouv.fr met à disposition la référence et l'adresse de la parcelle cadastrale, sans autre donnée personnelle. Des mesures sont prises pour limiter au maximum la diffusion de données à caractère personnel, ce qui matérialise le droit d'opposition des personnes concernées à la diffusion sur Internet de données les concernant : les photographies des maisons individuelles et des personnes sont occultées, ainsi que les mécanismes de sécurité des entrées ; les données de thermographie sont agrégées au niveau d'un quartier ; etc. Néanmoins, l'identité de ces personnes est susceptible d'être révélée par une simple recherche annuaire inversé.

L'autre exemple similaire est celui du portail « Paris Data », qui diffuse de nombreuses données cartographiques, par exemple la carte des 70 espèces d'arbres présentes à Paris, utile pour les allergiques. Les données mises à disposition sur ce portail peuvent néanmoins permettre l'identification des personnes via le plan parcellaire qu'il propose. Fort de ces informations « anonymes » conjuguées à des données personnelles déjà structurées ou simplement accessibles, tout responsable de traitement, et plus largement encore tout

internaute, pourra aisément compléter le profil des personnes dont il détient déjà des données identifiantes. De façon paradoxale, cette seconde hypothèse est donc à la fois la plus probable (les administrations n'ont pas la volonté première de diffuser directement des données à caractère personnel) et la moins prévisible : les réidentifications de personnes vont souvent intervenir de manière incidente, c'est-à-dire sans volonté particulière du réutilisateur qui va simplement enrichir son patrimoine informationnel préexistant. Quelle que soit l'origine ou la modalité d'une telle réidentification, il s'agira alors d'un traitement de données à caractère personnel.

A cet égard, il y a lieu de rappeler l'acceptation large des notions de donnée à caractère personnel et de traitement de données que la CNIL⁶⁶, comme le G29⁶⁷, a toujours retenus : toute information est susceptible de constituer une donnée à caractère personnel, dès lors que, combinée avec d'autres informations, elle est susceptible de permettre l'identification de personnes physiques. Cette acceptation large est d'ailleurs maintenue dans le cadre du projet de règlement communautaire concernant la protection des données personnelles⁶⁸.

□ Les problématiques « de vie privée » soulevées par l'Open Data

En postulant que les traitements liés à l'Open Data impliquent la mise en œuvre de traitements de données à caractère personnel, et la mise à disposition et à la réutilisation d'informations publiques, force est de constater que l'Open Data soulève, par essence, des difficultés importantes du point de vue de la protection des données personnelles, et plus globalement de la vie privée. Si ces risques sont difficiles à apprécier *a priori*, du fait du manque de recul et des possibilités infinies de traitement et de retraitement des informations publiques, il n'en demeure pas moins pour le CESE qu'il est nécessaire de les anticiper.

La seconde difficulté majeure cristallisée par l'Open Data est de raisonner en termes de collecte et de traitement alors qu'est en cause la réutilisation.

Ce qu'introduit l'Open Data, c'est précisément la déconnexion entre le temps de la collecte des données brutes et du traitement lui-même, et celui de la réutilisation des données lors des multiples traitements ultérieurs. On voit alors que les notions de finalités, destinataires, données pertinentes, etc. perdent une partie de leur sens.

En réalité, l'Open Data fait peser, par nature, des interrogations sur l'ensemble des principes cardinaux de la protection des données personnelles, au premier rang desquels le principe fondateur de finalité que nous avons parcouru plus haut. En effet, le seul objectif d'une plateforme Open Data est de rendre accessible l'information du secteur public au plus grand nombre. On pourrait dès lors considérer que la mise à disposition d'informations publiques a pour finalité d'assurer le « service public de diffusion de l'information », contribuant ainsi à la transparence du fonctionnement des organismes publics. Il n'en demeure pas moins que cette finalité très générale ne répond que difficilement à l'exigence d'une finalité « déterminée ».

Le principe de finalité est d'autant plus mis à mal que l'objectif de l'Open Data est précisément d'alimenter des traitements de réutilisation in(dé)finie. Ces traitements seront en effet développés au gré des innovations que les données ouvertes ne manqueront pas de susciter auprès de leurs lecteurs. Les finalités espérées par le mouvement de l'Open Data

66 Commission Nationale de l'Informatique et des libertés

67 Groupement des CNILs européennes

68 Le rapport du parlementaire européen ALBRECHT confirme la nécessité de maintenir une telle définition large

sont donc in(dé)finies avant toute utilisation par des personnes autres que le producteur des informations publiques⁶⁹.

Toutefois l'*Open Data* n'intervient pas en l'absence de tout cadre juridique : depuis 1978, la loi « Cada » et la loi « Informatique et Libertés » articulent l'accessibilité à l'information publique et la protection des données personnelles. L'article 13 de la loi du 17 juillet 1978 prévoit que les informations publiques comportant des données à caractère personnel peuvent être réutilisées si l'intéressé y a consenti, ou si l'autorité détentrice est en mesure de les rendre anonymes ou encore, à défaut d'anonymisation, si une disposition législative ou réglementaire le permet⁷⁰. Elle précise aussi que cette réutilisation est subordonnée au respect des dispositions de la loi n°78-17 du 6 janvier 1978 dite « Informatique et libertés ».

Cependant, la révolution technique et le changement d'échelle introduits par l'*Open Data* modifient la donne. Le volume des informations accessibles en *Open Data* sur support aisément exploitable permettant d'être combinées à d'autres données, est susceptible de remettre en cause l'équilibre précaire entre ces deux droits fondamentaux. Plus que l'*Open Data* lui-même, c'est bien le contexte dans lequel il s'inscrit (informatisation complète de la société, administrations comme acteurs privés ; diffusion spontanée de données personnelles par les internautes ; indexation sur des données nominatives par de puissants moteurs de recherche ; développement du *Big Data* ; etc.) qui rend nécessaire la recherche d'un nouvel équilibre entre protection de l'administré (et notamment de ses données personnelles) et transparence de l'administration (accès à l'information publique).

Il importe dès lors de définir un encadrement adapté qui, tout en étant suffisamment flexible pour permettre l'essor de l'*Open Data*, garantira des mesures efficaces pour protéger les administrés et leurs données personnelles.

Objets connectés et algorithmes : nouveaux enjeux et nouveaux risques

Dans les premiers temps du développement de l'Internet auprès du grand public, les données qui étaient échangées étaient souvent décrites comme celles d'un réseau distinct du monde physique créant une forme de réalité parallèle ou virtuelle. Désormais, les données qui transitent sur le réseau sont intégrées (ou issues) de l'ensemble des activités quotidiennes des citoyens. L'évolution prochaine vers ce que l'on nomme désormais l'Internet des objets devrait amplifier ce phénomène d'indistinction entre le réseau et les activités humaines.

⁶⁹ Exemples de finalités des réutilisations actuellement observables : nosdeputes.fr ; dentistedegarde.net (site récemment fermé pour cause d'interruption de la source) ; amel.fr ; etc. Autre exemple : en 2012, nombre de services publics d'archives ont largement diffusés sur Internet les images et données des actes de l'état civil devenus « librement communicables ».

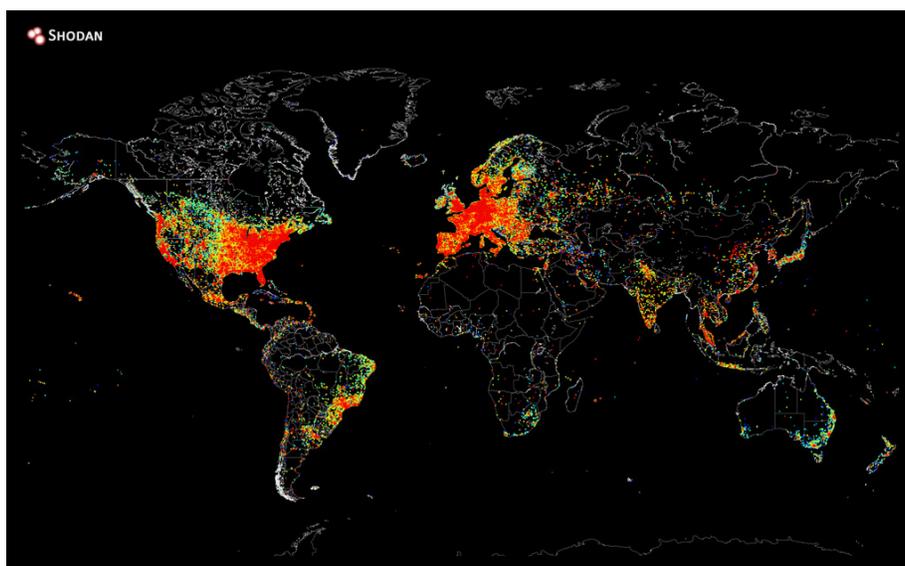
⁷⁰ C'est ce second volet de la loi qui devra être modifié pour le rendre conforme à la nouvelle directive de 2013/37/UE du 26 juin 2013 modifiant la directive 2003/98/CE concernant la réutilisation d'informations détenues par le secteur public. La nouvelle directive ne remet pas en cause ce principe, bien au contraire. Elle écarte en effet explicitement du droit à réutilisation les documents dont l'accès est exclu ou limité pour des motifs de protection des données à caractère personnel ou dont la réutilisation a été définie par la loi interne de l'Etat membre comme incompatible avec la législation protégeant les données à caractère personnel. Les Etats membres de l'Union Européenne disposent d'un délai de deux ans pour transposer cette directive.

□ Hyper-connexion et banalisation de la captation des données

La distinction qui existe encore aujourd'hui entre connexion et déconnexion vis-à-vis de l'Internet devrait tendre à disparaître à mesure que les capteurs et objets connectés transmettront des informations en permanence dans notre environnement. C'est déjà le cas de nombreux services issus des capteurs présents dans les terminaux mobiles (smartphones et tablettes) qui analysent les activités de leurs utilisateurs⁷¹. Cette évolution vers un usage massif des données issues des capteurs sera encore plus visible avec la montée en puissance des objets connectés qui seront pour la plupart dotés de capteurs. En effet, une fois équipés de capteurs et de dispositifs de transmission, les objets deviennent à leur tour des vecteurs de nouveaux services à valeur ajoutée⁷². La prise en compte de la dynamique de fonctionnement de ces objets connectés (depuis leur conception jusqu'à leur destruction) constituera l'une des nouvelles frontières de l'éducation numérique. Cette révolution numérique se traduit par une banalisation de la captation automatique de données personnelles. C'est ainsi le concept de ville intelligente, où le domaine des transports repose sur une géolocalisation permanente des individus, afin de répondre aux besoins de chacun et conduire une politique de développement durable au profit du bien commun.

La numérisation de nos activités humaines n'a dès lors plus de limites. Elle peut concerner notre voiture, nos appareils électroménagers mais également notre corps et ce que nous en faisons.

Cartographie mondiale des objets connectés réalisée par le moteur Shodan⁷³



71 *Les mouvements des smartphones pourraient révéler aux automobilistes les emplacements disponibles* (MIT Technology Review, 15 septembre 2014).

<http://www.technologyreview.com/news/530671/smartphone-movements-could-reveal-empty-parking-spots/>

72 *20 % des grandes entreprises investissent dans l'Internet des objets* (Proxima Mobile - 21 août 2014)

<http://www.proximamobile.fr/article/20-des-grandes-entreprises-investissent-dans-l'Internet-des-objets>

73 <http://www.proximamobile.fr/article/une-cartographie-mondiale-de-l'Internet-des-objets>

□ Du *quantified self* au système de santé⁷⁴

L'un des champs les plus complexes et les plus prometteurs mais parfois aussi les plus inquiétants dans l'utilisation des données personnelles concerne la santé et la prévention. Ce mouvement qui repose sur une utilisation croissante de capteurs corporels connectés – bracelets, podomètres, balances, tensiomètres, etc. – et d'applications sur mobiles, s'accompagnent de pratiques volontaires d'auto-quantification qui se caractérisent par des modes de captures de données de plus en plus automatisés, et par le partage et la circulation de volumes considérables de données personnelles. Un phénomène qui se développe à l'initiative des individus eux-mêmes et aussi, en raison des modèles économiques des acteurs investissant ce marché.

Ainsi, la montée en puissance de nouveaux dispositifs de suivi et de diagnostic pourrait transformer l'ensemble du système de santé. La chute des coûts des capteurs et l'articulation des objets connectés avec les terminaux mobiles (smartphones, tablettes, voire bientôt les lunettes et les montres connectées) permettent la mise en place de capteurs permanents auprès des patients afin de suivre leurs activités et détecter les premiers signes de certaines pathologies. Selon une étude de Bloomberg de 2013, les capteurs intégrés devraient passer de 100 millions d'unités en 2014 à 2800 milliards en 2020.

Cette évolution vers l'acquisition de données médicales au détour des activités quotidiennes constitue l'un des marchés clés pour les technologies mobiles. Selon les études de marché sur la santé mobile, l'ensemble de ces technologies pourrait ainsi représenter en 2017 un marché mondial de 26 milliards de dollars, dont plus du quart proviendrait de l'Europe⁷⁵. Au-delà des innovations qui seront mises en place auprès des patients, les technologies de la santé mobile devraient transformer l'ensemble des infrastructures de santé. Ainsi au niveau des centres de soin elles permettront de transformer les missions de ces structures à la fois pour orienter celles-ci vers la prévention des pathologies. La gestion des données pourrait ainsi devenir le cœur de métier des structures de santé. Ainsi, Eric Topol, professeur de génomique au Scripps Research Institute déclare : « *Excepté pour certaines fonctions clés comme les soins intensifs et la chirurgie, les hôpitaux seront entièrement transformés en centres de surveillance des données. Les gens souriront en repensant aux visites chez leur médecin avec le légendaire stéthoscope ainsi que l'ensemble des pratiques qui existaient avant l'ère numérique*⁷⁶ ».

Pour accompagner ces évolutions, il conviendra de permettre aux citoyens de s'appropriier les nouvelles formes que prendront les institutions sanitaires et le système de santé. Leur permettre aussi de mieux comprendre les évolutions de nos sociétés face à ces évolutions.

Les acteurs du secteur prudentiel sont aussi directement impliqués dans l'équation économique de la santé mobile⁷⁷. En effet l'articulation entre les acteurs des technologies de la santé mobile et les sociétés d'assurances a d'autant plus de sens que ces nouveaux

74 « Aujourd'hui nous appelons ces technologies "mesure de soi" (*quantified self*) demain nous les appellerons "système de santé" » « The Body-Data Craze » (*Newsweek*, 26 juin 2013).

75 <http://research2guidance.com/the-market-for-mhealth-app-services-will-reach-26-billion-by-2017/>

76 Eric Topol, « *On the Future of Medicine* » – *Wall Street Journal* 7 juillet 2014. <http://online.wsj.com/articles/eric-topol-on-the-future-of-medicine-1404765024>, voir aussi son ouvrage *The Creative Destruction of Medicine* (Ed. Basic Books - janvier 2012).

77 *Wearable Tech Is Plugging Into Health Insurance* (*Forbes*, 19 juin 2014). <http://www.forbes.com/sites/parmyolson/2014/06/19/wearable-tech-health-insurance/>

capteurs pourraient permettre la détection précoce des pathologies et ainsi repousser dans le temps la nécessité pour les assureurs d'avoir à prendre en charge dans la durée des pathologies lourdes et coûteuses.

Le traitement à distance des données des patients n'est pas encore intégré dans l'équation économique de la santé en France à l'inverse de nos voisins britanniques où les médecins peuvent prescrire des applications mobiles ou des objets connectés dédiés à la santé⁷⁸. Cette évolution n'est que le premier pas vers des transformations beaucoup plus radicales de l'économie de la santé. Le *Nouvel Économiste* résumait ainsi les raisons qui ont jusqu'ici prévalu pour expliquer les enjeux liés à aux évolutions de la médecine numérique ainsi qu'aux difficultés à faire évoluer le système de santé en France : « *Blocages défensifs, crispations corporatistes, carence de compétences, – de management surtout –, se conjuguent pour contrarier ces mutations majeures, plus certainement que l'argument traditionnel du manque de ressources financières. Et l'absence d'impulsion politique au plus haut niveau ne fait que rajouter à la difficulté*⁷⁹... »

Les débats sur la nécessité pour les citoyens de maîtriser l'usage qui est fait de leurs données personnelles ont conduit certains acteurs à envisager un « droit de propriété » sur ces données. Cela conduirait par voie de conséquence à envisager la cessibilité de ces données, en particulier pour des raisons économiques⁸⁰. Cette perspective a été à juste titre considérée par le Conseil d'État⁸¹ comme un risque pour les citoyens. En effet, la multiplication des opportunités offertes par les acteurs économiques en particulier dans le domaine de la santé de valoriser ces données pourrait mener à des situations de risques accrus pour les libertés individuelles. La publication des données relatives à la forme et à la santé (par exemple sur les réseaux sociaux) peut aussi devenir un outil de contrôle économique et social voire de « profilage » des risques associés à un individu. Les craintes concernant l'utilisation des données personnelles médicales sont d'autant plus légitimes que des données personnelles en apparence anodines peuvent être intégrées dans des algorithmes d'évaluation des risques de santé. Ainsi, l'achat d'une friteuse ou la consommation de substances riches en graisse pourraient participer à l'élévation des risques cardio-vasculaires d'un usager bien avant qu'il soit besoin de vérifier qu'une personne participe à un groupe de discussion sur une pathologie particulière sur les réseaux sociaux⁸². Lorsque les dispositifs de captation d'information de santé seront intégrés dans l'ensemble des terminaux mobiles et objets connectés (comme les nouvelles générations de montres connectées) ou les vêtements ou accessoires sportifs, le recueil de ces informations pourrait devenir encore plus sensible en termes d'évaluation précise du profil des risques associés à une personne. Ainsi, la transmission non contrôlée de ces informations à des annonceurs pourrait avoir

78 Le ministre de la Santé britannique incite médecins et patients à utiliser des applications mobiles <http://www.proximamobile.fr/article/le-ministre-anglais-de-la-sante-demande-aux-medecins-d-inciter-leurs-patients-utiliser-des-a>

79 e-Santé : les technologies sont là, les mentalités pas encore (Patrick Arnoux, *Le Nouvel Économiste* - 5 août 2014) <http://www.lenouveleconomiste.fr/e-sante-les-technologies-les-mentalites-pas-encore-23635/>

80 *How Much Is Your Privacy Worth ?* (MIT Technology Review, 26 août 2014).

<http://www.technologyreview.com/news/529686/how-much-is-your-privacy-worth>

81 « *Le droit sur les données personnelles, un droit à l'autodétermination plutôt qu'un droit de propriété* », étude annuelle 2014 du Conseil d'État : *Le numérique et les droits fondamentaux* (p264) <http://www.ladocumentationfrancaise.fr/rapports-publics/144000541-etude-annuelle-2014-du-conseil-d-État-le-numerique-et-les-droits-fondamentaux>

82 *The creepy side of data mining: Selling "sick" lists* (CBS Moneywatch 11 septembre 2014) <http://www.cbsnews.com/news/the-creepy-side-of-data-mining-selling-sick-lists/>

des conséquences imprévisibles. Ces préoccupations de maîtrise des données de santé liées aux objets connectés sont telles que la société Apple vient d'annoncer que les données qui transiteront via son système de centralisation des données de santé ne devraient pas être transmises (ou revendues) à des annonceurs publicitaires⁸³.

Puissance des plateformes et pouvoir des algorithmes

Cependant, l'un des enseignements de l'affaire Snowden aura été de montrer à quel point ces métadonnées, qu'elles soient téléphoniques ou liées à la navigation des internautes, peuvent être souvent plus révélatrices des individus que le contenu même des messages échangés. En effet, la puissance de traitement dont disposent ces plateformes et les algorithmes en permanence améliorés pour tirer parti de ces vastes collections de données permettent d'interpréter les comportements des utilisateurs ainsi que leurs préférences au point de prédire certaines de leurs actions.

Ces algorithmes deviennent d'autant plus cruciaux qu'ils s'appliquent à des services intégrés à chacune de nos activités quotidiennes, via les terminaux mobiles qui deviennent progressivement nos « exo-cerveaux » et cela avant même l'essor des objets connectés comme les lunettes à réalité augmentée ou les accessoires médicaux mobiles. L'ensemble des activités professionnelles qui auront recours à des technologies prédictives basées sur l'analyse de données en masse ne pourront faire l'économie d'une réflexion éthique sur la responsabilité des créateurs de ces algorithmes et des entreprises qui les emploient. Ainsi, à mesure que sont développées les voitures autopilotées, des questions nouvelles se posent quant au degré de responsabilité des personnes qui programmeront ces algorithmes lorsque des vies humaines auront été mises en danger⁸⁴.

Des questions de nature politique se poseront aussi lorsque l'analyse des données à l'échelle d'une population pourra aboutir à des ciblage ethniques, politiques ou religieux⁸⁵. Ainsi, l'analyse des données liées aux crimes et délits passés est désormais utilisée pour prévoir les lieux les plus probables pour les activités criminelles à venir. Aux États-Unis, les unités de police dotées de ces systèmes prédictifs commencent même à en mesurer les effets sur la diminution de la criminalité urbaine⁸⁶. Dès lors la poursuite légitime ou jugée comme telle de la diminution du risque peut conduire à la mise sous surveillance de tous, faisant de chacun un suspect potentiel, dans l'espoir ou l'assurance d'anticiper la survenance du fait poursuivi.

□ *La mise en donnée : du monde du profilage à la prédiction*

La « datafication » de toute chose est un phénomène récent, même si la mise en nombres et mesures du monde est un phénomène ancien, qui s'est accéléré à l'époque moderne.

83 Apple tells developers they may not sell personal health data to advertisers. The company has tightened its privacy rules in run up to announcements of new technology expected in September.

<http://www.theguardian.com/technology/2014/aug/29/apple-health-data-privacy-developers-advertisers>

84 *The Feds Stall Self-Driving Cars* (Wall Street Journal - 24 août 2014).

<http://online.wsj.com/articles/gordon-crovitz-the-feds-stall-self-driving-cars-1408919700>

85 *Big Data Can Be Used for Good in the Community* (New York Times 6 août 2014)

<http://www.nytimes.com/roomfordebate/2014/08/06/is-big-data-spreading-inequality/big-data-can-be-used-for-good-in-the-community>

86 *'Predictive Policing' Technology Lowers Crime In Los Angeles* (Huffington Post Greg Risling 7 janvier 2012)

http://www.huffingtonpost.com/2012/07/01/predictive-policing-technology-los-angeles_n_1641276.html

La mise en donnée, non seulement des personnes, mais des choses, s'est récemment intensifiée, notamment car nous nous sommes dotés d'outils d'enregistrement et de capture de ces données : là où, dans le passé, la mesure était une fonction confiée à certains, elle est désormais aux mains de tous et, le plus souvent, de manière involontaire et indistincte. Involontaire, car nous enregistrons en permanence ces informations, par nos pratiques de navigation ou nos usages de nos terminaux mobiles. Indistincte car, parallèlement aux données dont nous connaissons l'usage, nombre des données, personnelles ou non, qui sont collectées, le sont pour un usage futur possible, que nous ne connaissons pas encore. À titre d'exemple, on pourrait montrer le renversement qui s'est opéré entre un âge où réaliser une étude consistait à collecter volontairement des données, après coup, pour tester une hypothèse, et un âge, notre âge, où l'établissement de corrélations entre deux faits statistiques peut être établi sur-le-champ grâce aux grands nombres qui ont été collectés indistinctement par les individus et les entreprises.

Cette « datafication » est une progression quantitative qui a un effet qualitatif permettant deux actions auparavant difficilement accessibles : la prédiction et le profilage. La possibilité de prédiction apportée par le *Big Data* repose principalement sur l'idée que le *Big Data* permet de relever des corrélations statistiques régulières et récurrentes entre des phénomènes, en faisant l'économie de la compréhension exacte de ce qui cause tel ou tel phénomène. Concrètement, la prédiction, de causale, devient statistique. Là où auparavant, nous émettions des hypothèses (si telle chose se passe, telle autre chose devrait se passer), nous faisons désormais le pari, régulièrement juste, que si telle chose et telle chose se produisent habituellement ensemble (et même si la raison de leur corrélation nous échappe), alors, la survenance d'une des deux choses m'indique l'imminence de l'autre. D'un point de vue logique, les deux formes de prédiction sont problématiques. La prédiction causale est logiquement problématique car elle isole souvent une cause en la désignant comme déterminante. Alors que chaque phénomène est multifactoriel et que nous pouvons donc nous tromper dans le choix de la cause déterminante : un problème qu'illustre la difficulté de prédiction en économie. La prédiction statistique est logiquement problématique car elle nous permet de faire l'économie de comprendre le pourquoi d'un phénomène et elle ne permet que de prédire la répétition, et nous rend aveugles à l'émergence de phénomènes radicalement nouveaux. Mais, dans le cadre de phénomènes récurrents, la prédiction statistique fonctionne mieux que la prédiction causale. La force de la prédiction statistique repose sur le fait que si quelque chose se passe très régulièrement d'une certaine façon, il est probable que, si les conditions sont comparables, elle se passera de nouveau de la même façon. Or, ce probabilisme n'était pas possible dans une période de relative misère numérique. L'attachement aux causes était une manière de suppléer à ce manque de données. La donnée massive permet la prédiction. Elle permet aussi autre chose : le profilage. En effet, la vie dans les sociétés modernes, même si elle nous laisse croire que nous sommes très différents les uns des autres, accentuée, par la proximité sociale, qu'elle soit physique ou virtuelle, l'homogénéisation de nos pratiques et de nos pensées. Pour mémoire ces effets de ressemblance de nos pratiques étaient auparavant l'objet d'une typologisation par la sociologie, qui reposait à la fois, bien souvent, sur des déclarations, et sur des critères en nombre limités, critères qui avaient été jugés significatifs. Désormais, la variété des informations personnelles que nous donnons, souvent involontairement, permet un profilage précis, pour les entreprises privées, de qui nous sommes, de ce que nous pensons, de comment nous vivons. Il faut noter, en revanche, que ce profilage peut entraîner l'identification, à rebours. Même si ces entreprises n'ont que faire de nous

identifier comme personnes, puisque la valeur de nos données, à leurs yeux, n'est pas notre singularité, mais notre appartenance à un groupe précis, qui est une cible, le nombre de données qu'elles manient sur notre personne peuvent permettre notre individualisation, à terme, notre identification. Pour autant si nous pouvons consentir à céder certaines de nos données personnelles en échange d'un droit d'accès à des services, nous entendons souvent conserver un droit à la vie privée, que le profilage peut rendre fragile.

□ La nouvelle « révolution scientifique »

Ce n'est plus à démontrer, les nouvelles technologies changent la manière dont on fait de la recherche, ainsi que la manière dont on enseigne. Toutefois, au sein du simple cadre du *Big Data*, l'enseignement et la recherche peuvent se trouver transformés de deux façons, au moins. D'un point de vue de la recherche, le *Big Data*, que ce soit avec les données publiques, ou les données collectées, permet de changer complètement une des manières traditionnelles de tester une hypothèse. En effet, une manière classique de procéder consiste notamment à émettre une hypothèse, établir l'étendue des moyens qu'il faudrait pour la tester, recueillir un financement pour cette étude et relever des corrélations statistiques entre faits. Ce mode de recherche présente deux difficultés. D'une part, la collecte d'informations est faite après coup, après la formulation d'une hypothèse et souvent sans étudier le lien de causalité. D'autre part, cette collecte est orientée par une hypothèse, si bien que, si cette dernière est mal formulée et que l'analyse causale est absente, l'étude peut être un échec : elle ne permettrait ni de confirmer, ni d'infirmer une hypothèse. En outre, les résultats obtenus ne sont pas nécessairement réutilisables pour d'autres études. Pourtant ce mode de recherche domine encore aujourd'hui : pour montrer quelque chose, on postule la possibilité que son existence est si importante qu'elle permet un enregistrement statistique.

En un sens, ce procédé épistémologique a préparé la voie au triomphe du *Big Data* car, bien souvent, ces études font l'économie d'une compréhension des causes d'un phénomène, au bénéfice de sa seule quantification. Or, le *Big Data* a plusieurs avantages sur ce type de recherche. Tout d'abord, le *Big Data* accumule un volume et une variété de données qui seraient impossibles à assembler sans les outils actuels de collecte. Ensuite, cette collecte n'est pas orientée : le corpus de données se constitue comme une ressource dont l'utilisation peut être décidée ensuite. Enfin, la vitesse de traitement que rend possible le *Big Data* permet des manipulations beaucoup plus aisées et régulières. Dans des domaines comme la sociologie, la médecine ou l'économie, la recherche se transforme, sous l'effet du *Big Data*. Avec une réserve : comment les chercheurs peuvent avoir accès aux données, si ces données sont publiques (mais parfois payantes) ou aux mains d'entreprises privées (donc payantes, voire inaccessibles).

D'un point de vue de la recherche, le *Big Data* peut aussi être un outil de déploiement du *crowdsourcing* : en effet, il est possible de confier l'analyse de documents sur lesquels les robots peuvent manquer de finesse, comme les cartes, les photos, ou les phrases en langues naturelles (comme le français ou l'anglais) à des foules. L'innovation radicale, en ce cas relève de l'effet réseau, qui comme pour un processus scientifique permet une innovation incrémentale, en profilant les utilisateurs et pondérant, dans la masse des réponses, les réponses de certains. Du point de vue de l'enseignement, là encore, le *Big Data* n'est pas à l'origine d'une innovation radicale, qui vient davantage de la dématérialisation et de la massification, comme dans le cas des MOOCs, mais il permet un affinement, notamment en permettant la personnalisation d'un enseignement massifié, où le profilage permet de proposer à chaque utilisateur, soit des cours plus susceptibles de l'intéresser, soit, à l'intérieur

même d'un cours, un parcours d'apprentissage plus adapté. Concrètement, que ce soit du point de vue de la recherche ou du point de vue de l'enseignement, le *Big Data* change notre manière de faire.

□ *L'absence de maîtrise et perte de la décision « politique »*

Certaines entreprises comme Google estiment que la « mise en donnée du monde » est à la source de l'efficacité des décisions politiques ou d'investissement. Cette vision totalisante du monde se traduit par le rachat par Google de toutes les startups qui peuvent permettre de développer des applications dans tous les domaines essentiels à nos sociétés.

L'enjeu sera alors celui de la dépossession ou non du politique en terme de décision : l'expertise de l'ordinateur sera-t-elle la seule source d'aide à la décision ou au contraire permettra-t-on le débat et la discussion des citoyens autour des solutions proposées par les algorithmes ? En octobre 2008, Alan Greenspan est auditionné par le Sénat américain suite à la crise des *subprimes*. L'ancien directeur de la FED reconnaît publiquement s'être trompé en expliquant que « *les prix Nobel d'économie ont affirmé devoir automatiser absolument tout et que dès lors nous avons plus de savoir économique* ». À cette époque, le terme « *Big Data* » n'existait pas encore, mais c'est bien le *Big Data* qu'Alan Greenspan remet en cause. Quand on n'a plus de savoir économique, on ne peut plus critiquer le système. On n'en voit pas les limites et cela peut conduire à une catastrophe.

L'aide à la maîtrise des technologies et des services autour du « *Big Data* » apparaît plus que jamais comme un enjeu capital pour la citoyenneté de demain. Les citoyens devront être à même de bénéficier de formations leur permettant de faciliter la compréhension par les usagers des technologies et plateformes basées sur l'analyse des données en masse. Un volet de ces formations devra être consacré à l'analyse des usages des données ainsi collectées. De plus, les concepteurs de ces plateformes devront faire connaître de manière simple à leurs utilisateurs l'étendue exacte des données collectées et les modalités d'utilisation et de restriction de l'usage de ces données.

Protection et maîtrise des données : nouveaux enjeux et nouvelles approches

Si le *Big Data* représente une opportunité formidable de progrès, et il ne s'agit pas ici de résumer ni de réduire celui-ci seulement à la publicité toujours plus ciblée, il faut confronter les implications de celui-ci à nos valeurs, à nos principes fondamentaux. La collecte et l'usage des données personnelles ne devraient pouvoir se faire sans un niveau de confiance élevé des citoyens dans ces dispositifs. Déjà en 2002, Bill Gates avait écrit un mail à tous les salariés de Microsoft sur le *Trustworthy Computing*, indiquant que le développement du numérique passerait par la confiance et la transparence.

Or, force est de constater, comme l'a illustré l'affaire Prism, et pour reprendre une formule de l'ancienne ministre à l'économie numérique, Fleur Pellerin, « *Big Data* peut devenir *Big Brother* ». La collecte exponentielle des données personnelles à travers le *Big Data* et la réutilisation quasi immédiate de ces données sont porteuses de tensions sur les libertés individuelles et le respect des droits de l'homme. Ces tensions reposent le problème de la définition de la vie privée, de l'encadrement réglementaire et du contrôle des entreprises et administrations qui utilisent ces données. À terme, le pouvoir des algorithmes pourrait

amener à ce que la machine prenne des décisions sans intervention humaine, voire à la place des autorités politiques.

Si la donnée est au cœur de la société au plan individuel, d'une collectivité, d'une Nation, présente sous différentes formes, revêtant un caractère économique, social et culturel, sa maîtrise est en revanche et sans conteste un impératif démocratique. Nous voyons bien que cette donnée est une ressource dont la maîtrise offre un pouvoir. Une situation qui peut conduire demain à parler de pillages des données, de vol de données, de blanchissement de données pour reprendre Pierre Bellanger⁸⁷. Maîtriser ses données devient rapidement une nécessité pour envisager de se mouvoir dans l'univers numérique et si possible sans risque.

La protection des données à caractère personnel : un impératif démocratique

La loi « Informatique et Libertés »

La consécration de la vie privée des individus a entraîné le développement de nombreux moyens destinés à protéger les données personnelles recueillies par les professionnels. C'est le cas de la Commission Nationale de l'Informatique et des Libertés (CNIL) autorité administrative indépendante dont nous avons vu précédemment les raisons qui ont conduit le législateur à décider de sa création.

La CNIL constitue désormais le socle de la protection des données personnelles faisant l'objet d'un traitement informatisé et a pour objectif de recenser toute création de fichier regroupant des données personnelles et d'autoriser la constitution de dossiers comportant des données dites « à risque ».

Tout « fichier clients » informatisé qu'est amené à constituer un professionnel constitue, au regard de la loi, « un fichier de données à caractère personnel », « un ensemble structuré et stable de données à caractère personnel accessible selon des critères déterminés », et se doit donc de respecter les préconisations de la CNIL. C'est ce que rappelle l'article 34 de ladite loi en précisant que « *Le responsable du traitement est tenu de prendre toutes précautions utiles, au regard de la nature des données et des risques présentés par le traitement, pour préserver la sécurité des données et, notamment, empêcher qu'elles soient déformées, endommagées, ou que des tiers non autorisés y aient accès* ».

Pour être en règle, tout archivage de données personnelles de la part d'un professionnel doit faire l'objet d'un certain nombre de démarches. En effet, pour la constitution d'un fichier clients, il est obligatoire : d'obtenir l'accord préalable de la personne qui y sera enregistrée, de mettre en œuvre des moyens de sécurisation efficaces, d'imposer une limite de temps au registre conservé et enfin de préalablement le déclarer à la CNIL.

Pour exemple, de nombreuses décisions administratives de la CNIL sont d'ailleurs venues sanctionner pécuniairement des agences privées de recherche pour non-respect des obligations prescrites par la loi de 1978.

En revanche, pour les professionnels soumis au secret professionnel, l'article 21 de cette même loi précise que l'individu qui fait l'objet d'un contrôle de la CNIL peut opposer

87 Pierre Bellanger, *Op.cit.*

le secret professionnel auquel il est soumis pour s'abstenir de fournir tout renseignement. Pour le cas des enquêteurs privés, ce principe a d'ailleurs été confirmé par une décision du Conseil constitutionnel du 29 juillet 2004, pour qui ces derniers peuvent opposer le secret professionnel au cours d'un contrôle sans que ceci ne porte en aucun cas atteinte aux pouvoirs de la CNIL.

☐ *Les trois principes fondamentaux de la loi du 17 juillet 1978*

Aujourd'hui, la CNIL est compétente sur les données à caractère personnel et sur la mise en place des fichiers informatiques, avec ou sans traitement automatisé. Ce qui entraîne la neutralité technologique ou plutôt l'insensibilité aux changements techniques qui permet à la CNIL d'appréhender toutes les mutations sociales dans leurs aspects technologiques et d'interroger le dispositif basé sur cette technologie au regard de la finalité qu'elle est censée poursuivre pour en apprécier la proportionnalité du dispositif au sens de la loi Informatique et libertés. Dans ce cas elle peut tout à fait refuser d'autoriser la mise en œuvre d'un dispositif souhaité par un responsable de traitement.

La CNIL utilise les moyens que lui confère le législateur et les sanctions qu'elle inflige peuvent être rendues publiques. La CNIL a d'ailleurs imposé à Google la publication de sa sanction sur son moteur.

La régulation telle que la CNIL la préconise, avec un principe de droit précis autour de la protection de la vie privée, est un élément fort au service des acteurs du numérique. Un élément de différenciation compétitive qui peut fortement servir à la restauration d'une confiance nécessaire dans l'usage du numérique. A la CNIL, cette gamme d'outils de régulation comporte plusieurs volets dirigés vers des publics différents : des outils de communication et d'information, des normes simplifiées et des autorisations uniques pour traiter les cas les plus fréquents de traitement et qui préfigurent la tendance lourde de l'allègement des formalités, des packs de conformité pour une application plus adaptée à des secteurs professionnels avec un travail de concertation et des documents purement techniques permettant le déploiement au niveau des systèmes d'information de la dimension *privacy*.

Les autorisations de la CNIL pour les traitements de données à « risques » ou sensibles sont soumis à autorisation. Les responsables de fichiers qui ne respectent pas ces formalités s'exposent à des sanctions pénales. Pour les traitements ou fichiers de données personnelles les plus courants et les moins dangereux, la CNIL élabore des textes-cadres auxquels les responsables de données personnelles doivent se référer pour accomplir des formalités déclaratives allégées ou en être exonérés.

À l'heure où certaines entreprises font de la gestion du risque contre la fraude par exemple un acte fort de management, les tentations de recourir à des dispositifs bien souvent en contradiction avec les principes de la loi Informatique et libertés sont grandes. Le rôle de la CNIL est alors de veiller au respect de la loi tout en travaillant en amont sur un rôle d'information et de conseil.

En ce qui concerne les traitements automatisés qui relèvent de la puissance publique, la CNIL ne peut émettre qu'un avis. Ses pouvoirs sont assez limités. Ces avis sont rendus avant ceux du Conseil d'État. Il arrive également que la CNIL ne soit pas consultée en amont de la mise en place de certains dispositifs alors même que cela devrait être le cas. On peut citer l'exemple de la loi de programmation militaire 2013.

Dans tous les cas, trois principes fondamentaux de droit structurent le raisonnement juridique de la CNIL et précisent un ensemble d'exigence légale dont le respect s'impose au responsable du traitement sous peine de sanctions pénales.

Principe de finalité

Le premier de ces principes est le principe de finalité. Ce principe posé par la loi tient à ce que les données personnelles doivent être « collectées pour des finalités déterminées, explicites et légitimes et ne sont pas traitées ultérieurement de manière incompatible avec ces finalités. La loi impose ici en réalité deux obligations : d'une part, réaliser une collecte pour des finalités déterminées, explicites et légitimes, ce qui contraint le responsable du traitement à établir de manière précise la finalité pour laquelle un traitement va être réalisé. On peut comprendre également cette règle a contrario, celle-ci sanctionnant alors des finalités vagues, ou inexistantes, inscrites lors des formalités préalables (telle que « collecte pour exploitation », « collecte pour conservation », « récupération de données pour tout usage », etc.). D'autre part, la loi impose également de ne pas détourner le traitement des finalités initiales. Une exception est toutefois prévue pour les traitements réalisés à des fins statistiques, historiques ou scientifiques à condition qu'un tel traitement soit réalisé dans le respect des autres dispositions légales et qu'il ne soit pas utilisé pour prendre des décisions à l'égard des personnes concernées (art. 6, 2°).

Principe de loyauté

La loi impose que « les données [soient] collectées et traitées de manière loyale et licite » (article 6), dictant ainsi au responsable du traitement un principe de transparence lors du traitement. Ce devoir de loyauté est exécuté entre autres à l'occasion de l'information des personnes lors de la collecte des données, autant que lors de l'exercice potentiel du droit d'opposition des personnes sur les données qui les concernent. Cette règle de droit trouve son versant pénal dans l'article 226-18 du Code pénal qui dispose que : « Le fait de collecter des données à caractère personnel par un moyen frauduleux, déloyal ou illicite est puni de cinq ans d'emprisonnement et de 300.000 € d'amende » (ou 1.500.000 euros lorsque l'auteur de l'infraction est une personne morale).

Principe de proportionnalité

Le troisième principe impose que les données soient « adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont collectées et de leurs traitements ultérieurs ». Sans doute l'une des illustrations les plus significatives de l'application de ce principe tient aux demandes de mise en œuvre de dispositifs biométriques que la CNIL a assez largement récusées en particulier lorsque ceux-ci permettaient la constitution de bases de données d'empreintes digitales, sans justification particulière.

Le droit à l'oubli : de la loi du 17 juillet 1978 à l'arrêt « Google Spain » de la CJUE

Le droit à l'oubli est une garantie fondamentale des libertés, ainsi qu'une nécessité humaine et sociétale. Sous l'angle « Informatique et Libertés », le droit à l'oubli se matérialise aujourd'hui en France dans des concepts juridiques issus de la directive 95/46/CE du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, de la convention 108 du 28 janvier 1981 et de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, modifiée en 2004. Il s'agit, notamment, au-delà des principes de finalité, de

loyauté, d'exactitude et de mise à jour des données, de l'obligation de définir et de respecter des durées de conservation et de prise en compte des demandes de droit d'opposition.

La loi Informatique et Libertés impose en effet un principe de durée ou plus exactement de conservation des données. Ce principe impose que les données soient conservées pendant une durée limitée, au-delà de laquelle les données à caractère personnelles doivent être effacées. L'article 6 de la loi du 6 janvier 1978 précise à ce titre que les données "sont conservées sous une forme permettant l'identification des personnes concernées pendant une durée qui n'excède pas la durée nécessaire aux finalités pour lesquelles elles sont collectées et traitées." En pratique cette durée est fixée par le responsable du traitement qui doit procéder à une estimation au regard des finalités indiquées. Avec le droit d'information, de modification et d'opposition prévu par la loi 78⁸⁸, cet élément de durée constitue le fondement du « droit à l'oubli ». Toute personne a le droit de savoir si elle est fichée et dans quels fichiers elle est recensée. Ce droit de regard sur ses propres données personnelles vise aussi bien la collecte des informations que leur utilisation. Ce droit d'être informé est essentiel car il conditionne l'exercice des autres droits tels que le droit d'accès – « toute personne a le droit d'interroger le responsable d'un fichier pour savoir s'il détient des informations sur elle »⁸⁹ - ou le droit d'opposition – « toute personne a la possibilité de s'opposer, pour des motifs légitimes, à figurer dans un fichier »⁹⁰.

Très récemment deux arrêts de la CJUE sont venus compléter au plan européen le droit à l'oubli. L'arrêt du 8 avril 2014⁹¹ qui a invalidé la directive sur la rétention des données de connexion (directive 2006/24/CE), communément dite « data retention »⁹², et l'arrêt du 13 mai 2014, arrêt dit « Google Spain ». Avec ce dernier arrêt, la Cour reconnaît à toute personne un droit à ce qu'une information relative à sa personne ne soit plus liée à son nom par une liste de résultats affichés lors d'une recherche effectuée à partir de son identité. Il convient de souligner que, contrairement à ce qui a été régulièrement dit de manière erronée, le déréférencement ne constitue pas une suppression de l'information source, mais la seule décorrélation entre le nom de la personne et la liste de résultats correspondant à ce nom dans les résultats des moteurs de recherche. Bien que ce droit « au déréférencement » ou « à l'effacement » (et non « droit à l'oubli », contrairement à ce qui est souvent indiqué) consacre le principe nouveau selon lequel le droit individuel à la suppression de liens prévaut, en règle générale, non seulement sur l'intérêt économique de l'exploitant du moteur de recherche, en revanche, ce principe n'est pas absolu. Il convient en effet de veiller à ce que le droit à la protection des données ne prime pas de manière systématique sur d'autres libertés fondamentales, au premier chef la liberté d'expression.

Or si la décision de la Cour affirme à juste titre la nécessité d'une garantie étendue du droit à la protection des données personnelles, elle n'approfondit guère le point crucial de la mise en balance de la protection des données personnelles avec celle de la liberté d'expression et d'information en confiant aux moteurs de recherche la gestion de l'équilibre

88 Il s'agit du droit, reconnu à toute personne, de demander au détenteur d'un fichier de lui communiquer toutes les informations la concernant. Ce droit permet de vérifier l'exactitude de ces informations et, le cas échéant, de faire rectifier celles qui sont erronées.

89 Source : www.cnil.fr

90 Op.cit

91 Arrêt Digital Rights Ireland Ltd (C-293/12) et Kärntner Landesregierung (C-594/12)

92 Directive 2006/24/CE du Parlement européen et du Conseil du 15 mars 2006, sur la conservation de données générées ou traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public ou de réseaux publics de communications, et modifiant la directive 2002/58/CE

des droits en cause, alors mêmes qu'ils n'ont ni la compétence, ni la légitimité de se substituer à un juge, ce qui remet en cause les principes les plus fondamentaux de l'État de droit.

Les différents textes et accords-cadres : de la Convention 108 à la Directive 1995

De nombreux textes existent au plan international et tout particulièrement au plan européen. Des textes qui placent le droit à la protection des données personnelles comme un droit fondamental et inaliénable de chaque individu ; le modèle européen de protections des données issu de la directive de 1995 et de la convention 108 du Conseil de l'Europe en sont un exemple. D'autres textes contribuent également à définir un cadre protecteur en la matière. Dans l'une de ses publications sur l'enjeu de la protection des données personnelles présenté lors de l'organisation de leur colloque au sein de notre assemblée, le Forum d'Avignon a réalisé une présentation et une analyse objective de ces différents textes que nous reprenons ici :

- **« La Convention européenne des droits de l'Homme et des libertés fondamentales (CEDH) du 4 novembre 1950, en particulier, l'article 8.1 de la CEDH qui prévoit que « toute personne a droit au respect de sa vie privée et familiale, de son domicile et de sa correspondance ».**
- **Le Pacte international de l'Organisation des Nations unies (ONU) relatif aux droits civils et politiques du 16 décembre 1966, en particulier son article 17.1 prévoyant notamment que « nul ne sera l'objet d'immixtions arbitraires ou illégales dans sa vie privée, sa famille, son domicile ou sa correspondance, ni d'atteintes illégales à son honneur et à sa réputation ».**
- **les lignes directrices régissant la protection de la vie privée et les flux transfrontières de données à caractère personnel de l'Organisation de coopération et de développement économiques (OCDE) du 23 septembre 1980.** L'OCDE, créée en 1961, a notamment pour objectif d'apporter son aide en favorisant l'échange de compétences et le partage d'expertises entre ses membres ou entre les pays membres et les autres pays. En adoptant ces lignes directrices, l'objectif de l'OCDE était de disposer de principes communs permettant ainsi de contribuer à l'harmonisation des législations nationales en matière de protection des données. Ces principes sont principalement les suivants : principes de la limitation de la collecte et de l'utilisation des données, principe de la qualité des données (pertinence des données, etc.), principe de la spécification des finalités de la collecte, principe des garanties de sécurité des données, principe de transparence (information des personnes concernées), principe de la participation individuelle (possibilité pour un individu d'obtenir la confirmation d'une utilisation de données le concernant) et principe de responsabilité du responsable de traitement (cf. infra, les principes prévus par la réglementation française applicable en la matière). Les principes de l'OCDE n'ont toutefois aucun caractère contraignant.
- **la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (Convention 108) du Conseil de l'Europe ouverte à la signature le 28 janvier 1981. Cette Convention constitue le premier instrument international juridique contraignant en matière de protection des données à caractère personnel.** Les États signataires ont l'obligation de prendre les mesures nécessaires et appropriées, dans leur législation nationale,

afin d'en appliquer les principes (à savoir notamment le principe de collecte licite et loyale, le principe de conservation limitée des données, le principe de qualité et de proportionnalité des données, le principe d'information des personnes concernées, le respect des droits d'accès et de rectification, etc.).

- **les accords de l'APEC (Asia Pacific Economic Cooperation)** : la zone APEC créée en 1989 regroupe les pays suivants : Australie, Brunei, Canada, Corée du Sud, Chili, États-Unis, Indonésie, Japon, Malaisie, Mexique, Nouvelle-Zélande, Philippines, Singapour, Thaïlande, Chine, Hong Kong, Taïpei, Papouasie-Nouvelle-Guinée, Pérou, Russie et Viêt Nam). L'APEC a notamment pour objectif de renforcer la coopération économique de la zone Asie-Pacifique. Fin 2004, l'APEC a adopté des principes directeurs en matière de protection de la vie privée et des données à caractère personnel (APEC Privacy Framework) qui sont en accord avec les lignes directrices de l'OCDE du 23 septembre 1980. Ces principes n'ont aucun caractère contraignant. Ils appréhendent la question des transferts de données hors des frontières et encouragent notamment les pays membres de l'APEC à adopter une approche commune. Un dispositif visant à encadrer ces flux transfrontaliers entre les membres de l'APEC a été finalisé fin 2011 (à savoir les Cross Border Privacy Rules - CBRP). Les organismes souhaitant mettre en place ces CBRP pourront réaliser, sur la base d'un questionnaire revu par un organisme certificateur (APEC-recognized Accountability Agent), une auto-évaluation en matière de protection des données à caractère personnel et pourront ainsi obtenir une certification. Pour plus de détails voir notamment le document intitulé « CRPB Policies, Rules and Guidelines » disponible sur le site de l'APEC – www.apec.org.
- **les principes directeurs des Nations unies** pour la réglementation des fichiers informatisés contenant des données à caractère personnel adoptés le 14 décembre 1990 par l'Assemblée générale des Nations Unies dans sa résolution 45/95. Ces principes n'ont pas non plus de valeur contraignante et les lignes introductives précisent que leurs modalités d'applications « sont laissées à la libre initiative de chaque État ».
- **la directive n° 95/46/CE du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données** constitue le texte de référence, pour le droit communautaire, en matière de protection des données à caractère personnel.
- **la Charte des droits fondamentaux de l'Union européenne en date du 7 décembre 2000** (cf., en particulier, l'article 8 de son titre II) a également consacré expressément le droit à la protection des données. En effet, l'article 8 de la charte précitée prévoit que « toute personne a droit à la protection des données à caractère personnel la concernant ». La charte ajoute notamment que le traitement de ces données doit être réalisé loyalement et sur la base du consentement de la personne concernée ou en vertu d'un autre fondement légitime prévu par la loi. La charte prévoit également la nécessité de mettre en place des autorités de contrôle indépendantes afin d'assurer le respect des règles édictées en la matière. Cette charte, qui n'avait initialement qu'une valeur d'accord interinstitutionnel liant le Parlement, le Conseil et la Commission européenne, s'est vue reconnaître la valeur de traité par son intégration au traité de Lisbonne (traité modifiant le traité sur l'Union européenne et le traité instituant la Communauté européenne) signé le 13 décembre 2007.
- **le Conseil de l'Europe a adopté le 16 avril 2014** une recommandation sur un guide des droits de l'Homme pour les utilisateurs d'Internet ».

Le projet de règlement européen

L'évolution des techniques numériques et les opportunités immenses qu'offre le *Big Data* conduisent à réadapter les cadres réglementaires en matière de protections des données personnelles et des libertés dans le monde numérique. Il s'agit de revenir à des fondamentaux et repenser complètement ce qui se reconstruit sur ces fondamentaux. Un certain nombre de faits conçus dans le domaine matériel volent en éclats dans le domaine d'Internet (on rentre dans les maisons par Internet même si la porte est physiquement fermée). D'où l'exigence d'un nouveau cadre juridique au moins européen en réponse à l'intensification de la collecte des données et de la prise de conscience par l'opinion publique des usages qui peuvent être abusifs de ces données collectées.

Le projet de règlement des données personnelles est une première réponse d'homogénéisation du cadre réglementaire entre tous les États membres et tous les acteurs de la chaîne numérique et pas seulement les opérateurs téléphoniques. La proposition vise à réformer la législation européenne datant de 1995 en harmonisant les règles européennes et en renforçant le rôle des autorités nationales de protection des données.

L'engagement français face à la réforme à venir de la législation européenne sur la protection des données personnelles (CEPD) est indispensable. Le CESE souhaite que les pouvoirs publics français dans leur ensemble se mobilisent fortement par rapport à cette question. Ce texte présente des avancées considérables. Son avantage majeur est de soumettre au droit européen tout traitement de données concernant un résident européen par une entreprise non établie en Europe.

Mais il pose en revanche le problème de la notion d'« établissement principal », selon lequel l'autorité de régulation compétente en cas de différend avec un citoyen européen est celle du lieu où se trouve l'entreprise et non celle du plaignant. Concrètement, si une entreprise est localisée au Luxembourg ou à Malte, en cas de plainte d'un citoyen français, cette plainte sera exclusivement instruite par la CNIL luxembourgeoise ou maltaise.

Or, ce dispositif ne peut marcher, car dans une part très importante des cas, les autorités nationales ne seraient plus compétentes par rapport à leurs propres ressortissants.

La protection des données personnelles : entre régulation et autorégulation

Un certain nombre d'actions en faveur d'une protection et d'une maîtrise des données numériques est possible en partant du principe selon lequel l'innovation s'enrichit du respect des principes éthiques de transparence et de confiance. Opposer l'un à l'autre comme le font certains est un non-sens ou plutôt l'expression d'un cynisme dangereux. Autrement dit, la *privacy* et l'innovation ne sont pas antagonistes. L'*open innovation* n'est pas seulement d'ordre technologique mais est également une ouverture aux attentes, aux aspirations de la société. Le principe d'innovation responsable doit inclure cette dimension éthique comme un moteur de nouveaux usages et de nouveaux outils.

Par rapport à cette préoccupation éthique, le dialogue peut être fructueux entre les entreprises et les régulateurs pris au sens large. Toutefois il n'appartient pas aux entreprises de se substituer à la décision du politique. C'est la raison pour laquelle l'autorégulation ne doit pas se substituer à la régulation. L'autorégulation doit être un étage supplémentaire,

qui s'ajoute et peut apporter une différenciation, le cas échéant un usage, qui protège les valeurs encore mieux que ce que le législateur a fixé comme principe. Autrement dit, elle peut faire vivre concrètement les principes qui ne peuvent pas aller dans les détails ni être amendé à la vitesse de l'innovation dans le numérique. Il faut trouver la juste articulation entre les principes durables et la corégulation les faisant vivre au fil du temps et des évolutions et nouveaux usages. En voici trois illustrations.

L'autorisation de la Cnil est l'exemple d'une régulation par le respect des prescriptions réglementaires. L'introduction de clauses contractuelles types encouragée par la Commission européenne est du ressort de la co-régulation. Enfin l'exemple du « *Do Not Track By Default* » des navigateurs de recherche introduisant par défaut des fonctionnalités destinées à mieux protéger les utilisateurs d'internet contre le suivi abusif de leur navigation sur le web illustre l'exemple type de l'autorégulation.

Complémentarités de la loi et de la technologie

□ *L'exemple du privacy by design*

La protection des données et le *Big Data* sont intrinsèquement incompatibles. Pour fonctionner, un dispositif s'appuyant sur le *Big Data* requiert d'absorber rapidement, continuellement, des données variées, et en grande quantité. À l'inverse, la loi protège, que ce soit préalablement, ou en post-régulant quand un problème apparaît, les données personnelles. Le paradoxe demeure : pour améliorer leur vie personnelle, les individus ont recours à des services qui, tout en leur offrant des bénéfices souvent réels, peuvent se retourner contre eux, soit par leurs effets propres (par exemple, quand Facebook, changeant ses règles de *privacy*, rend publiques des informations que les individus auraient voulu réserver à un cercle restreint) soit par leurs effets cumulés (par exemple, quand un croisement de vos comptes Facebook, Four Square et Trip Advisor révèle que vous êtes en congé et non en arrêt maladie). Cela étant, le législateur structure les conditions de fonctionnement des outils technologiques, et la collecte et le traitement des données sont encadrés. En ce sens, loi et technologie sont doublement complémentaires : la technologie s'insère dans le cadre décrit par la loi et la loi se modifie selon les problèmes que la technologie suscite. Toutefois, la difficulté propre au *Big Data*, une fois écartés les cas d'irrespect, par les acteurs, du cadre légal et réglementaire, est que les usagers peuvent eux-mêmes provoquer des infractions à leur vie privée.

Il s'agit là d'un passage obligé de protection de la vie privée. La loi doit interdire certaines pratiques et affirmer la primauté de l'individu en matière de gestion des données personnelles. C'est ce qu'établit la loi Informatique et libertés de 1978 mais aussi la Charte européenne des droits fondamentaux.

En revanche, la loi ne peut pas gérer la protection et l'édition de données par la personne elle-même. Cette possibilité de divulgation mais aussi de protection passe par des applications techniques au sein des logiciels dits *privacy by design* permettant de gérer l'utilisation de données personnelles, mais aussi la possibilité de ne pas être traqué par des enseignes commerciales avec, par exemple, l'ajout par Microsoft à son Internet Explorer du *do not track by default*, ce que l'on appelle le *privacy by default*. On peut également citer la limitation de conservation à six mois des données de connexion d'une adresse IP comme une bonne pratique.

Cette complémentarité entre la loi et la technologie permet de retrouver la confiance mise à mal par certains opérateurs du Net, mais elle est encore peu pratiquée et exige une prise de conscience des GAFAs sur ce sujet.

□ *Le enjeu de l'anonymisation : l'exemple de l'Open Data*

L'*Open Data* permet le développement d'un aspect collaboratif qui est source de démocratie. L'idéal est le contrôle en amont de la mise en ligne, c'est le rôle notamment du Comité du secret statistique qui définit des règles strictes. Le Comité du secret statistique a été créé en 1984 à la suite de la loi du 7 juin 1951 qui interdisait toute atteinte à la vie privée pour les ménages et pour les entreprises et imposait la non-utilisation de leurs réponses à des enquêtes pouvant permettre une atteinte au secret commercial, une utilisation à des fins fiscales ou de répression économique. Peu à peu, l'INSEE a mis à disposition des chercheurs des fichiers anonymisés pour les ménages, mais pour les entreprises il a fallu ouvrir certaines possibilités de traitement.

C'est en 1984 que l'on crée le Comité du secret statistique concernant les entreprises. Il est placé auprès du Conseil national de l'information statistique (CNIS). Il est présidé par un membre du Conseil d'État et composé de membres de l'administration, des entreprises, un représentant des organisations syndicales des salariés et un des utilisateurs régionaux des statistiques.

En 2004, l'action du Comité est étendue aux ménages, aux personnes morales de droit public. Le Comité donne donc des avis sur la transmission des données publiques sensibles, sous certaines conditions, notamment en matière d'utilisation et d'objectif poursuivi. En 2008, la loi sur les archives a permis d'ouvrir des données personnelles privées après 75 ans au lieu de 100 ans et après 25 ans pour les documents d'ordre économique et financier. Cela a obligé le Comité à se scinder en deux sections : l'une sur les données personnelles avec une composition revue avec l'arrivée de membres du Parlement et du CESE, de représentants des Archives de France, de la CNIL, de l'UNAF et de l'INED ; en parallèle la section entreprise s'est ouverte au MEDEF, à la CGPME, la FNSEA, l'UPA, les CCI et les chambres de métiers, ainsi que les collectivités territoriales.

L'enjeu démocratique de l'*Open Data* pour rendre compte des actions publiques est extrêmement important vis-à-vis des collectivités territoriales, l'action des parlementaires et du gouvernement. Un *Open Data* sécurisé, gratuit, anonymisé mais ouvert et permettant des comparaisons, est source d'une démocratie renouvelée. Il convient toutefois que tous les citoyens puissent se saisir de tels outils.

La maîtrise des données personnelles : entre confiance et réciprocité

Les données personnelles sont défendues par principe. La loi les défend, les bonnes pratiques sont encouragées et diffusées pour que les entreprises les défendent, et les usagers sont encouragés à défendre eux-mêmes, dans leurs pratiques, leurs données. Toutefois, ce que change le *Big Data*, c'est qu'il accompagne et amplifie la collecte et le traitement des données personnelles, avec deux conséquences. Tout d'abord, les erreurs, manquements, infractions, tout en demeurant à la marge, deviennent de plus en plus nombreux. Ensuite, et c'est là la vraie nouveauté, un usager peut avoir, auprès des solutions en ligne qu'il emploie, une bonne maîtrise de ses données, mais la dispersion de ses données sur un très grand nombre de plateformes rend possible sa ré-identification et donc, en cela, une

perte de contrôle sur ce que de nombreux internautes perçoivent comme une nécessité : la dissociation entre l'identité réelle et l'identité virtuelle, qui demeure toujours incomplète. En ce sens, il y a donc bien un problème nouveau posé par le *Big Data* et une nécessité de voir comment le résoudre, que ce soit par la régulation, l'autorégulation, ou l'éducation.

□ *Restaurer la confiance et le partage*

Le *Big Data* est comme nous venons de voir constitué de données qui sont de plus en plus coproduites par les personnes et les acteurs du numérique. La multiplication des objets connectés participera d'une inflation de cette masse de données ; même si ces dernières ne seront pas nécessairement des données à caractère personnel, les risques de surveillance et d'authentification seront élevés. Face à cela, les mesures réglementaires que nous venons d'entrevoir sont une réponse indispensable. Il n'y a pas de liberté sans État de droit. Or, force est de constater que le « temps long » associé à la loi rend souvent caduque ses effets de protection face à des technologies dont les caractéristiques et les finalités évoluent rapidement.

Pour autant, l'abandon de la démarche de régulation au profit de mesures de laisser faire est inenvisageable. Elle conforterait la logique de prédation des données par des plateformes avides de les commercialiser aux détours de méthodes pas toujours conformes avec les principes élémentaires de la loi Informatique et libertés.

Complémentaires aux dispositions réglementaires, les approches dite relationnistes sont en mesure de restaurer la confiance nécessaire à l'usage éthique du numérique sans abandonner la dimension coercitive quand celle-ci s'impose. L'éducation au numérique comme enjeu de citoyenneté doit participer à cette restauration nécessaire de la confiance, qui passe certes par une meilleure protection des données personnelles, mais pas seulement. L'enjeu, c'est de redonner aux personnes du pouvoir sur leurs données, en leur permettant de les récupérer, d'en produire de nouvelles, de les partager et ce dans un cadre qui soit protecteur et qui ait du sens.

□ *La propriété des données, une fausse bonne idée*

L'éducation au numérique appelle une démarche de réappropriation des enjeux et des mécanismes de fonctionnement de ces plateformes. Mais la réappropriation de leviers propres à une maîtrise de la gestion des données et notamment des données personnelles ne doit pas s'entendre comme le glissement vers un régime de propriété où les données personnelles seraient d'une certaine façon considérées comme une œuvre de l'esprit bénéficiant d'un droit de propriété intellectuelle ou comme une marchandise négociable et cessible. Une telle approche couplée dans tous les cas à la monétisation des données personnelles prendrait le contrepied de la conception française et européenne de la vie privée qui place sa protection sur le terrain des droits et libertés fondamentaux.

Aller sur ce terrain, c'est inévitablement « [renvoyer] sur l'individu la responsabilité de gérer et de protéger ses données, au lieu de trouver des réponses collectives à un problème de société [et] participe d'une vision qui renforce l'individualisme et nie les rapports de force entre les consommateurs et les entreprises »⁹³. C'est s'inscrire très en rupture avec la culture humaniste française où la donnée n'est pas un élément patrimonial mais un élément de droit fondamental. Plus encore, le risque est d'apporter moins de garanties que le système actuel : aujourd'hui, même si les données sont traitées par des tiers (Google, Facebook, États...), les droits sur les données des personnes, droit à l'oubli, droit de rectification et

93 Valérie Peugeot - *Données personnelles : sortir des injonctions contradictoires*, Vecam. 13/04/2014.

de suppression, demeurent. Dans le cas où ces dernières deviennent propriétaires de leurs données et qu'une cession de celles-ci est conclue, la personne n'est alors plus détentrice d'aucun droit sur les données et par extension sur une partie d'elle-même.

Le pari de l'innovation et de la protection est un pari gagnant. Les deux termes de cette équation ne sont pas incompatibles. Mais cela suppose en plus du cadre réglementaire de s'orienter plus généralement vers une régulation du marché des données en passant notamment par une exigence de transparence sur l'utilisation qui est faite des données d'un utilisateur d'une plateforme ou d'un service. L'idée est alors de rompre « le déséquilibre qui devient intenable entre, d'un côté des organisations surinformées notamment à propos de leurs clients, suréquipées en outils décisionnels, surprotégées et, de l'autre, des individus dotés de leur seul navigateur web »⁹⁴.

□ Les CGU

La gratuité apparente des services en ligne qui sont autant de collecteurs de données personnelles susceptibles de nourrir le *Big Data* est une source majeure des problèmes que les individus peuvent rencontrer. Toutefois, sous l'apparence de la gratuité, cette relation reste une relation marchande et l'affirmation de ce fait explique une des évolutions sur l'encadrement des pratiques de collecte et de traitement, qui s'inspire de plus en plus du droit de la consommation, et notamment de l'idée de la nécessité du consentement libre et éclairé du consommateur, qui se manifeste désormais par un double *opt-in* (accord explicitement demandé et explicitement donné), ou par l'affichage que le site que l'internaute consulte collecte des informations sur sa navigation.

Devant l'étendue du problème que le *Big Data* peut contribuer à amplifier, une solution envisageable, parallèlement à la régulation, l'autorégulation ou l'éducation, est d'adopter des outils, ou applications, ou dispositifs qui auraient pour mission explicite de redonner aux internautes la maîtrise de leurs données personnelles ou, à défaut, n'auraient pas besoin de nos données personnelles pour fonctionner. Le dispositif le plus connu est ce contrat d'échange de consentements explicites et éclairés qu'incarnent les conditions générales d'utilisation (CGU). Mais ces CGU présentent trois types de difficultés. Tout d'abord, si un outil s'impose, alors il peut y avoir une forte pression à l'usage, même si l'internaute réprovoque les CGU dudit outil. Ensuite, ces CGU sont notoirement longues et rarement lues : ce qui explique des tentatives pour imposer un simple code visuel qui signale clairement ce que fait l'entreprise des données personnelles, si elles sont revendues ou non. Enfin, les CGU changent parfois : ainsi, Twitter a changé en 2009 ses règles de confidentialité pour revendre en 2013 deux ans de tweets à des sociétés de *data-mining*. Ainsi, même si des bonnes pratiques peuvent être encouragées du côté des CGU, ce ne peut être une solution.

□ Tiers de confiance

Les enjeux éthiques du numérique se posent à travers le respect de la vie privée et la liberté individuelle qui semblent mis constamment en question. Ces enjeux qui concernent la protection des données personnelles, le droit à l'oubli, le droit à la déconnexion, la fracture numérique ou encore la surveillance électronique, peuvent au fond se résumer en un enjeu générique, majeur, celui de la confiance dans la société.

L'intérêt de respecter des règles éthiques, et de faire preuve de transparence vis-à-vis des politiques d'exploitation des données personnelles, est de conserver du mieux possible la confiance de ses clients/consommateurs. À titre d'exemple, Orange a publié en février

94 Marine Albarède, René Francou, Daniel Kaplan. *Mes Infos : cahier d'exploration*. FING. Mars 2013.

les résultats d'une nouvelle étude, « *Future of Digital Trust* », sur les préoccupations des consommateurs à l'égard du traitement de leurs données personnelles par les entreprises. Cette étude met en évidence le manque de confiance des consommateurs : 78 % d'entre eux estiment qu'il est difficile de faire confiance aux entreprises en ce qui concerne l'exploitation de leurs données personnelles. La même proportion de consommateurs estime que les fournisseurs de services détiennent trop d'informations sur leurs habitudes et leurs préférences. 70 % pensent qu'il y a peu ou pas de possibilités de savoir comment ces données personnelles sont utilisées.

Parallèlement, 82 % considèrent qu'ils ont peu de moyens de contrôler la façon dont leurs données personnelles sont utilisées par les entreprises et les institutions. D'après cette étude, le traitement des données personnelles constitue un élément essentiel à la préservation de la confiance que va accorder un consommateur à une entreprise ou une institution, pratiquement au même titre que la qualité des services.

En raison du constat d'une incompréhension du droit et des exigences réglementaires en matière de protection des libertés numériques, beaucoup de projets sont en marge de la loi et mériteraient une étude de conformité plus approfondie. Dans ce domaine, la CNIL adopte une doctrine qui tient compte également des échanges qu'elle opère avec les acteurs de l'économie numérique et de la société civile. D'autres approches doivent nécessairement être discutées, pour accompagner le développement de modèles économique et sociaux associant des dispositifs de traçabilité et de prestations de services. Parmi ces pistes de réflexion concernant les évolutions normatives possibles susceptibles de permettre de redonner confiance dans la collecte et la gestion des données dans un contexte législatif évolutif, le concept d'autorégulation (*accountability*) comme celui de la prise de pouvoir par l'utilisateur (*empowerment*) ou sa participation spontanée à la production de données (*crowdsourcing*) apportent des réponses susceptibles de confirmer le couple protection/innovation. Ce qui suppose plus largement l'existence d'un projet politique à même de replacer la confiance au cœur des débats et des échanges démocratiques.

Afin de répondre à la problématique de l'interconnexion des nombreuses données que nous avons à gérer au quotidien, ou que des équipes de recherche peuvent avoir besoin de traiter, il pourrait être envisagé que les acteurs d'un même projet, publics et privés, désignent, parmi eux ou par l'intermédiaire d'un « tiers de confiance », dans le cadre d'une démarche d'autorégulation, une entité chargée de centraliser l'ensemble des informations nominatives issues des divers fichiers destinés à être intégrés à l'application, cette personne étant ainsi la seule à maîtriser et gérer les fichiers interconnectés. On réduirait ainsi le risque de dissémination de telles informations connectées et l'on faciliterait alors le rapprochement entre acteurs publics et privés. Ce tiers de confiance serait alors soumis à des obligations de sécurité et de conformité renforcées, qu'il pourrait définir lui-même sous le contrôle de la CNIL. Agissant comme un « coffre-fort de données », c'est également ce tiers de confiance qui déciderait, au cas par cas, de libérer certaines informations nominatives au bénéfice des partenaires pour des besoins spécifiques, en prenant le soin de cloisonner certains fichiers, anonymiser certaines données, exiger certaines conditions d'utilisation spécifiques en fonction des besoins rencontrés. Ces transferts de données, réalisés sous la forme contractuelle, pourraient être soumis à des « *binding corporate rules* » (BCR, règles internes d'entreprise), déjà connues par ailleurs pour les échanges intragroupes ou en dehors de l'Union européenne, sorte de contrats types dont la formulation a été soumise préalablement à l'approbation de la CNIL.

Préconisations

La révolution du numérique a ouvert de gigantesques chantiers et opportunités dans notre vie quotidienne et domestique mais également dans des domaines d'activités variés (téléchirurgie, gestion intelligente de la ville, objets connectés, géolocalisation pour détecter les accidents...). Or les conséquences des révélations d'Edward Snowden sur la gestion des données numériques ont profondément altéré la confiance que la société civile pouvait avoir dans l'usage et les finalités de cette technologie.

La restauration de la confiance est donc nécessaire mais ce travail requiert face à la complexification des technologies, de rendre aux individus la maîtrise de cet environnement numérique, tant sur le volet de la protection de leurs données que sur le volet de l'exploitation éthique des ressources numériques.

S'il s'avère nécessaire de diffuser plus largement cette culture de la sécurité renforcée des échanges, de nouvelles générations d'outils plus transparents et plus ergonomiques devront être développées pour être en mesure de donner aux citoyens un véritable contrôle démocratique sur les architectures numériques qui détermineront leurs modes de vie et d'échange. Là encore, la sensibilisation et l'éducation des usagers mais aussi la compréhension de ces sujets par les responsables politiques conditionneront pour une grande part les formes que prendront nos sociétés.

Construire une stratégie d'ensemble pour une véritable culture numérique et une protection des données efficace.

Le développement du numérique ne peut se faire au détriment du respect des personnes et de la dignité humaine. Pour cela il faut pouvoir concilier impérativement l'innovation et la protection. Il doit également s'inscrire dans la transition écologique. L'univers numérique ne doit pas être un univers sans droit. Pour construire cet édifice, l'éducation au numérique est la meilleure arme. Une arme au service de l'intelligence collective et de l'émancipation. Pour préparer l'ensemble de la société à la révolution numérique, les efforts doivent d'abord porter sur l'éducation par une diffusion de la culture numérique vers les entreprises et sur l'édification d'un cadre de protection des données.

Promouvoir l'éducation au numérique

A l'ère du numérique où la complexité et la puissance des technologies de l'information et de la communication ne cessent de s'accroître, l'exigence de protection des libertés et de la vie privée doit s'accompagner d'une communication accrue en direction des citoyens, destinée à mieux les informer de leurs droits et de leurs obligations, et à mieux identifier les risques auxquels ils s'exposent. Une exigence citoyenne qui doit accompagner également la découverte des potentialités créatives offertes par cette révolution numérique. La question du numérique nous concerne tous : elle ne peut être réservée aux seuls initiés. Plus les personnes seront informées, formées et sensibilisées aux enjeux du numérique et de protection des données personnelles, plus elles seront exigeantes à l'égard de leurs représentants politiques.

Accompagner et soutenir le rôle éducatif de la famille dans la transition numérique

Sensibiliser les enfants dès leur plus jeune âge au numérique revêt donc un caractère primordial. Il est en effet impératif que nous apprenions à nos enfants non seulement à se repérer, à s'orienter dans ces nouveaux environnements, mais également à en tirer profit, pour leurs loisirs ou leur scolarité et ce en toute sécurité. La famille est un lieu privilégié d'apprentissage où les enfants adoptent de manière durable les pratiques observées chez leurs parents. Or, les parents d'aujourd'hui appartiennent à la première génération véritablement touchée par les importantes évolutions des modes de communication et d'information. Toutes les familles n'ont pas les mêmes possibilités dans le domaine numérique. Certaines n'ont par conséquent que très peu de références en termes d'usage numérique tant dans le domaine pédagogique que dans les domaines aussi variés que sont les nouvelles formes de communication et de correspondance. C'est sans compter que ces nouvelles pratiques d'éveil à l'espace numérique restent onéreuses et peuvent se trouver contrariées par les situations de chômage et de précarité et renforcer la fracture numérique. Pour autant ce travail de sensibilisation et de découverte d'un univers en perpétuelle mutation, doit se poursuivre tout au long de la vie.

Si l'information du public sur l'ensemble des pratiques de conservation des données sur Internet est indispensable pour améliorer la confiance dans le numérique, les approches par la mise en garde des dangers d'internet en tant que tel sont contre-productives. Pour une meilleure efficacité, elles doivent, tout en montrant le profit que l'on peut tirer de l'utilisation d'internet, porter sur les dangers d'une utilisation incomprise et irresponsable du réseau, en soulignant notamment les risques liés à la captation induite des données et sur les actions de sensibilisations aux données de chiffrement et aux outils de sécurisation de l'anonymat sur Internet.

Promouvoir des campagnes publiques de sensibilisation à la protection des données personnelles

Il faut aider les parents dans l'accompagnement de leurs enfants, pour amener ces derniers à être plus autonomes et plus responsables dans la gestion de leurs réseaux sociaux et de la confidentialité de leur vie privée. **A cet effet, le CESE préconise le développement de campagnes publiques de sensibilisation à la protection des données personnelles avec le concours de la CNIL et l'ensemble des associations concernées, notamment de parents d'élèves, familiales et péri éducatives.**

À destination du grand public, et en tout premier lieu des jeunes, ces campagnes doivent aider à faire comprendre les risques inhérents à la diffusion incontrôlée sur Internet de données personnelles, et à mieux faire connaître les règles de protection des données pour permettre de protéger plus efficacement sa vie privée.

Dans cette perspective **le CESE recommande de faire de l'éducation au numérique la grande cause nationale de 2016** et de soutenir sur ce point le collectif EducNum pour mettre en œuvre des actions de sensibilisation autour des potentialités, des connaissances et des compétences numériques et une labellisation des sites répondant aux critères de protection des données.

Cette ambition citoyenne doit s'accompagner également de la mise en place de tutoriels pour apprendre à se mouvoir en toute sécurité sur les réseaux ou pour protéger les données émises par les smartphones. **Le CESE propose la création d'une plateforme collaborative sous l'égide de la CNIL** pour mettre en commun ce type de ressources et de compétences serait un support idéal pour une meilleure appropriation par les enfants et leurs parents. Compte tenu de la réalité des nouvelles fractures numériques qui excluent un nombre encore trop important de familles de l'accès au numérique, la mise en œuvre des formes plus classiques de sensibilisation (lieux d'information comme les points d'accès au droit, les livrets et guides pratiques, etc..) devra être envisagée.

Le CESE souligne également les actions de la CNIL en faveur d'un site dédié à l'usage des écrans par les jeunes, la mise en œuvre d'une application smartphone pour les 6-14 ans leur permettant de découvrir les règles de protection et l'édition de plaquettes en direction des jeunes publics.

Convaincu du rôle essentiel du cadre familial pour l'éducation numérique, **le CESE soutient la mise en œuvre d'actions visant à sensibiliser les parents à l'importance à accorder, dans l'intérêt de leurs enfants, et particulièrement les plus jeunes d'entre eux, à la pratique du numérique.** Pour autant, en raison d'effets sanitaires suspectés, le CESE rappelle que l'ANSES recommande d'appliquer le principe de précaution à l'égard des plus jeunes, particulièrement des moins de 16 ans, et de réduire l'exposition des enfants en incitant à un usage modéré du téléphone mobile. Ces actions de sensibilisation et de formation ne doivent pas se développer sans un travail parallèle pour promouvoir l'usage créatif de l'ensemble des outils numériques et sans un effort particulier en faveur des milieux les plus défavorisés et des zones concernées par la fracture numérique. Les actions doivent associer dans leurs formations les parents et les enfants.

Renforcer la protection des mineurs

La présence quasi-permanente des terminaux mobiles dans l'environnement familial présente de nouveaux risques pour les enfants d'accéder à des contenus inappropriés. De plus, les fonctionnalités dites de « partage » qui sont à l'origine du succès des réseaux sociaux rendent plus nécessaires encore la prise en compte du contrôle par les parents des contenus accessibles via ces terminaux. S'il est actuellement possible aux parents de demander à l'opérateur une ligne dans laquelle les fonctions Internet sont limitées, cette limitation n'est en fait qu'une fausse sécurité. En effet, pour des raisons de coûts mais aussi de rapidité d'accès, de nombreux utilisateurs de mobiles et en particulier les plus jeunes, ont recours à des accès via des émetteurs Wi-Fi. Or, dans la plupart des cas, ces émetteurs donnent accès à l'intégralité des ressources de l'internet sans filtrage aucun. Des dispositifs de contrôles parentaux sur les mobiles devraient être élaborés en commun avec les constructeurs et les développeurs de plateformes mobiles. Pour être efficaces, ceux-ci devront être intégrés au système d'exploitation des terminaux mobiles comme ils le sont sur les systèmes d'exploitation des ordinateurs aujourd'hui.

Le CESE plaide pour une stratégie européenne de protection des mineurs sur les terminaux mobiles. La représentation française auprès de la Commission européenne devra favoriser la mise en place à l'échelle de l'Union d'une obligation pour les entreprises d'intégrer des dispositifs de contrôles parentaux dans les systèmes d'exploitation des terminaux mobiles.

Soutenir le déploiement d'une éducation au numérique de la maternelle à l'enseignement supérieur

En interaction avec la famille, l'école constitue le lieu privilégié d'information et d'éducation des enfants et des adolescents en matière d'éducation au numérique, que ce soit dans le cadre des enseignements eux-mêmes ou plus largement dans les différentes composantes de la vie scolaire.

La loi de refondation de l'école rappelée en novembre 2014 par le président de la République, lors de la présentation du grand plan numérique à l'école, doit amener à une véritable politique publique en termes d'accès, de réduction de la fracture numérique, d'apprentissage de tous et de lutte pour l'e-inclusion.

Lors de son avis du 16 janvier 2013 sur *L'avant-projet de loi d'orientation et de programmation pour la refondation de l'école de la République* (rapporteur : M. Xavier NAU), le CESE indiquait que la question du numérique relève de trois problématiques distinctes :

- *« l'apprentissage par tous les élèves de l'usage quotidien des outils numériques (bureautique basique, Internet, messagerie, etc.). Il s'agit ici essentiellement de maîtrise technique de l'outil ;*
- *l'apprentissage par tous du « bon usage », notamment d'Internet, de la messagerie, des réseaux sociaux, de la circulation des images et de leur contrôle : sont à considérer ici la protection de la vie privée, la capacité à distinguer les sources et à ne pas tomber dans les phénomènes de rumeur, etc., en lien avec la Commission nationale de l'informatique et des libertés (CNIL). Il s'agit bien là du lien entre numérique, médias (qu'ils soient numériques ou non) et citoyenneté ; cet apprentissage gagnera à être mis en lien avec l'éducation du sens moral et de l'esprit critique;*
- *l'intérêt pédagogique du numérique : en tant qu'outil utilisé en classe aussi bien que comme banque de données et de ressources au bénéfice des élèves et des enseignants, dans le respect des libertés et de la confidentialité. Il s'agit des espaces numériques de travail (ENT), de l'enseignement à distance, des compléments à l'enseignement donné dans l'établissement, mais aussi du cartable numérique, dont l'utilisation demande encore à être pensée ».*

Concernant l'apprentissage par tous du « bon usage », **le CESE recommande de développer, en milieu scolaire, l'apprentissage, par le biais par exemple des *serious games* (jeux sérieux), des lois et textes réglementaires liés aux usages de l'internet et des réseaux sociaux.** Sur ce point la mise en place d'actions spécifiques vers la communauté pédagogique dans le cadre de l'enseignement moral et civique et doit être poursuivie. Plusieurs académies se sont lancées dans ce challenge de la formation (exemple de l'académie de Versailles et le Citoyen de l'Internet).

Le CESE souligne également la démarche entreprise depuis plusieurs années par l'association Initia-Droit. Cette association d'avocats bénévoles intervient dans les établissements scolaires à la demande des enseignants pour sensibiliser les élèves.

Favoriser l'acquisition d'une éducation à l'esprit critique du développement et de la maîtrise des techniques numériques-

Contrairement à une idée reçue, la culture numérique est distincte de la culture scientifique. Très longtemps, l'informatique a été liée à l'éducation scientifique. L'imaginaire de l'informatique a eu deux effets regrettables. D'une part, la population des acteurs du numérique a longtemps manqué de personnes issues d'autres parcours scolaires. D'autre part, cela a distingué la population en deux groupes : ceux qui codent des programmes, et ceux qui les utilisent.

Il est possible d'avoir une connaissance des principes du code⁹⁵ non pour produire des programmes complexes mais simplement pour mieux comprendre les programmes existants, mieux cerner leurs mécanismes, être en capacité de discerner les fonctionnalités qui sont conformes à nos principes personnels.

Le CESE propose que l'initiation à l'informatique à l'école, qui ne saurait se limiter à l'utilisation d'un ordinateur, vise à initier les élèves à trois notions fondamentales de l'informatique : celles de langage, d'information et d'algorithme.

En ce qui concerne l'apprentissage du codage, le CESE souhaite qu'il ne donne pas lieu à la création d'une nouvelle discipline. Il doit être conçu comme une intégration des trois notions fondamentales de l'informatique dans les enseignements disciplinaires ou transversaux. La transversalité doit pouvoir se mettre en place au collège et au lycée. C'est pour cette raison qu'en l'état actuel du débat il n'est pas favorable à la création d'une discipline nouvelle.

Le développement du numérique accroît la nécessité d'un regard critique vis-à-vis des représentations et des visualisations des données : cela implique que le système éducatif s'en saisisse. Cette dimension transversale peut s'appuyer également des apports de l'ISN (Informatique et sciences du numérique) au lycée, de la technologie au collège ou encore du travail des documentalistes.

Renforcer l'Éducation au numérique dans les programmes scolaires

Comme le souligne le CESE dans son étude sur *L'alternance dans l'éducation* « l'avènement du numérique constitue, à l'évidence, une opportunité à saisir pour offrir des présentations inédites des différents savoirs et des compétences à acquérir pour les traiter au sein du cadre scolaire. De nouveaux formats pédagogiques innovants deviennent, en effet, possibles. Les ressources de l'hyper-texte, les vidéos, l'infographie, les tutoriels sont autant de supports et de moyens pour permettre des présentations variées des savoirs et augmenter ainsi la probabilité de leur appropriation par le plus grand nombre ».⁹⁶

Le numérique est à la fois une source de contenus et un outil pour les enseignants, au service de leurs missions pédagogiques. Pour que les outils numériques fassent partie

⁹⁵ Le code est un ensemble d'instructions qui sont exécutées par un microprocesseur et représentées sous forme binaire constituée d'une suite de 0 et de 1 appelée *bit* (*Binary Digit*). Un fichier informatique est un ensemble de bits.

⁹⁶ Conseil économique, social et environnemental, *L'alternance dans l'éducation*, étude présentée par M. Jean-Marc Monteil au nom de la section de l'éducation, de la culture et de la communication, 2014

de tous les enseignements, **le CESE recommande de veiller à une meilleure intégration du numérique dans les contenus et les modalités pédagogiques des programmes scolaires.**

Le Conseil supérieur des programmes, créé par la loi de juillet 2013, et installé au mois d'octobre 2013, doit participer sur les cinq prochaines années à la définition du socle commun de compétences, des nouveaux programmes de l'école maternelle, à la conception de certains programmes (éducation civique...) ou à la prise en compte de certains parcours (éducation artistique...) dans les programmes. Il a déjà produit des textes importants en ce domaine.

La mise en œuvre des programmes en première année de chacun des cycles à la rentrée scolaire 2015 devra prendre en compte cette ambition puis la poursuivre pour chaque année suivante. Enfin, s'il existe déjà, dans certaines disciplines, un contrôle continu portant sur des enjeux du numérique, **le CESE considère que pour accompagner la prise en compte de l'Éducation au numérique dans les programmes, un contrôle des connaissances acquises est nécessaires. Ses principes ne peuvent être laissés à l'initiative des établissements.**

Pour le CESE, il appartiendra au conseil supérieur des programmes de veiller, conformément à la conception qu'il a proposée pour le socle commun, à ce que l'Éducation au numérique soit traitée de manière transversale, afin qu'elle irrigue l'ensemble des disciplines.

Promouvoir la certification renforcée via le brevet informatique et internet B2i

Créé en 2001 avant d'être généralisé en 2006, le Brevet informatique et internet (également appelé B2i), est une attestation délivrée aux élèves des écoles élémentaires (B2i niveau 1), des collèges (B2i niveau 2), des lycées (B2i niveau 3), qui sanctionne leur capacité à utiliser les outils informatiques et Internet mais également certaines compétences documentaires et éthiques.

Plus spécifiquement, le B2i certifie la maîtrise de la compétence numérique ainsi que l'usage sûr et critique des technologies du numérique. Or, si le B2i est aujourd'hui intégré au socle commun, la certification n'est pas valorisée en collège, comme le sont par exemple les mathématiques ou les sciences physiques.

Aujourd'hui la question est posée du maintien de ce B2i et de son articulation avec les nouvelles modalités d'évaluation du socle commun dont le Conseil supérieur des programmes a la charge.

Si le B2i est maintenu le CESE recommande d'adapter son contenu en permanence pour l'enrichir aux aspects liés aux enjeux socio-économiques et citoyens. Le volet « éthique numérique » de cette certification pourrait laisser une place importante à la réflexion sur la sécurité des données personnelles, à l'heure du *Big Data*. Dans le cas où d'autres modalités seraient retenues le CESE recommande que ce volet reste présent. Ce contrôle mériterait d'être étendu dans une approche transdisciplinaire qui pourrait s'appuyer notamment sur des modalités d'évaluation analogues aux travaux personnels encadrés (TPE), aux itinéraires de découverte (IDD), etc.

L'établissement d'une organisation commune de cette certification, quitte à la dématérialiser via *une plateforme internet*, une forme qui serait cohérente avec son contenu, pourrait permettre une meilleure diffusion.

Dans le cadre d'une évolution du brevet et du baccalauréat, une évaluation des compétences numériques pourrait être proposée dans une épreuve terminale de synthèse, comme indiqué précédemment.

Le travail sur l'enseignement moral et civique confié au conseil supérieur des programmes devra être l'occasion de souligner tout ce que l'Éducation au numérique peut apporter à l'éducation à la citoyenneté en général et de mettre en avant le point d'appui qu'elle pourrait constituer.

Renforcer la formation au numérique au sein de l'Éducation nationale et de l'enseignement supérieur

□ *Former les enseignants aux enjeux de l'éducation au numérique*

Pour réussir ce pari de l'éducation au numérique, la formation des enseignants est une priorité absolue. **Le CESE recommande que le chantier majeur de la formation des enseignants aux usages numériques soit développé le plus rapidement possible.**

Actuellement, l'informatique demeure une discipline dont l'enseignement est confié à des enseignants spécifiques. Or, s'il est bien nécessaire pour les élèves qui se destinent à être des acteurs du numérique de leur offrir un enseignement spécifique avec des enseignants spécialisés, pour la formation commune à tous les élèves, l'approche doit être transversale.

C'est dans ce sens que va la seconde proposition du rapport Jules Ferry 3.0 du Conseil national du numérique. La littératie numérique comprend des savoirs, des compétences et des méthodes permettant à l'individu d'être acteur de sa vie dans nos sociétés du tout numérique : « *Ancrer l'école dans cette dynamique, c'est inviter les élèves à participer à une culture et à une économie, fondées sur l'échange des savoirs, la coopération, la création* ».

Les Technologies de l'information et de la communication (TIC) doivent cesser d'être une fin en soi, incarnée par une matière propre, mais doivent irriguer chacune des disciplines du parcours scolaire. Il faut en tirer les conséquences en matière de formation des enseignants en faisant preuve d'anticipation.

Concrètement, donner les outils, à la fois techniques et pédagogiques, pour que chaque enseignant puisse enseigner sa discipline en s'appuyant sur les TIC demeure le moyen le plus sûr de permettre la diffusion d'une culture numérique dans les établissements scolaires.

Les enseignants demeurent actuellement recrutés par des concours qui certifient principalement leur maîtrise d'une ou de quelques disciplines académiques spécifiques. Il est peu envisageable d'insérer en l'état, parmi les critères de leur recrutement, une maîtrise des TIC, d'autant que leur diplôme intègre la validation du C2i. **Toutefois, le CESE considère qu'il est souhaitable d'insérer dans leur formation une part plus importante consacrée à celles-ci, quelle que soit leur discipline ou spécialité afin de permettre l'établissement d'un socle commun de culture numérique.**

Le CESE préconise que la formation des enseignants dans les écoles supérieures du professorat et de l'éducation (ESPE) permette des mises en situation pédagogiques

d'utilisation du numérique, sous forme par exemple de classes inversées, de pratiques coopératives, d'entraide entre les élèves.

Il préconise plus encore un effort d'ampleur dans ce sens en matière de formation continue afin de former massivement les enseignants déjà en exercice. En effet si certains enseignants sont réticents à utiliser les outils numériques c'est principalement par manque de formation aux technologies de l'information et de la communication. C'est la raison pour laquelle il est important de veiller à ce que les enseignants en poste puissent également bénéficier de formations pour s'initier aux technologies, aux logiciels ou applications spécifiques à leur discipline ou réactualiser leurs connaissances.

Le CESE recommande d'intégrer un volet « éducation au numérique » dans les projets d'établissement et d'école accompagné d'une ingénierie pédagogique et d'un responsable à cet effet. Cela permettra de recenser au sein des établissements les besoins de formation des personnels à l'usage du numérique et de mettre en place un plan pluriannuel pour développer des formations pour les enseignants qui associent la maîtrise technique du couple « numérique/pédagogie ».

□ Développer la formation au numérique des ingénieurs

Au sein de l'enseignement supérieur, l'utilisation du numérique doit devenir la norme. A ce jour seul le certificat informatique et internet (C2i) répond en partie aux enjeux de l'éducation au numérique qui s'inscrit dans le dispositif général de certification B2i/C2i mis en place par le ministère de l'Éducation nationale et de l'Enseignement supérieur. Le C2i se décline en deux volets, un volet de compétences numériques générales, le C2i niveau 1, et un volet de compétences numériques à finalités professionnelles, le C2i niveau 2 (C2i2e). L'objectif du premier est de munir l'étudiant dès son entrée dans les études supérieures des compétences numériques nécessaires au bon déroulement de ses études. Le second volet, quant à lui, se décline en de multiples filières de formation propres aux métiers de l'enseignant, du droit, de la santé, de l'ingénieur, etc.

Le CESE préconise de renforcer l'attrait du C2i dans l'ensemble des titres et diplômes délivrés par les écoles et les universités.

Pour s'assurer de l'adéquation des infrastructures informatiques et des outils d'analyse et de traitement du *Big Data*, et pour anticiper les besoins de l'entreprise **en matière de protection des données personnelles, il est nécessaire selon le CESE que la formation en informatique des ingénieurs et scientifiques non-informaticiens aborde précisément tous ces enjeux.**

La formation d'ingénieurs et de scientifiques passent notamment par les classes préparatoires et les Grandes Écoles. Elle conduit une grande partie des élèves obtenant un diplôme d'ingénieur à un niveau correspondant à la troisième année ou quatrième année d'université en mathématiques et en physique.

Aujourd'hui, on délivre 48 000 diplômes ou grades de master au grade de master en technologique de l'information, dont 34 000 issus des écoles d'ingénieurs. Le CESE considère qu'il est essentiel, notamment pour renforcer la formation et l'acquisition de compétence au risque numérique, de fixer des objectifs similaires en informatique. Il existe un certificat informatique et internet niveau 2 « métiers de l'ingénierie » (C2i2mi), un certificat dans cinq grands domaines dont 2 spécifiques ingénieurs et dont la mise en place graduelle à partir 2009 demeure encore sur la base du volontariat.

Le CESE recommande que le volume d'heures d'informatique en classes préparatoires scientifiques, aujourd'hui de 2 heures, soit revu à la hausse pour permettre notamment au sein des écoles d'ingénieurs une meilleure acquisition des enjeux de sécurité informatique.

Si de nombreuses écoles d'ingénieurs accordent une place importante à l'enseignement de l'informatique. Il est important de s'assurer que le contenu est approprié et ne délaisse pas l'enseignement des bases au profit de l'enseignement d'outils et de techniques qui pourraient être rapidement obsolètes. Il conviendra d'examiner dans quelle mesure le référentiel C2i2mi est couvert par le cursus proposé par les écoles pour ensuite corriger les lacunes. Antoine Fréchet⁹⁷ ajoute : « *le fait de connaître en plus les enjeux réglementaires et juridiques est un plus* ».

Le CESE recommande que le référentiel des C2i et C2i2mi tout particulièrement sur les volets « protection des données personnelles » et « informatique et libertés » fasse l'objet d'une labellisation avec le concours de la Commission des titres d'ingénieur (CTI) et celui de la CNIL.

Plus spécifiquement, **le CESE préconise le développement de formations de haut niveau autour des métiers de spécialistes de la donnée (*data scientists*) mais aussi des métiers de vente de la donnée (*Data brokers*) et encourage la CNIL à renforcer ses partenariats avec l'ensemble des établissements d'enseignements concernés.**

□ *Education numérique et formation continue.*

Il faut renforcer l'enseignement de la sécurité informatique dans le cadre de la formation continue. Sur ce point, **le CESE recommande notamment la mise en place d'un plan national de financement avec le Centre des études supérieures de l'industrie (CESI).**

Établissements scolaires et le déploiement des outils numériques

La loi de refondation met en place le service public du numérique éducatif et transfère la maintenance informatique à la collectivité de rattachement. Ce choix doit s'accompagner des moyens humains et financiers nécessaires à son bon fonctionnement afin que le développement des Espaces numériques de travail (ENT) soit équilibré sur l'ensemble du territoire et que la poursuite de l'équipement en outils et ressources numériques (tableau numérique interactif, tablettes) soit assuré pour l'ensemble des établissements scolaires.

La réussite d'une éducation au numérique sur l'ensemble du territoire national est subordonnée en tout premier lieu au déploiement de réseaux de très haut débit. La qualité du débit et la maintenance des outils informatiques par des personnels qualifiés doivent être prioritaires. Cela implique notamment le recrutement d'ingénieurs systèmes. Ce chantier, qui doit mobiliser l'ensemble des collectivités territoriales, est stratégique pour notre pays. Or, nombre d'écoles notamment celles situées dans les zones les plus rurales n'ont pas aujourd'hui accès à un haut débit permettant de répondre à un besoin en connectivité d'au moins 8 mégabits par seconde.

Le CESE recommande que le Plan France très haut débit fasse du raccordement en fibre optique à court et moyen terme des sites d'intérêt général, notamment des

⁹⁷ Directeur général du Groupe des écoles nationales d'économie et statistiques (GENES).

établissements scolaires, une priorité. Il s'agit d'assurer l'accès à un internet de qualité dans chaque école, collège et lycée, public ou privé.

Le CESE demande qu'un an environ après le lancement de l'appel à projets « Ecoles connectées » (mai 2014), soit réalisé un bilan qualitatif et quantitatif et que, selon les résultats, le budget initial de 5 millions d'euros soit réévalué pour répondre à l'objectif que tous les établissements scolaires, en particulier collèges et lycées, puissent accéder à l'internet haut débit.

Pour permettre l'indispensable compatibilité entre une vraie liberté pédagogique et un travail collaboratif, le CESE recommande que soit systématisé dans l'éducation nationale le recours aux applications et aux formats libres et ouverts. Au-delà d'une visée citoyenne, cela permettrait également de réaliser des économies significatives. Au-delà d'une visée citoyenne, cela permettrait également de réaliser des économies significatives. Il recommande également le développement de plateformes propres à l'Education nationale proposant aux personnels et aux élèves des ressources indépendantes.

Le CESE considère enfin qu'il est nécessaire de lutter contre la banalisation du recours à la vidéosurveillance et à des procédés de captures biométriques pour assurer la sécurité dans les établissements scolaires. **Le CESE recommande de rendre exemplaire l'école face à la biométrie et d'interdire l'usage de la capture de données personnelles par les procédés biométriques dans ces établissements.**

Lutter contre les nouvelles fractures numériques

Au-delà des jeunes scolarisés, la culture du numérique doit s'étendre à l'ensemble de la population, notamment les plus éloignées en termes d'accès et de difficultés sociales.

Comme la citoyenneté réelle, la citoyenneté virtuelle est concrètement inégale. En droit, nous sommes tous égaux, mais de multiples facteurs nous rendent, de fait, inégaux. Nous n'avons par exemple pas tous de connexion à internet. Et quand bien même l'accès à internet existe, nous n'avons pas tous un usage instruit du fonctionnement des outils que nous utilisons au quotidien. Enfin, même si nous avons un usage instruit de nos outils habituels, nous pouvons ne pas avoir le temps ou le désir de participer à des expériences de démocratie virtuelle. L'enjeu, sur ce plan, est clair : comment donner des nouveaux moyens d'agir aux citoyens en termes de débat public ? Ceci concerne les données publiques mais aussi les applications numériques par exemple dans le domaine de la santé, de l'éducation, du développement durable ou des transports. Il s'agit de peser sur la prise de décision publique, et sur les moyens qui y sont liés pour que cela constitue un progrès démocratique et non une régression, qui reposerait sur la création de nouvelles distinctions entre classes de citoyens.

L'enjeu de l'e-inclusion a donné lieu en novembre 2013 à un rapport du Conseil national du numérique, intitulé *Citoyens d'une société numérique - accès, littératie, médiations, pouvoir d'agir : pour une nouvelle politique d'inclusion*. Cet enjeu consiste à mettre en place des projets de courts et de longs termes, et de cibler des actions sur des publics qui sont à des points différents de l'inclusion ou de l'exclusion : sont-ils exclus pour des questions matérielles, économiques, sociales, géographiques ?

Le CESE considère que la problématique de l'inclusion s'est par le passé trop fortement focalisée sur la question de l'accès aux équipements et aux réseaux. Cette vision étroite de

l'inclusion a conduit à la cristallisation du débat et à la concentration des efforts de l'action publique autour du déploiement nécessaire des infrastructures. Or la fracture numérique d'équipement se double désormais d'une fracture numérique d'usage et ce sont les populations les plus éloignées de l'emploi, en situation de précarité ou qui sont les plus désavantagées sur le plan de l'accessibilité aux différents espaces de médiation numérique (illettrisme, personnes en situation de handicap, personnes âgées, personnes issues de zones péri-urbaines ou rurales) qui en sont les premières victimes.

Dans le prolongement des conclusions des différents travaux du Conseil national du numérique, le CESE considère que la vision de l'e-inclusion doit désormais être indissociable de l'inclusion sociale, et se penser à travers une action publique continue et globale. Ce travail considérable qui doit rassembler l'ensemble des acteurs - qu'ils soient institutionnels ou citoyens pour éviter qu'une partie de la population ne puisse pas contribuer entièrement au débat public et se retrouve sous-représentée.

Dans un monde où tout incite les gens à utiliser les services numériques, il faut être attentif au sentiment d'exclusion. Si nous voulons renforcer la participation démocratique, il ne faut laisser personne à côté du chemin.

Redynamiser les politiques publiques sur les territoires

Les politiques publiques du numérique doivent toucher tous les territoires. Cet effort passe par une redynamisation des politiques publiques en faveur du numérique sur les territoires.

Le CESE recommande à l'Etat et aux collectivités territoriales de veiller au soutien de l'éducation au numérique au sein de l'ensemble des territoires de la République. Il s'agit tout particulièrement de favoriser l'accès à la ressource numérique dans les zones rurales et périurbaines qui sont les plus en difficulté. Dans le cadre des politiques culturelles, les orientations pour une culture pour tous doivent s'accompagner d'actions en matière d'accueil et d'accès aux lieux dédiés à l'inclusion, la mixité et l'innovation sociale par le numérique. Cela est indispensable pour rendre plus lisible et plus accessible des projets d'innovation sociale au stade de l'expérimentation locale et favoriser un meilleur maillage numérique du territoire national.

Le CESE préconise la mise en œuvre systématique d'un volet numérique au sein des schémas de développement des territoires. Ces schémas territoriaux doivent être l'occasion de soutenir l'ensemble des partenaires que sont les associations, notamment d'éducation populaire, qui investissent le champ du numérique et permettent des formes de médiations en direction des populations que nous avons précédemment décrites dans la première partie de cet avis.

Revitaliser les Espaces publics numériques (EPN)

Pour le CESE, les politiques publiques de formation aux « enjeux du numérique » doivent combattre la méconnaissance des mécanismes sociaux engendrés par les nouveaux usages liés au numérique et la faible prise en compte de ces enjeux dans les politiques locales. Celles-ci doivent pour cela favoriser la diversité des partenaires (scientifiques, culturels, techniques, sociaux, éducatifs, sportifs etc.) et des bénéficiaires des services (jeunes, parents, seniors..) dans une perspective de transformation sociale par les

usages du numérique (esprit critique, nouvelles formes d'engagement, de productions du savoir, de créations culturelles).

Pour que les individus deviennent des utilisateurs avertis et responsables des données numériques et non de simple consommateurs, pour éviter que l'utilisation et le traitement de ces données ne soient l'apanage que des entreprises ou administrations, il faut déployer sur l'ensemble du territoire des points d'accès. Ces relais faciliteront pour tous la manipulation, la compréhension, la valorisation des données dans le respect des droits et des libertés.

Les EPN sont une première réponse. En raison de la diversité des organismes auxquels ils étaient adossés mais aussi des missions culturelles, sociales ou professionnelles auxquelles ils se sont consacrés, les réseaux d'EPN constituent une mosaïque de plus de 7000 lieux sur l'ensemble du territoire. Cette diversité de missions des EPN est l'une des richesses du paysage français de la médiation numérique.

Le CESE propose que soit réaffirmé le rôle des Espaces publics numériques (EPN) afin qu'ils deviennent à la fois des lieux de proximité et d'éducation populaire pour tous et de véritables espaces de sensibilisation, de médiation à la manipulation et à la fabrication des données. Les efforts pour leur revitalisation doivent être à la hauteur des enjeux et des opportunités portées par la révolution numérique.

Une spécialisation accrue des EPN nuirait à la démultiplication des apprentissages qui doit toucher toutes les applications du numérique (accès aux administrations, éducation à la protection des données, créations d'applications numériques, apprentissage de l'imprimante 3D...) et tous les publics avec l'aide du milieu associatif.

Le CESE considère que les EPN doivent s'ouvrir plus largement à toutes les modalités de l'expression numérique, et à l'ensemble des usages que favorisent le numérique, que ce soit dans le domaine de la culture, des transports, de la fabrication, de la vie associative.

A cet effet, le CESE recommande que dans le cadre de la consultation publique sur la médiation numérique initiée par Axelle Lemaire, secrétaire d'Etat chargée du Numérique, les moyens de créer un nouveau label mis en œuvre pour servir une véritable politique de transition numérique et qu'à cette occasion soit créée une plateforme publique pour requalifier des établissements culturels en faveur de l'éducation au numérique.

Plus que jamais, un tel label doit être développé pour faire des EPN des centres de ressources pour la culture numérique dans les territoires. Ce mouvement nécessite de faire un premier bilan sur l'état de compétence en relation avec l'usage du numérique. Or l'absence de bilan de l'expérience des EPN (chiffres, indicateurs...) et ce depuis plus de 15 ans rend plus difficiles les réflexions prospectives sur leur éventuel nouveau redéploiement.

C'est pourquoi le CESE préconise la réalisation d'un bilan-audit du dispositif EPN et recommande dans le même temps la mise en place de missions statistiques dédiées à la production de nouveaux indicateurs sur les usages du numérique.

Ce programme de revitalisation doit s'appuyer sur une ingénierie publique en matière de développement d'espace public numérique. Une ouverture du champ d'activité des EPN aux différentes facettes de l'économie numérique oblige à accompagner ces acteurs dans l'élévation de leurs compétences dans le champ de l'innovation. La formation des animateurs est de ce point de vue une question centrale pour adopter une démarche de projet dans la formation numérique des citoyens.

La revitalisation des EPN nécessite de revoir également les rôles et la formation des animateurs qui composent ces lieux et plus encore dans le nouveau champ d'innovation qu'elles sont amenées à promouvoir.

L'éducation au numérique et à la protection des données doivent être pensée et intégrée en amont des projets collaboratifs. **Le CESE recommande qu'au sein des EPN, cette dimension de l'éducation au numérique soit favorisée à l'occasion de l'élaboration des programmes de formation et d'action.** Il s'agit d'aider les jeunes et moins jeunes à mieux organiser et maîtriser la totalité des données et les accompagner à concevoir des objets ou des applications numériques au-delà des simples usages bureautiques. Ces travaux doivent s'engager sur des projets en lien avec le territoire, le développement durable, le tissu urbain ou la valorisation des données collectées.

En complément du soutien à l'innovation numérique, la culture de la protection des données et leur maîtrise doit faire partie des futures missions des animateurs EPN. Cette orientation doit s'inscrire dans un mouvement d'accompagnement des usages collaboratifs à l'aide par exemple de sites contributifs (emploi, services, culture...).

Afin de familiariser les citoyens aux ressources informationnelles mises à disposition dans le cadre de la démarche Open Data par l'État et les collectivités territoriales, des projets devraient être mis en place afin de créer de nouveaux services d'intérêt général.

Dans cette perspective, le CESE préconise l'organisation de nouvelles formes de concours afin, d'une part d'aider à créer de nouvelles générations de services numériques utiles pour les citoyens et d'autre part associer les EPN à la démarche de développement de ces services. Ces services pourraient à la fois être liés à la santé, au tourisme ou à la maîtrise de l'énergie⁹⁸. L'une des bases de développement de ces services serait liée aux données publiques mises à disposition des citoyens dans le cadre de démarches open data. C'est en se basant sur ce principe que quatre agences fédérales américaines ont développé un concours pour aider à créer un appareil mobile permettant de mesurer l'impact de la pollution sur la santé⁹⁹.

De plus, parallèlement à l'ouverture par l'État des données publiques aux citoyens, les entreprises commencent aussi à mettre à disposition de leurs usagers des données liées à leur consommation par exemple dans le domaine de l'énergie. Ce principe est aussi appelé « ouverture intelligente » des données (ou *Smart Disclosure*). Cette ouverture des données des entreprises peut donner lieu à la création de nouveaux services par des tiers en particulier pour favoriser les démarches de maîtrise de l'énergie. À terme, d'autres secteurs pourraient s'emparer de ce type de dispositifs pour favoriser la création de nouvelles générations de services à valeur ajoutée utiles aux citoyens.

Le CESE préconise d'associer « démarche projet » et utilisation des données issues de la démarche open data dans les actions de formation numérique des citoyens.

Dans le cadre des dispositifs d'accompagnement à la maîtrise des données numériques,

98 <http://www.proximamobile.fr/article/une-initiative-americaine-pour-maitriser-la-consommation-electrique-depuis-les-mobiles> <http://petitlien.fr/CESEnum2>

99 États-Unis : un concours pour créer un appareil mobile mesurant l'impact de la pollution sur la santé (Proxima Mobile - 6 octobre 2012) <http://www.proximamobile.fr/article/etats-unis-un-concours-pour-creer-un-appareil-mobile-mesurant-l'impact-de-la-pollution-sur-l> <http://petitlien.fr/CESEnum3>

les citoyens devront être en mesure de participer à des projets basés sur les données publiques mises à disposition des citoyens par l'État et les collectivités territoriales (par exemple dans le domaine de la valorisation des territoires, du patrimoine ou de la protection environnementale).

Repenser un « service universel » dédié aux actions d'accompagnement des citoyens vers la maîtrise des données numériques

Les mutations des usages numériques rendent désormais nécessaires la pérennisation des dispositifs d'accompagnement afin qu'ils soient adaptés aux nouvelles modalités d'accès aux réseaux, en particulier via les mobiles. De nouvelles sources de financement des activités d'accompagnement numérique des citoyens doivent être mises en place. Si, à l'origine, la notion de service universel de téléphonie avait pour objectif d'éviter les discriminations géographiques, ce principe doit désormais inclure les dimensions de maîtrise des technologies et des données par l'ensemble des usagers et en particulier les plus défavorisés. Ainsi la montée en puissance des usages mobiles et l'obsolescence progressive des cabines téléphoniques devenues un poste de dépense pour les opérateurs de télécommunications offre l'opportunité de réorienter ces fonds afin de créer les dispositifs permettant l'inscription durable des formations au numérique dans le paysage éducatif des citoyens.

Le CESE suggère la création d'un volet du « service universel » dédié à la médiation numérique. Les fonds actuellement versés par les opérateurs de télécommunication dans le cadre du service universel de téléphonie (et en particulier à la publiphonie)¹⁰⁰ pourraient pour partie être réalloués au financement de la revitalisation des EPN en vue d'assurer la formation numérique des citoyens. Ces dispositifs de formation prendraient ainsi en compte les mutations des nouvelles générations de services mobiles et d'objets connectés afin notamment d'accompagner les personnes à l'acquisition d'une culture de la gestion et de la protection des données issues ou émises par ces objets connectés.

Une telle option ne doit pas exclure de réfléchir à l'augmentation de ce fonds en favorisant notamment un abondement par d'autres acteurs du numérique autres que les opérateurs de télécommunication.

¹⁰⁰ L'article L35 du code des postes et des communications électroniques (CPCE) dispose : « Les obligations de service public sont assurées dans le respect des principes d'égalité, de continuité et d'adaptabilité. Elles comprennent :

- a) Le service universel des communications électroniques défini, fourni et financé dans les conditions fixées aux articles L. 35-1 à L. 35-4 ;
- b) Les services complémentaires au service universel des communications électroniques offerts dans les conditions fixées à l'article L. 35-5 ;
- c) Les missions d'intérêt général dans le domaine des communications électroniques, en matière de défense et de sécurité, de recherche publique et d'enseignement supérieur, assurées dans les conditions fixées à l'article L. 35-6 ».

Soutenir les initiatives des « tiers-lieux »¹⁰¹ pour renforcer les réseaux d'accompagnement à la maîtrise du numérique

À cette diversité s'ajoutent désormais des missions spécifiques de certains tiers-lieux : *FabLabs* (lieux d'apprentissages des technologies de fabrication numérique), espaces de travail partagé (*coworking*).

Les espaces de médiation numérique doivent être des lieux de socialisation et ne pas renvoyer l'intéressé à une application pour obtenir via un abonnement une ressource. L'intermédiation et l'échange doivent être au fondement des démarches collectives pour faire émerger des projets culturels numériques. Pour la formation il faut s'inspirer de ce qu'a fait de Caisse des dépôts et consignations (CDC) pour développer des modules de formation, des kits tutoriels pour accompagner les animateurs.

Dans le domaine culturel, on peut évoquer les Maisons des jeunes et de la culture 2.0 (MJC 2.0) et les équipements socio-culturels qui permettent de développer des ateliers créatifs autour de la musique, de la culture, de la peinture en utilisant le numérique. Des pratiques qu'il convient d'encourager et de démultiplier sur tout le territoire.

Sur le plan économique, c'est aussi une opportunité de favoriser les lieux de créations et les entreprises naissantes du numérique. Il s'agit là de nouveaux lieux de formation et de diffusion d'une culture de l'innovation. C'est le cas des *FabLabs* qui sont des laboratoires de fabrication ouverts aux publics et qui mettent à disposition du matériel informatique pour la conception et la réalisation d'objets, comme les imprimantes 3D, par exemple. Ces lieux permettent de passer rapidement de la phase du prototype à celle de la mise au point et du développement de nouveaux objets ou de nouveaux services. Ces *FabLabs* peuvent également être un outil d'aide à l'insertion des publics défavorisés en leur ouvrant le champ du numérique et en favorisant l'e-inclusion.

Aussi le CESE recommande qu'une évaluation de ces initiatives soit engagée : c'est un outil indispensable au pilotage des politiques publiques.

Le CESE recommande qu'un travail de redéfinition des labels concernant certains type de *FabLabs* à la française soit entrepris et préconise que ces derniers viennent compléter les Espaces publics numériques (EPN).

C'est autour de la diversité des acteurs du numérique qu'émergeront les profils et les idées à même de relever le défi de la transition du numérique. C'est ainsi que les populations les plus éloignées qui en sont le plus éloignées seront prises en compte. Le potentiel d'innovation porté notamment par l'entrepreneuriat sera le plus flagrant et utile à notre société, et ce sur l'ensemble des classes d'âges.

Ces lieux d'expérimentation doivent agir comme des outils de régulation de l'utilisation des données personnelles pour empêcher la formation de monopoles sur la création de valeur autour des données numériques et l'orienter au profit de la communauté. A la fois lieux d'échange, de débat, de création et d'apprentissage, les tiers-lieux représentent un

¹⁰¹ Le tiers-lieu, ou la troisième place, ou est un terme traduit de l'anglais *The Third Place*. Il fait référence aux environnements sociaux se distinguant des deux principaux que sont la maison et le travail. Dans son livre datant des années 1980 *The Great, Good Place*, Ray Oldenburg, professeur émérite de sociologie urbaine à l'université de Pensacola en Floride, indique que les troisièmes places sont importantes pour la société civile, la démocratie, l'engagement civique et instaurent un sentiment d'espace. Il s'entend comme volet complémentaire, dédié à la vie sociale de la communauté, et se rapporte à des espaces où les individus peuvent se rencontrer, se réunir et échanger de façon informelle ». Source Wikipédia

levier puissant de citoyenneté. Ils sont également essentiels pour accompagner les citoyens dans l'utilisation et la protection des données et pour diffuser une culture de la donnée au sein de la société.

Lutter contre l'enfermement de l'internet en renforçant le lien intergénérationnel.

La fracture générationnelle sur Internet est souvent décrite sous l'angle du défaut de maîtrise des technologies par les seniors et donc des handicaps sociaux et culturels auxquels seraient soumises les personnes âgées. Cependant, cette fracture peut revêtir d'autres formes à travers le risque d'enfermement des usagers des plateformes autour des seules personnes qui partagent leur opinion. Cela peut se révéler dangereux pour le débat démocratique comme le rappelle le constitutionnaliste Cass Sunstein¹⁰² :

Cet appauvrissement du débat public, voire la radicalisation progressive de certains des groupes sur Internet, constitue un risque démocratique majeur pour nos sociétés ; un risque qui est renforcé par l'accélération de l'information que permet le numérique. Cette « *polarisation de groupe*¹⁰³ » permet en effet aux seuls membres les plus actifs d'une communauté en ligne de devenir « audibles ». Sans compter que les algorithmes qui régissent le fonctionnement des principales plateformes peuvent être entièrement opaques pour le commun des mortels. Ainsi, les systèmes de recommandation sur Internet peuvent avoir un rôle d'élimination des opinions contraires sur Internet en orientant les internautes vers les opinions « dominantes » et en évitant qu'ils ne soient là encore confrontés à des arguments qui remettraient en cause leurs préjugés. Or, le dialogue entre générations est justement l'un des moyens de remettre en cause certains préjugés d'autant que les seniors continuent d'être sous-représentés sur Internet. En plus de ses conséquences sociales et politiques, cette fracture générationnelle pourrait aussi avoir des conséquences économiques sur la création des entreprises. En effet pour résoudre les problèmes nouveaux liés à l'énergie, la santé ou l'environnement, il sera nécessaire d'intégrer des savoirs et des savoir-faire qui ne peuvent être issus des seules fractions les plus jeunes des populations¹⁰⁴.

Afin de combattre le risque d'enfermement générationnel sur internet, **le CESE recommande qu'en plus du fait de renforcer les mesures d'accompagnement des seniors vis-à-vis des technologies, des programmes spécifiques soient mis en place pour permettre l'échange entre les générations.**

102 « En premier lieu, les citoyens doivent être mis en contact avec des sujets qu'ils n'ont pas choisis par avance. Les rencontres non prévues, non planifiées sont un élément central de la démocratie elle-même. De telles rencontres concernent souvent des opinions et des sujets que les citoyens n'ont pas recherchés et que peut-être ils trouvent dérangeants. Ces rencontres sont importantes en partie pour se prémunir contre les risques de fragmentation ou d'extrémisme qui sont le résultat prévisible d'une situation dans laquelle des personnes ayant les mêmes opinions n'échangent qu'entre elles. Je ne suggère pas que les gouvernements devraient forcer les citoyens à être soumis à des choses qu'ils souhaitent éviter. Mais je prétends que, dans une démocratie digne de ce nom, les citoyens sont souvent mis en contact avec des idées et des thèmes qu'ils n'ont pas spécifiquement choisis ». Republic.com (Princeton 2001).

103 Cass Sunstein, *The Law of Group Polarization*- University Of Chicago Law School 1999.
http://www.law.uchicago.edu/files/files/91.CRS_.Polarization.pdf
<http://petitlien.fr/CESEnum4>

104 *Why teaching grandmothers to code isn't a crazy idea* (Washington Post 15/8/2014)
<http://www.washingtonpost.com/blogs/innovations/wp/2014/08/15/why-teaching-grandmothers-to-code-isnt-a-crazy-idea> <http://petitlien.fr/CESEnum5>

Entreprises, administrations : quelle éducation au numérique ?

Un développement numérique sans confiance ne peut pas produire tous les effets positifs que l'on peut espérer en termes de progrès économiques, sociaux et environnementaux. Le besoin de confiance, de sécurité et de protection de nos concitoyens crée donc une exigence nouvelle pour les entreprises et les administrations qui devront y répondre pour utiliser harmonieusement et de manière équitable les données. « *La confiance devient une valeur centrale dans le monde numérique caractérisé par l'incertitude, la dématérialisation et la vitesse. Elle est non seulement nécessaire pour lier des communautés de travail en réseau mais aussi indispensable aux transactions avec les clients et les autres partenaires. La confiance est également partie prenante de l'e-réputation. Elle constitue une préoccupation majeure de la protection des données. En somme, elle devient une valeur fondamentale de la bonne gouvernance de l'entreprise* ». ¹⁰⁵

Promouvoir une politique de sécurité et de protection des données au sein des entreprises et des administrations

Tous les observateurs de bonne foi reconnaissent que les Big Data posent des questions de sécurité, de confidentialité et de propriété des données. Une question qui dépasse le seul enjeu de la protection des données personnelles puisqu'elle concerne directement et plus encore les ressources stratégiques d'une entreprise ou d'une administration de l'Etat. Dès lors évoquer la protection des données personnelles renvoie à ce stade à la nécessité d'assurer en amont des entreprises ou des administrations les conditions suffisantes d'un environnement sécurisé dans le stockage, le traitement et le partage des données. Une exigence qui ne peut être portée que par une politique de sécurité et de protection intégrée à la politique globale de l'entreprise. Et bien que la plupart de ces questions puisse être résolues grâce aux techniques de cryptage, d'anonymisation, de codage et de lignes sécurisées, le débat de société autour des risques liés à la capture illicite de données et à la surveillance continue demeure entier.

L'un des principaux freins à la promotion de la culture de la protection des données est à l'absence de gestion responsable du développement des *Big Data*. En effet, il manque pour cela des analystes de données aux compétences croisées et multiples, en statistique, en informatique et en économie. La France ne dispose pas de personnels suffisants pour développer ces méthodes analytiques ¹⁰⁶. Et les écoles d'ingénieurs ne préparent pas leurs élèves à ces mathématiques très spécialisées. Il en va de même aux États-Unis, où il manquerait entre 140 et 190 000 analystes des données.

Certaines entreprises souffrent également d'un déficit de protection de leurs données et de sécurité informatique. Une situation qui peut nuire à leur réputation et à leurs intérêts dans les domaines de l'innovation et de la recherche.

¹⁰⁵ Pascal Buffard. Président du CIGREF.

¹⁰⁶ Hervé Collignon – associé d'A.T.Kearney, coauteur d'une étude sur le secteur de la haute technologie en Europe – Février 2014.

Aussi le CESE préconise de développer la formation et le recrutement d'experts en sécurité informatique et en protection des données numériques.

Concernant les administrations publiques, **le CESE recommande un effort conséquent de formation des agents publics à l'utilisation des données personnelles, à leur traitement et à la nécessité de l'anonymisation de certaines d'entre elles notamment dans le déploiement de l'open data.**

Faire de la protection des données personnelles un nouvel avantage compétitif de l'entreprise

L'une des conséquences de l'affaire Snowden aura été de montrer qu'au-delà de la surveillance des citoyens mise en place auprès des grands acteurs industriels de l'internet, les normes et les technologies de sécurité elles-mêmes avaient été altérées ou corrompues. Cela a par exemple été le cas avec le programme Bullrun¹⁰⁷ de la NSA dont les ingénieurs ont volontairement altéré la confidentialité des échanges en introduisant dans les dispositifs de chiffrement¹⁰⁸ des « portes dérobées » (*backdoors*¹⁰⁹) qui permettaient aux services de la NSA de décrypter les messages.

Cette fragilisation des dispositifs cryptographiques constitue une menace sur l'ensemble des processus qui assurent la confidentialité des échanges (qu'il s'agisse du commerce électronique, des échanges de données sensibles pour les États ou de la protection des secrets industriels...). Dans un autre domaine crucial pour nos démocraties, la suspicion née de ces révélations pourrait aussi être à l'origine de la remise en cause des scrutins menés grâce à des dispositifs électroniques. Ces constatations ont été à l'origine de nombreuses remises en question du fonctionnement actuel des organismes chargés d'élaborer les normes et standards de l'internet, en particulier dans le domaine de la sécurité¹¹⁰.

Or encore trop peu d'entreprises, notamment les PME et les ETI, bénéficient de politiques de sécurité des données en leur sein. Une situation qui bien souvent résulte d'une méconnaissance du cadre légal en la matière. Pourtant la protection des données des entreprises et la promotion d'une éthique du numérique sont pour le CESE la possibilité offerte aux entreprises de mettre en avant la sécurité des données en tant qu'avantage compétitif et de consolider la relation de confiance avec l'utilisateur.

Promouvoir des tests de maturité numérique

Une très grande partie des entreprises et des établissements publics étant passés au numérique de manière désordonnée se retrouvent dans une situation d'usage et traitement intensifs de ressources numériques, y compris de ressources issues de la collecte et du traitement de données, ou de ressources nourrissant le *Big Data*. Ceci est en outre doublé d'une croyance illusoire et leur maîtrise des contraintes et enjeux de ces technologies. Un grand nombre de ces acteurs n'identifient pas leurs faiblesses résultant de leur manque de maturité numérique.

107 <http://www.theguardian.com/commentisfree/2013/sep/05/government-betrayed-Internet-nsa-spying> <http://petitlien.fr/CESEnum7>

108 Plus précisément dans les systèmes de génération des nombres aléatoires (Dual Elliptic Curve Deterministic Random Bit Generator (Dual_EC_DRBG).

109 *The Internet after Snowden : New threat model army* (*The Economist*, 11/11/2013) <http://econ.st/1r5U71J> <http://petitlien.fr/CESEnum8>

110 *Panel recommends NIST declare independence from NSA* (FCW – 14/07/2014) <http://petitlien.fr/CESEnum9> <http://fcw.com/articles/2014/07/14/nist-panel-on-nsa.aspx>

Concrètement, la plupart des tests de maturité numérique sont dispensés par des établissements privés qui en font commerce. Or, la majorité des petites structures, TPE et PME, ne perçoivent pas l'intérêt de ces tests et ne les passent pas. Quand bien même elles les passeraient et repéreraient des vulnérabilités dans leurs structures, il n'est pas certain qu'elles puissent s'acquitter d'un investissement financier nécessaire à une mise à niveau de leurs pratiques.

Le CESE considère indispensable, pour promouvoir des bonnes pratiques, que la puissance publique mette elle-même à disposition de tous des outils d'auto-évaluation simples et gratuits, qui fournissent un étalon sur les bonnes pratiques en termes de données personnelles, mobilité, cloud et Big Data.

□ *Repenser le rôle des Directeurs de systèmes d'information (DSI)*

La politique de sécurité des données d'une entreprise doit concerner l'ensemble des personnes occupant des postes stratégiques dans les systèmes d'informations et le traitement de celles-ci. Cela va pour les plus grandes entreprises du directeur des données (*Chief data officer*) au directeur des systèmes d'information, sans oublier l'ensemble des ingénieurs liés au numérique et la direction générale de l'entreprise.

Souvent le directeur des données est essentiellement un fournisseur de données qu'il obtient tant en interne de l'entreprise que par des sources externes privées ou publiques. Il produit l'analyse de ces données afin de développer de nouvelles données prises « en connaissance de données ». Il est également celui qui pilote le développement d'algorithmes et l'automatisation des traitements de données. Dans les PME, la fonction de directeur de données est souvent remplie par le directeur des systèmes d'information (DSI). Certains DSI travaillent pour plusieurs PME. À ce poste, ils administrent les bases de données des entreprises mais ils sont aussi ceux qui organisent les postes en réseau à l'intérieur de l'entreprise.

Dans l'esprit de restaurer le climat de confiance qui préside à l'élaboration du futur règlement européen, **le CESE recommande que la fonction de directeur des données puisse si les conditions sont réunies inclure celle d'un directeur de la protection des données personnelles.** En tant que fournisseur de données, il est le plus à même de permettre la mise en œuvre au sein de son entreprise d'une politique de protection des données personnelles. De par sa position hiérarchique, il peut alerter la direction générale en cas d'utilisation illégale des données personnelles.

La cohabitation des usages privés et professionnels sur un même équipement est fréquente dans le monde professionnel. L'utilisation d'un seul téléphone portable par exemple pour les deux usages ne peut pas être toujours évitée. Dans tous les cas il convient de mettre en œuvre des solutions dédiées pour cloisonner efficacement chaque environnement dont il a été vérifié qu'elles répondent aux besoins de sécurité de l'entreprise d'une part et du salarié ou de l'agent public d'autre part.

De façon générale, **le CESE recommande d'encadrer l'usage de l'apport d'appareil personnel (BYOD, BYOA)¹¹¹ et l'utilisation des applications informatiques personnelles par des règles claires dont la mise en œuvre relève de la responsabilité des organisations syndicales de salariés et d'employeurs**

¹¹¹ BYOD : *Bring Your Own Device* qui signifie « apporter nos appareils personnels » ; BYOA : *Bring Your Own Application* : Utiliser ses propres applications informatiques

C'est l'occasion de sensibiliser et d'informer les salariés sur les risques de sécurité susceptibles d'engendrer des incidents critiques sur les données professionnelles. Une exigence qui doit conduire d'une part à prévoir une politique de sécurité informatique et un système de gestion de la sécurité de l'information (envisager la possibilité d'avoir recours à une norme de sécurité de l'information sur les bases des recommandations de l'ANSSI¹¹² et, d'autre part, à promouvoir la séparation hermétique, quand cela est possible, entre environnements personnels et professionnels au sein d'un même terminal.

Développer le *Privacy by design* comme facteur de différenciation compétitive

Pour lutter contre les difficultés que peuvent provoquer tous les outils dont le modèle économique repose sur le *Big Data* et la collecte massive, indifférenciée et variée des données personnelles de leurs utilisateurs, deux solutions sont envisageables. D'un côté, agir sur les utilisateurs, de manière à ce qu'ils soient plus instruits du volume et de l'usage des données qu'ils transmettent. D'un autre côté, agir sur les outils : soit en limitant leurs possibilités de collecte, soit même en les concevant de manière à ce qu'ils ne reposent pas, techniquement ou économiquement, sur la collecte d'informations.

Cela étant, même si tous les acteurs s'accordent sur l'intérêt de ce principe, son application reste pour certain complexe : notamment le *privacy by design* au-delà d'une « contrainte technique » permettant de concevoir des outils en conformité avec le principe du respect des données personnelles, est une « contrainte incompatible » avec le *Big Data*. Ce dernier défierait les principes de finalité et de proportionnalité dans la mesure où il consiste en une « accumulation sans cesse croissante de données afin d'augmenter toujours les potentialités d'exploitation et de faciliter l'apparition d'usages imprévus lors de la collecte »¹¹³.

Bien qu'en partie fondée, la critique est souvent développée pour mettre à mal les dispositifs normatifs, dans le sens voulu des détracteurs du droit et des promoteurs de la *soft law* ou autres dispositifs d'auto-régulation. Certes, répondre par une solution technique à un problème posé par une technologie n'est pas un gage d'assurance tant il vrai que la vitesse des évolutions technologiques est source d'obsolescence. **Le CESE considère toutefois qu'il ne faut pas écarter cette forme de régulation (*privacy by design*) au risque de se priver d'outils et de conceptions technologiques pouvant contribuer à l'application effective du droit.**

Le CESE considère que la protection n'est pas un obstacle à l'innovation. Elle est au contraire une exigence qui stimule la croissance de l'expertise et dans le cas d'espèce contribue dans et par la technologie à intégrer la protection juridique des données personnelles. C'est tout l'intérêt de l'approche en termes de « *privacy by design* » ou « confidentialité des données dès la conception ». Reste à savoir comment l'on peut, par exemple, intégrer dans les outils une anonymisation initiale des données, tout en évitant de priver les entreprises ou les institutions des bénéfices du *Big Data*.

La vie des objets qui nous entourent devra aussi être examinée dans la durée depuis leur conception jusqu'à leur destruction. En effet, à mesure que nos objets quotidiens seront connectés et qu'ils recueilleront des informations sur notre environnement, ils seront aussi

112 http://www.ssi.gouv.fr/IMG/pdf/NP_Ordiphones_NoteTech.pdf

113 Laurent Cytermann, rapporteur général adjoint du Conseil d'Etat, Audition rapport d'information – *L'Europe au secours de l'internet*, n°696 – Tome II, 2013-2014 – Sénat.

la cible potentielle d'attaques informatiques. Or pour la plupart, ces objets à la différence des ordinateurs ou des terminaux mobiles, ne font pas encore systématiquement l'objet de mises à jour de sécurité.

Qu'il s'agisse du recueil d'informations médicales personnelles voire de prise de contrôle à distance, **le CESE recommande que la sécurité des objets fasse l'objet d'une attention particulière. Parmi les mécanismes de sécurité de ces objets connectés, le CESE considère que deux d'entre eux devront faire l'objet de mesures d'encadrement :**

- **l'obsolescence ou la mort programmée des objets** en particulier pour les objets liés à des fonctions critiques et qui ne seraient plus « supportés » en termes de sécurité par leurs constructeurs ;
- **le droit au silence des puces¹¹⁴** : la possibilité qui devra être donnée à l'utilisateur de faire « taire » les puces et autres dispositifs interrogeables à distance afin qu'ils ne puissent communiquer des informations sans son consentement. C'est en particulier le cas pour les puces à radiofréquence (RFID) qui, pour leurs modèles les plus simples, « parlent » quel que soit l'émetteur et peuvent donc révéler des informations à l'insu de leur détenteur.

Le CESE recommande d'encadrer la maîtrise des données issues et transmises par les objets connectés en faisant de la protection des données le critère par défaut dans le réglage des paramètres d'un appareil ou d'une application. Le CESE milite pour un droit des citoyens au « silence des puces » et pour la généralisation de l'*opt-in* qui repose sur un consentement libre et éclairé qu'un accès aisé à l'information notamment via les conditions générales d'utilisation (CGU) et ou de vente (CGV) doit pouvoir offrir.

Le CESE recommande que la promotion du *privacy by design* et du *privacy by default* s'appuie sur le développement de référentiels solides en matière de protection « informatique et libertés ». L'exemple des labels produits par la CNIL et par d'autres pays européens qui se sont engagés dans des démarches similaires doit être encouragé notamment au plan européen. La création d'organismes de certification est une nécessité. Sur ce point le CESE soutient la proposition de la création d'un mécanisme de certification européen tel que proposé par le projet de règlement relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données dans son considérant 77¹¹⁵.

Promouvoir une éthique numérique au sein des entreprises et des administrations

Pour promouvoir une éthique du numérique au sein des entreprises relevant du secteur numérique et administrations, il convient de renforcer la confiance dans le numérique au sein de celles-ci, notamment dans l'usage qu'il en est fait dans le cadre de la gestion des ressources humaines.

114 *Les mutations économiques, sociales et politiques de l'Internet des objets* (Bernard Benhamou - Cahiers de la Documentation Française – décembre 2012)
<http://www.netgouvernance.org/IOT%20Cahiers%20DOC%20FRANCAISE.PDF>
<http://petitlien.fr/CESEnum6>

115 « Afin de favoriser la transparence et le respect du présent règlement, la création de mécanismes de certification, ainsi que de marques et de labels en matière de protection des données, devrait être encouragée pour permettre aux personnes concernées d'évaluer rapidement le niveau de protection des données offert par les produits et services en question ».

La plupart des entreprises investies dans le numérique se caractérisent par des marchés bi ou tri faces : d'un côté, elles développent des services gratuits, très innovants, très simples à utiliser, changeant la vie des individus (un moteur de recherche, un réseau social par exemple), d'un autre côté, elles collectent massivement des données sur les individus partout dans le monde. Enfin (et c'est la troisième face du marché), ces mêmes entreprises peuvent développer des services concurrents à des acteurs à qui ils vendent de l'espace publicitaire. L'enjeu ne concerne dès lors plus la simple gestion des données mais surtout leur interopérabilité et leur hybridité.

Il est donc nécessaire que la dimension du respect de la vie privée des individus soit partie intégrante de leur modèle économique. Cela est indispensable pour construire un modèle économique reposant sur la confiance des clients finaux. Ce modèle de confiance requiert pour distribuer ces nouvelles technologies une évaluation des risques potentiels, une information en direction des autorités et des clients et une réponse adaptée pour parer les risques.

Respecter la vie privée des salariés

Il est nécessaire également que la dimension du respect de la vie privée des salariés soit partie intégrante d'une gestion éthique et responsable.

Pour aider au développement d'une culture numérique vertueuse au sein des entreprises, le CESE recommande la promotion et la mise à jour des guides de la CNIL relatifs au monde du travail.

Le CESE recommande également que les instances représentatives du personnel puissent bénéficier de formation adaptées aux enjeux de la gestion de la protection des données numériques au sein des entreprises et que cet engagement s'étende aux données personnelles des salariés afin que ceux-ci puissent bénéficier d'une information complète en la matière.

Généraliser la désignation des Correspondants informatique et libertés (CILs)

Un levier évident pour diffuser la culture numérique dans les entreprises, et notamment l'éthique du numérique que le *Big Data* peut, dans certaines situations, mettre à mal, est de désigner, dans chaque entreprise, y compris les plus petites, un correspondant informatique et libertés. La loi prévoit déjà la possibilité pour un organisme privé ou public de nommer un « correspondant à la protection des données à caractère personnel », couramment appelé « Correspondant informatique et libertés » (CIL). Ce correspondant est chargé d'assurer l'application des dispositions de la loi à l'intérieur de l'organisme. Pour les PME et TPE, l'existence de ce correspondant est facultative. Pourtant, rendre obligatoire ce correspondant comme le propose le projet de règlement européen aurait pour bénéfice une action de prévention où ce correspondant n'aurait pas simplement une mission de contrôle mais aussi une mission de conseil, sur toutes les questions relatives au respect des données à caractère personnel. Une mise en conformité après coup est toujours complexe à gérer pour une entreprise. À l'inverse, une sensibilisation initiale à ces problématiques permettrait de diffuser des bonnes pratiques. Le caractère facultatif actuel de ce correspondant est particulièrement épineux dans le cas des start-ups, qui sont des entreprises comprenant souvent moins de cinq salariés, et pourtant susceptibles de manier des données personnelles en très grande quantité.

Ce correspondant est avant tout un facilitateur des rapports entre l'entreprise et la CNIL en termes de conformité à la loi de 1978 et un simplificateur des formalités administratives.

Mais au-delà de ces fonctions, il doit pouvoir être la preuve d'un engagement éthique et citoyen de l'entreprise en garantissant le respect de la vie privée et des droits des personnes dont les données sont traitées.

Aussi pour diminuer les risques de contentieux pour les entreprises et les administrations, pour renforcer les droits des salariés à la protection de leur vie privée, et pour faciliter les démarches administratives et déclaratives, **le CESE recommande que soient nommés dans les entreprises, dans chaque ministère, EPL et collectivité territoriale ainsi que dans les établissements hospitaliers, universitaires, et régionaux des Correspondants informatique et libertés (CIL). En ce qui concerne les TPE et les PME, tout comme les collectivités territoriales de petite taille, le CESE préconise la mutualisation des moyens afin de permettre un lissage des coûts associés au bénéfice d'un CIL présentant la disponibilité et les compétences requises.**

Bâtir une politique publique du numérique et construire une stratégie industrielle

Le développement d'une politique industrielle européenne numérique, exige une vision politique privilégiant l'innovation, la recherche, la protection des technologies, et le financement de plateformes alternatives, c'est-à-dire d'acteurs économiques pouvant rivaliser avec les entreprises américaines.

Le CESE recommande de protéger les technologies qui sont à la base de la sécurité et de la confiance sur Internet et préconise de veiller à l'indépendance des organismes chargés des normes et standards de l'internet en particulier lorsqu'il est question des dispositifs qui assurent la sécurité des échanges. Des mesures devront être prises pour éviter que les organisations chargées d'élaborer les normes et standards de sécurité sur Internet ne soient couplées (ou dépendantes) des agences de renseignement.

Développer une stratégie numérique pour les données et les technologies de l'État

La nomination récente d'un administrateur général des données doit permettre de mettre en œuvre une politique publique du numérique autour de la protection des données mais aussi des techniques de sécurisation et d'anonymisation de ces données.

L'exemplarité de l'ouverture des données publiques pourrait permettre d'essaimer les bonnes pratiques vers les entreprises privées. Le choix des technologies qui permettront l'accès aux données et aux services créés pour les citoyens pourra se révéler crucial tant d'un point de vue économique que politique. Les services publics, du fait de leur statut de premier prescripteur des technologies numériques en France mais aussi par le nombre d'utilisateurs en constante augmentation, ont un rôle essentiel à jouer dans l'accompagnement des citoyens vers une meilleure maîtrise des technologies numériques.

Le CESE préconise comme le suggère entre autres la mission commune d'information sur l'accès aux documents administratifs et aux données publiques du

Sénat¹¹⁶ d'inscrire le calendrier de l'ouverture des données publiques *Open Data*, dans les contrats d'objectifs des administrations et de définir une formation continue sur la donnée pour développer les compétences des agents en la matière.

Enfin à l'instar des choix de nos partenaires européens (en particulier allemands et britanniques), la France devra se doter d'une véritable stratégie technologique à l'échelle de l'État. Ainsi, parallèlement à la création d'un poste d'Administrateur général des données pour l'État (équivalent du titre de *Chief data officer*) et comme propose Tariq Krim dans son rapport remis au gouvernement¹¹⁷, **le CESE préconise la création d'un poste d'administrateur général des technologies de l'État CTO (*Chief Technology Officer*) afin de coordonner la « plateforme technologique France » et de valoriser le capital de technologies développées en France. Ce poste devra être directement rattaché au Premier ministre.**

L'administrateur général des technologies devrait avoir un rôle de conseil et de conception en concertation avec les institutions scolaires et universitaires chargées de former les élèves et les étudiants ainsi qu'avec les réseaux d'espaces publics numériques sur l'ensemble du territoire, afin de participer à la coordination des actions de formation liées au maniement du « code ». Des projets pourraient ainsi être mis en place à grande échelle auprès des universités et des organismes de formation afin de mettre en place des services utiles à l'ensemble des citoyens.

Etablir de nouveaux principes « *Design et ergonomie* » pour la démocratie à l'ère numérique

L'organisation des données numériques accessibles par les citoyens constitue un nouvel enjeu pour la puissance publique. En effet, s'il est toujours possible d'accéder à la partie d'un ouvrage papier que l'on sait consacrer au sujet qui vous intéresse, il en va tout autrement lorsque les mêmes informations sont disponibles en ligne. En effet, ces informations peuvent devenir inaccessibles si les concepteurs d'un site ou d'une application n'ont pas pris en compte l'ergonomie de la navigation. Cela peut ainsi mener à une situation paradoxale où des informations de plus en plus massives ne deviendraient accessibles qu'aux seules personnes ayant une bonne maîtrise des moteurs de recherche et des outils de navigation dans l'information.

En ce sens, l'ergonomie et le design associés aux données numériques, loin d'être des variables d'ajustement, deviennent des fonctions cruciales pour les architectes des systèmes d'information. À mesure que la quasi-totalité des mécanismes de transmission de l'information deviennent numériques, ces principes de simplicité et d'accessibilité des ressources numériques relèvent d'impératifs démocratiques. Il est à noter que c'est l'ergonomie des terminaux mobiles qui a pour partie permis aux personnes aux revenus les plus modestes de se connecter en particulier pour effectuer des démarches sociales comme la recherche d'emploi¹¹⁸

116 Rapport au nom de la mission commune d'information sur l'accès aux documents administratifs et aux données publiques présidé par M. Jean-Jacques Hysted, Sénateur, présenté par Mme Corinne Bouchoux, Sénatrice, juin 2014.

117 http://www.redressement-productif.gouv.fr/files/20140306_rapport_tariq_krim.pdf

118 *L'accès aux télécommunications pour tous : la parole aux personnes en situation de précarité*, étude ANSA – avril 2012)
http://www.solidarites-actives.com/pdf/ANSA_TIC_contribution_15_acces_telecoms.pdf

De plus, les spécificités actuelles des terminaux mobiles rendent souvent nécessaires la simplification des informations affichées en particulier sous forme graphique pour les données numériques. Cette visualisation des données (ou *datavisualisation*) peut à son tour devenir un facteur d'exclusion voire de manipulation des informations présentées suivant les choix « éditoriaux » des personnes qui mettent à disposition ces représentations.

Aussi le CESE préconise qu'un organisme indépendant établisse chaque année un bilan de l'accessibilité et de l'ergonomie des ressources informationnelles en vue de faciliter leurs mises à disposition des citoyens par les organismes publics. Cet organisme établira à intervalles réguliers des recommandations concernant ressources et services existants ainsi que des pistes technologiques et ergonomiques, pour les concepteurs de ressources nouvelles.

Afin de rendre accessibles l'ensemble des services dédiés aux citoyens sur les plateformes mobiles, le CESE recommande que les organismes publics qui mettront en place de nouveaux services à destination des citoyens veillent à ce qu'ils soient accessibles sur les terminaux mobiles en priorité sous forme de sites web mobiles (en particulier avec les technologies HTML5) ou à défaut sous formes d'applications natives accessibles via les principaux systèmes d'exploitation mobiles.

Développer une politique publique du numérique articulée à une politique industrielle en faveur notamment des jeunes « pousses ».

Une politique publique et industrielle du numérique doit reposer sur la nécessité de faire évoluer l'ensemble des entreprises vers une culture du numérique leur permettant de se développer au sein de ce nouveau paradigme que représente le numérique. Mais il est également essentiel de permettre l'émergence de « jeunes entreprises » dans le domaine du numérique, ce qui implique une réflexion par filières.

Considérant que l'ensemble des secteurs (industrie, agriculture, services, artisanat, associations...) est concerné par la révolution numérique et l'enjeu du traitement des données, le CESE encourage la mise en œuvre concrète de cette évolution dans les contrats de filière, pour celles consacrées au numérique mis en place dans le cadre du Conseil national de l'industrie et qui associent les organisations syndicales et les entreprises.

L'innovation n'est pas hors sol : les nouveaux produits et services rentrent dans la vie des citoyens, dans l'école, dans la rue. La captation des données d'usage ne suffit pas à rendre compte des interactions sociales complexes. Nous devons repenser la diffusion d'une culture de l'innovation et d'une culture de la donnée dans une perspective de co-construction de savoirs. Les réalisations matérielles permises par le numérique s'intègrent dans la ville et ont vocation à propager la culture numérique et sont le symbole de l'importance que l'on donne à l'innovation, à l'esprit d'entreprise, à la créativité, au retour vers le physique et le réel (machines-outils, imprimantes 3D...).

Dans la France d'après-guerre, les MJC ont été créées pour signifier l'importance de l'éducation populaire et du développement culturel. Dans les années 2010, on a créé les *FabLabs* pour signifier l'importance de l'acculturation numérique de la société. Des réseaux comme celui des cantines qui a vu le jour en 2008 contribuent à cette dynamique, tout autant que les lieux de *coworking*, privés, associatifs, municipaux, les réseaux d'innovation

ouverte et les tiers-lieux. Demain, ce seront de nouveaux espaces publics de production, d'expérimentation et de médiation associant de plus en plus tôt les citoyens aux processus de R&D et qui doivent être le reflet le plus juste de cette société. Ils seront les espaces de concertations et de décisions publiques nouvelles, devront être directement appropriables par les citoyens pour créer de véritables « agoras » de l'innovation, pour reconstruire des espaces de formation, de socialisation, d'interaction et donc de création. Ils doivent contribuer à recomposer les contours de la démocratie locale et les dynamiques territoriales en créant la rencontre, à la source d'innovations disruptives répondant à des besoins collectifs et de proximité.

Le CESE préconise d'orienter la commande publique vers la conception de services à haute valeur ajoutée sociale et environnementale. Le levier de la commande publique devra être orienté vers les PME innovantes pour favoriser le développement de projets de technologiques et de services numériques d'intérêt général auxquels les citoyens seront associés non seulement en tant qu'utilisateur mais aussi en tant que co-concepteurs.

Pour le CESE, il convient de mettre en œuvre une politique industrielle tournée vers les jeunes entreprises du numérique afin de les conforter et de les amener à se développer en faveur de l'emploi dans le secteur du numérique comme le préconisait la grande coalition lancée par la Commission européenne en mars 2013 dont les fonds doivent être abondés. Les investissements autour des 34 plans de reconquête industrielle sont pour plus d'un tiers sont tournés vers le numérique (véhicule à pilotage automatique, textiles techniques et intelligents, Big Data, *cloud computing*, objets connectés, nanoélectronique, cybersécurité...).

Le CESE préconise que des incubateurs soient présents au sein de tous les pôles de compétitivité mais également proches des universités et des communautés d'universités et d'établissements d'enseignement supérieur (COMUE), afin de renforcer les synergies entre universités, recherche et entreprises. Les incubateurs apportent un appui en termes d'hébergement, de conseil et de financement (universités, écoles d'ingénieurs ou de commerce) et c'est le cas à Paris, Nantes, Grenoble, Lyon, Toulouse...

Le CESE encourage le financement public pour favoriser des écosystèmes thématique autour de la gestion responsable des données numériques. Cela pourrait conduire à :

- **Consentir des prêts aux PME et aux entreprises de taille intermédiaire pour engager une numérisation de leur activité et une intégration plus poussée des technologies « *privacy by design* » dans leurs produits. L'enveloppe de 300 millions d'euros gérée par la Banque publique d'investissement (BPI) et l'État pourrait comme cela est prévu subventionner des prêts à hauteur de 27 millions d'euros dans le Programme d'investissements d'avenir ;**
- **Créer un écosystème favorable à l'émergence et à l'essor de *start-ups* susceptibles de devenir les champions numériques de demain.**

Ces acteurs doivent se saisir de l'effet accélérateur des dispositifs d'innovation ouverte et se construire ou se repositionner autour de l'usage et de la circulation des données. Dans ce contexte, ce phénomène est encore amplifié par les nouveaux moyens d'actions de l'utilisateur, sa capacité à accéder à la connaissance sur les données, produire lui-même des contenus et à les partager, créer de l'innovation de service et de la valeur - économique et

sociale - selon d'autres modèles. Les offres autoproduites venant concurrencer l'économie installée, le besoin d'expérimenter se fait plus prégnant.

Le CESE soutient les initiatives autour des plateformes de types concours ou challenges qui contribuent notamment à l'utilisation des données, leur normalisation et donc à la restauration des capacités d'agir des utilisateurs. Ces dispositifs répondent à des objectifs de rétablissement de la confiance, de transparence et de responsabilité, des principes clés de l'action politique, mais aussi de revitalisation de la vie citoyenne et d'émergence de nouvelles formes de participation.

Le CESE souligne l'intérêt des challenges *Big Data* coordonnés notamment par Cap Digital. La plateforme Cap Digital propose une médiation à forte valeur ajoutée entre ceux qui expriment des besoins du marché autour de leurs données, et ceux qui sont porteurs de technologies et de solutions ; elle s'appuie sur une structure assez souple pour intégrer les contextes particuliers (typologie, volume des données, modalités et rythmes du changement, partage de la propriété intellectuelle), modulant des partenaires technologiques, d'animation, des fournisseurs d'infrastructures et de données. Le pôle de compétitivité met également son expertise de mise en relation qualifiée pour rassembler grands comptes et start-ups sur des formats innovants dans le but de faire émerger des offres de services nouvelles. L'exemple du concours AACC *Cap Digital Startup Project* a associé une start-up innovante et une agence de conseil en communication sur un modèle collaboratif et a conduit depuis sa création à l'émergence de prototypes et de services innovants.¹¹⁹

La politique nationale en faveur du numérique passe également par un effort de recherche sur les enjeux sociétaux de l'économie du numérique notamment en matière de coût-bénéfices de certaines applications dans le domaine de l'énergie, des transports ou de la santé.

Alors que les géants extracommunautaires d'Internet échappent à toute régulation, le CESE considère qu'il est urgent de promouvoir l'innovation technologique comme moteur de la compétitivité de l'industrie numérique européenne et de travailler sur le rééquilibrage des obligations et des profits dans la chaîne de valeur.

Relayant l'avis du CES européen *Société numérique : accès, éducation ; formation, emploi, outils pour l'égalité*, des 9-10 juillet 2014, le CESE soutient la proposition d'encouragement des PME européennes dans le secteur du numérique et du soutien aux « jeunes pousses » autour de programmes à haut risque par exemple dans le secteur de la santé dans le cadre de la stratégie numérique.

Le CESE appelle comme son homologue européen à un « renforcement du soutien financier » et partage la déception du CES européen « concernant la forte réduction du budget alloué à la stratégie numérique pour la période 2014-2020, qui est passé d'une proposition initiale de 9,2 milliards d'euros à 1,14 milliard d'euros ».

Maîtriser les impacts énergétiques pour une meilleure protection des données

Aujourd'hui il est difficile d'avoir des données exhaustives sur les impacts des *data center*. Selon l'ONG Greenpeace, la transparence n'est pas la règle dans cette activité et,

119 (Plus de 120 projets de R&D, dont des projets collaboratifs rassemblant acteurs académiques, grands comptes et start-ups, autour de la donnée ont également été labellisés et financés par Cap Digital depuis sa création).

pour des raisons de sécurité ou de concurrence, même l'implantation des sites peut ne pas être connue. Exception faite de quelques opérateurs de premier plan, la volonté n'est pas là d'évaluer les externalités réelles de cette activité et d'y remédier. Ainsi, l'impact le plus important est lié à la consommation électrique. Greenpeace pointe dans son rapport que l'électricité nécessaire est produite en majorité à partir de charbon, entre 50 à 80 % pour les plus grosses sociétés du numérique (GAFA et autres).

Il y a là un paradoxe entre la volonté de dématérialiser au maximum pour réduire la consommation de ressources, notamment d'énergies fossiles, et ainsi accompagner la transition écologique, et la réalité du fonctionnement des *data center* qui sont à la base d'émissions croissantes de Gaz à effet de serre (GES).

Un autre impact évident est lié à l'utilisation de groupes électrogènes, fonctionnant au diesel. Ces équipements de secours doivent être testés régulièrement. Résultat, dans certaines métropoles ayant de nombreux DC, la qualité de l'air s'en ressent¹²⁰. S'y rajoute un risque d'incendie pour les résidents, lié au stockage de carburants à proximité des groupes électrogènes

Dans le domaine de l'économie numérique et de l'internet des objets les projections et les prévisions sur les besoins réels, en termes de puissance de calcul, de capacité de stockage et de communication sont difficiles. Même pour les professionnels, les chiffres en jeu sont stupéfiants¹²¹! Chaque année, la puissance des processeurs et la densité des disques augmentent, mais le volume de données à traiter encore plus ! C'est une course entre la capacité de créer de la donnée et la capacité à la stocker et la gérer.

La Commission européenne a établi un code de bonne conduite¹²² pour apporter des réponses à la consommation croissante d'énergie ainsi qu'à la nécessité de réduire les impacts environnementaux, économiques et énergétiques de cette activité. Il s'agit d'informer et de motiver les opérateurs à réduire la consommation énergétique de manière rentable sans compromettre les fonctions critiques des *data center*. Depuis 2008, 184 DC ont adhéré à cette charte, dont quelques-uns hors Europe. Les actions proposées sont très larges et couvrent le cycle de vie complet du *data center*.

Les objectifs de ce code européen, à travers l'amélioration de l'efficacité énergétique des *data centers*, sont de diminuer les émissions de gaz à effet de serre, de limiter le réchauffement climatique, de faire des économies. **Le CESE soutient ce code de bonne conduite et demande d'accentuer sa diffusion au niveau européen, mais aussi auprès de nos partenaires dans le monde. Du fait du développement très important du secteur, le CESE estime nécessaire que la Commission se donne des objectifs ambitieux d'adhésion à ce code et en assure la promotion et le suivi, notamment en proposant des indicateurs d'efficacité de ce type d'infrastructure.**

Par ailleurs, le CESE plaide pour une plus grande transparence des opérateurs de *data center* concernant leurs besoins énergétiques réels, afin que les collectivités puissent anticiper les impacts environnementaux et énergétiques sur leurs territoires, et mettre en adéquation l'offre d'électricité avec les besoins, sans pénaliser les autres activités économiques locales.

120 Glanz, *New York Times*, 22/09/2012.

121 *Idem*.

122 <http://iet.jrc.ec.europa.eu/energyefficiency/ict-codes-conduct/data-centres-energy-efficiency>
<http://petitlien.fr/CESEnum11>

Certaines mesures relèvent du bon sens et de la sobriété : augmenter la température du *data center* (gain important), la valeur recommandée par les spécialistes étant de 27°C¹²³ au lieu des 20°C habituels ; désinstaller les applications obsolètes et libérer les ressources correspondantes, comme éteindre les serveurs qui ne sont plus utilisés ; mettre en place une politique d'archivage des données avec des durées de vie précises.

D'autres sont plus en lien avec l'efficacité énergétique : renouveler les équipements anciens pour du matériel plus performant (densité supérieure, ventilation et alimentation variable) ; mutualiser les serveurs et le stockage ; utiliser un refroidissement naturel ; récupérer la chaleur produite sur le site ; alimenter le *data center* à partir de sources d'énergie renouvelable.

À ce stade, il semble évident qu'une action déterminante doit être faite en direction des utilisateurs par l'ensemble des acteurs de l'éducation au numérique pour leur apprendre que le monde virtuel a un impact de plus en plus lourd sur notre monde réel, et qu'il existe un certain nombre de bonnes pratiques pour diminuer son empreinte « énergétique » sur le web. La « liberté » a un prix, il faut pouvoir le mesurer.

C'est un véritable enjeu de citoyenneté, comme tenu du fait que la transition énergétique nécessite une gestion fine de nos besoins, et donc participe au *Big Data*.

Le CESE recommande de profiter des campagnes de sensibilisation du public aux enjeux de la protection des données personnelles, pour les informer sur les bons usages des TIC en lien avec l'efficacité environnementale. Les guides de bonnes pratiques de l'ADEME, ainsi que de certaines associations, devraient être promus dans tous les lieux de sensibilisation ou de formation des jeunes et des citoyens.

Bâtir un cadre réaliste et exigeant de protection des données à l'ère du numérique

Les révélations d'Edward Snowden et l'affaire Prism ont fait apparaître la nécessité d'un renforcement des règles visant à assurer la protection de la vie privée pour les citoyens. L'enjeu de l'équilibre entre la sécurité nationale et les libertés individuelles est un défi pour les sociétés et les Etats de droit. Cela impose de définir de toute urgence un cadre éthique universel pour redonner confiance dans l'économie numérique et sa capacité de protection des libertés. Ce constat confirme la nécessité d'accélérer les travaux de révision de la directive européenne de 1995, ceux de la modernisation de la Convention 108 du Conseil de l'Europe, et de prendre part activement dans la définition des objectifs à l'ONU où les principes directeurs « informatique et libertés », adoptés à l'unanimité par l'Assemblée générale en 1990, sont, hélas, restés non contraignants.

Bâtir et organiser la nécessaire régulation du numérique par une force, qui en dit le droit et nécessairement en limite et en réprime les abus, revient à défendre une souveraineté numérique. L'efficacité d'une telle régulation oblige à l'appréhender à l'échelle du net c'est-à-dire au niveau mondial. Cela suppose le renforcement de la coopération juridique de tous les États souverains et de tous les acteurs concernés. Cette régulation internationale doit être fondée sur l'autorité et la décision des États pour reconstituer une véritable souveraineté des

123 <http://www.greenit.fr/article/acteurs/hebergeur/data-center-quels-impacts-sur-le-territoire-5057>
<http://petitlien.fr/CESEnum12>

individus sur une technologie qui doit être maîtrisée. La réflexion d'un droit international public du numérique doit voir le jour afin de réguler les normes des conflits potentiels du numérique et d'assurer l'indépendance politique et de nos décisions individuelles.

Pour l'heure cette affirmation forte des droits fondamentaux que porte l'Europe dans le domaine des données et du numérique doit primer par rapport à la libéralisation du transfert des données voulue par les États-Unis. **Le CESE recommande que les pouvoirs publics français s'impliquent plus clairement et avec audace dans les réformes des textes européens ou de portée mondiale. Il préconise la mise en œuvre d'une véritable diplomatie du numérique.**

La France peut agir au niveau européen, en lien étroit avec l'Allemagne, afin de développer une définition de la société numérique. La France et l'Europe peuvent être leaders pour proposer une alternative de pensée par rapport au modèle américain. L'Europe, dont les ingénieurs figurent parmi les meilleurs, a aussi une culture historique de la défense des libertés individuelles, elle peut construire cette pensée d'une société numérique respectueuse des individus.

Parce que l'innovation n'est pas menacée par la garantie des droits, nous devons aller vers une innovation responsable, qui doit intégrer la préoccupation de la société.

Créer un cadre de protection des données au niveau international

La protection des données personnelles affirmée au niveau européen comme un droit fondamental de portée internationale est un pilier de la souveraineté numérique pensée et construite comme une coopération juridique et judiciaire de tous les acteurs et de leurs représentants et qui institue l'état de droit du numérique.

Cette nécessaire régulation internationale ne doit pas se substituer aux autres formes de régulation nationale elle doit pouvoir compléter la lutte contre les risques extérieurs, contre les discriminations pour l'accès du Net par une approche intégrant la dimension européenne et accompagnant les acteurs du numérique et s'ouvrant à la société civile globalisée. Nous avons, à la penser dans la coopération et l'équilibre des pouvoirs, selon des règles de justice à l'échelle de l'Europe pouvant nous permettre de bâtir les contours d'une déclaration des droits de l'Homme à l'ère du numérique.

Promouvoir un cadre protecteur au niveau international

De risque démocratique insupportable pour la vie privée de l'individu, la transparence devient le préalable indispensable de l'utilisation des données personnelles par les entreprises et les États; mais la transparence doit changer de camp aujourd'hui. L'enjeu est au contraire de faire preuve de clarté sur les données personnelles dont ils disposent, en faciliter l'accès, la traçabilité et la sécurisation.

Ce cadre protecteur pourrait se traduire par une reconnaissance universelle où l'adoption de règlements, lois et pratiques respectueuses de la vie privée s'articulerait avec une double action de sensibilisation, des acteurs publics et du législateur d'un côté, et des citoyens d'un autre côté. À titre d'exemple, lors de son forum du 19 septembre 2014, le Forum d'Avignon a publié une tribune intitulée « *Pour une déclaration préliminaire des droits*

de l'homme numérique ». Dans le paragraphe 5 de ce texte, il associe données personnelles et créations : « *Toute exploitation des données comme des créations de tout être humain suppose son consentement préalable, libre, éclairé, limité dans le temps et réversible* ». Même si cette déclaration montre une piste à suivre et est un premier pas vers l'établissement d'une charte internationale du numérique, il convient de relever qu'elle n'a pas suscité l'unanimité et ne pourrait être transposée directement en une charte, dans la mesure où, en rapprochant données personnelles et créations, elle prend aussi une position sur le droit d'auteur, une question connexe, mais qui demeure débattue. Il serait ainsi plus efficace que cette future charte ne s'appuie pas sur une position sur le droit d'auteur en vigueur qui ne manquerait, quelle qu'elle soit, d'affaiblir sa portée et sa capacité à établir un consensus minimal.

Plus récemment *The European Data Governance Forum* organisé le 8 décembre 2014 à Paris (UNESCO) s'est achevé par la présentation d'une déclaration¹²⁴ adoptée par le G29, lors de sa séance plénière du 25 novembre 2014. Par cette déclaration, les autorités de protection des données de l'Union européenne souhaitent réaffirmer les valeurs communes de l'Europe et proposer des actions concrètes pour élaborer un cadre éthique européen.

Bien que cette charte et cette déclaration ne soient pas contraignantes, elles sont néanmoins un début de réponse.

Le CESE préconise en tout premier lieu l'adhésion aux instruments juridiques internationaux existant déjà dans ce domaine, tels que la Convention 108 du Conseil de l'Europe ainsi que la négociation d'une convention internationale de la protection des données personnelles.

De plus, ces positions européennes doivent pouvoir être pour le CESE confortées au sein d'une charte internationale et à terme d'une convention qui affirme le droit au contrôle de l'utilisation des données personnelles et un droit au consentement qui en découle. Cette charte doit exiger une totale transparence de tous les utilisateurs de données personnelles et affirmer également l'intérêt général au partage de données anonymisées dans le cadre de l'open data et du *Big Data*.

Le CESE préconise que cette charte constitue une forme de « légitimité et de reconnaissance de la société civile mondiale » comme partenaire de la gouvernance d'Internet¹²⁵.

Favoriser une culture européenne du numérique garante de l'architecture du net

La neutralité du net ou la neutralité du réseau est un principe qui garantit l'égalité de traitement de tous les flux de données sur Internet. Ce principe exclut toute discrimination à l'égard de la source, de la destination ou du contenu de l'information transmise sur le réseau. Alors que les équipements techniques qui forment le réseau Internet rendent désormais possible une gestion discriminatoire du trafic, ce principe doit être garanti par la législation. Dans le cadre du *Big Data* et de l'*Open Data*, ce principe est un outil de démocratie et d'innovation. Démocratie car elle met tous les acteurs, sans discrimination, financière notamment, sur un pied d'égalité. Innovation, car la neutralité du réseau permet

124 <http://europeandatagovernanceforum.com/pro/fiche/quest.jsp?jsessionid=ms74wMFu96vxlWTyKWgCXx7.gI3>

125 Conseil économique social et environnemental, *Internet : pour une gouvernance ouverte et équitable*, étude présentée Mme Nathalie Chiche au nom de la section des affaires européennes et internationales, 2013.

une « innovation sans permis », une mise à disposition des outils à tous les acteurs sans discrimination. L'annonce de la fin du lien contractuel entre l'*Internet Corporation for Assigned Names and Numbers* (ICANN) et le gouvernement américain est un progrès vers la neutralité du net. Celui-ci doit être pour le CESE l'occasion de promouvoir une gouvernance démocratique de l'ICANN autour notamment d'une Assemblée générale rassemblant les différentes parties prenantes du monde numérique et pouvant exercer un contrôle sur le conseil d'administration.¹²⁶

Au-delà de l'encadrement juridique de la collecte des données et des pratiques liées à la surveillance, il s'agit aussi de protéger l'architecture d'internet en tant que tel via les normes et standards qui lui permettent de fonctionner (de nouveau) dans un cadre de confiance. En effet si l'internet a été jusqu'ici à même de se développer sans connaître de « crises de croissance » et qu'il est à même de résister à de nombreuses attaques sur ses infrastructures, il ne pourrait pas résister une « crise de confiance » globale¹²⁷ comme celle qui aurait pu naître à l'issue des révélations d'Edward Snowden. C'est précisément pour lutter contre cette crise de confiance que les organismes chargés de la régulation technique de l'Internet ont souhaité intervenir dans ce débat hautement politique de la surveillance de masse.

Il est à noter en effet que les organisations chargées de la régulation technique du réseau ont, pour la première fois depuis leur création, décidé de prendre part au débat politique sur la nécessité pour les États de ne pas remettre en cause l'architecture de l'internet. Cette confiance qui est la clé de voûte du fonctionnement de l'internet pourrait, si elle était durablement remise en cause, induire une stagnation des échanges et avoir des conséquences sociales, économiques et politiques considérables.

Ainsi, l'*Internet Engineering Task Force* qui regroupe de manière informelle l'ensemble des ingénieurs chargés d'élaborer les normes et standards de l'Internet a émis une « loi technique » (aussi appelée *Request for Comment*) qui décrit la surveillance de masse comme une attaque contre l'internet¹²⁸. Cependant, pour que cette « loi technique » puisse s'imposer dans les faits auprès de l'ensemble des acteurs technologiques et surtout des agences de renseignement, il conviendra d'élaborer des mécanismes internationaux de limitation des actions des États sur Internet.

En effet comme le rappelait le rapport du groupe d'experts sur la cybersécurité remis à la Maison Blanche¹²⁹, en plus d'une efficacité encore limitée, ces programmes de surveillance de masse peuvent avoir des « effets de bord » insoupçonnés sur les libertés et

126 Cf Etude annuelle 2014 du Conseil d'Etat, *Le numérique et les droits fondamentaux*.

127 Bernard Benhamou, Architecture et gouvernance de l'internet, *Revue Esprit*, mai 2006.
www.netgouvernance.org/ArchitectureEsprit.pdf <http://petitlien.fr/CESEnum13>

128 *Pervasive Monitoring Is an Attack* (RFC 7258 IETF mai 2014)
<http://tools.ietf.org/html/rfc7258> <http://petitlien.fr/CESEnum14>

129 « Notre travail suggère que les métadonnées collectées dans le cadre de l'utilisation de la Section 215 n'ont pas été essentielles pour la prévention d'attaques. Ces données pouvaient de surcroît être obtenues de manière rapide via les procédures traditionnelles. De plus, la prudence exige de remettre en cause l'idée que ce programme est efficace dans la prévention des attaques terroristes étant donné que les métadonnées recueillies ne couvrent qu'une partie des enregistrements de certains opérateurs. » *Liberty And Security In A Changing World, Report and Recommendations of The President's Review Group on Intelligence and Communications Technologies* (décembre 2013)
http://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf <http://petitlien.fr/CESEnum15>

plus généralement sur le fonctionnement même de nos sociétés¹³⁰. Cette « retenue » des activités des États vis-à-vis de leurs activités de surveillance ne doit pas se limiter à la seule remise en cause de la collecte des informations en masse (*bulk collection*) mais elle doit aussi être étendue aux activités qui ont pour objectif de modifier les technologies et les standards sur Internet à des fins de surveillance.

Pour le CESE il convient de préserver l'architecture de l'internet et ce à l'échelle internationale. Les attaques contre la sécurité et la confiance de l'internet doivent désormais être considérées comme des atteintes graves au fonctionnement de nos sociétés. Que ces attaques soient liées aux activités d'entreprises, de particuliers ou mêmes d'agences gouvernementales. **Un traité multilatéral devra être initié par la France, l'Allemagne et le Brésil qui partagent des préoccupations communes sur les libertés fondamentales et leur expression sur internet. Il devra à moyen et long terme en favoriser l'adoption par l'ensemble des pays membres des Nations unies pour préserver l'architecture de l'internet vis-à-vis des attaques dont il pourrait faire l'objet.**

Améliorer et soutenir le projet de règlement européen sur la protection des données

Le cadre européen est proche du cadre français ; la France a la possibilité de l'influencer. Or dans le cadre du *Big Data*, la majeure partie des acteurs de la collecte et du traitement n'est pas localisée en France. Il est donc fondamental, parallèlement à la sensibilisation des utilisateurs français, et à la diffusion de bonnes pratiques auprès des entreprises françaises, de développer à l'échelle internationale un cadre contraignant. Concrètement, cette amélioration doit passer par un renforcement de la coordination du G29 afin de permettre l'adoption de règlements ou lois similaires dans tous les pays européens. Par exemple, le droit à l'oubli, qui consiste pour un individu à demander et obtenir le retrait de données personnelles le concernant en ligne est un droit dont l'établissement s'est fait à l'échelle européenne, dans le sillage de la directive 95, et dont on peut envisager l'extension à toutes les données collectées dans le cadre du *Big Data*, même si ces données ne sont pas publiques.

Le CESE soutient l'approche européenne du projet de règlement sur la protection des données personnelles en tant que droit fondamental de chaque individu. Cette approche permet en effet de faire valoir un droit indéniable au contrôle de la donnée, à sa modification et à sa suppression ou à son retrait (droit à l'oubli).

Il recommande de poursuivre l'harmonisation au sein de toutes les autorités de contrôle européennes les conditions de mise en œuvre de droit à l'oubli suite à l'arrêt de la Cour de Justice de l'Union européenne concernant Google. Dans ce cadre le principe de l'application du droit en vigueur en fonction de la résidence du plaignant et la possibilité de faire appel à une autorité de contrôle unique dans chaque pays de l'Union Européenne devraient compléter le dispositif de protection.

130 « Les révélations de la NSA ont déclenché avec elles une incertitude existentielle : "tout ce que vous direz pourra et sera utilisé contre vous". Et les conséquences à long terme d'une telle destruction de l'échange informel sont encore inconnues. » déclare Geert Lovink, directeur de l'Institut des cultures en réseaux. (*Comment le logiciel nous influence* – Hubert Guillaud InternetActu, le 29 août 2014)
<http://Internetactu.blog.lemonde.fr/2014/08/29/comment-le-logiciel-nous-influence/>
<http://petitlien.fr/CESEnum16>

Le CESE recommande d'assurer un même niveau de protection dans tous les pays de l'Union, indépendamment du lieu d'établissement du responsable de traitement. L'harmonisation doit se faire en prenant en compte les meilleurs niveaux de protection dans chacun des pays de l'UE et en apportant des améliorations.

La protection des libertés et des droits fondamentaux relève d'abord de la loi. Il n'y a pas de liberté sans état de droit. Il faut toutefois encourager l'autorégulation mais cela ne peut se concevoir qu'au sein de ce cadre réglementaire sans pour autant se substituer à lui.

La modification de la directive de 95 doit avoir pour axe structurant une meilleure protection des libertés et des droits fondamentaux des personnes. Ce sont ces droits qui induisent des règles pour la libre circulation des données à caractère personnel dans le marché intérieur, et non l'inverse.

Dans cette perspective, **le CESE considère que le projet de règlement en cours de discussion doit comprendre les éléments suivants :**

- **l'application des garanties offertes par la réglementation européenne à tous les traitements** de données de personnes résidant sur le territoire de l'Union européenne ;
- **l'encadrement des transferts de données en direction des États tiers**, de sorte à assurer une protection adéquate de leur accès et à ne pas procurer d'avantage concurrentiel aux entreprises extra-européennes exerçant en Europe ;
- **la mise en place d'un guichet unique**, la simplification des formalités pour les entreprises, la possibilité pour les personnes concernées de s'adresser à leur autorité de contrôle nationale pour défendre leurs droits ;
- **la mise en place d'un mécanisme permettant une étroite coopération entre autorités de contrôle nationales** sur les décisions concernant les traitements de données personnelles.

Il convient également pour le CESE de garantir la sécurité juridique des échanges commerciaux dématérialisés et de promouvoir ainsi la confiance dans le commerce en ligne en mettant pleinement en œuvre les directives sur les droits des consommateurs et sur le commerce en ligne, pour garantir un haut niveau de protection des consommateurs ;

Sécuriser les transferts de données à l'international

Enfin, à l'heure de la mondialisation des échanges sur internet et des traitements de données, de l'externalisation informatique dans des pays ne disposant pas, le plus souvent, de législation de protection des données, la France doit promouvoir sur les plans européens et internationaux la protection des données personnelles. L'approche européenne permet également de faire valoir le principe d'encadrement du transfert ou de divulgation des données personnelles à la demande d'autorités administratives ou judiciaires de pays tiers.

L'établissement à l'échelle européenne de pratiques communes sur la collecte et le traitement des données personnelles dans le cadre du *Big Data* ne doit pas faire oublier qu'une part importante des solutions techniques de *Big Data* sont conçues et localisées sur le sol américain, donc, en dehors de l'Union européenne. Les *Binding Corporate Rules* (BCR) désignent un code de conduite interne qui définit la politique d'un groupe en matière de transferts de données personnelles hors de l'Union européenne. Les BCR doivent être contraignantes et respectées par toutes les entités du groupe, quel que soit leur pays

d'implantation, ainsi que par tous leurs salariés. Ces BCR constituent une alternative aux clauses contractuelles types puisqu'elles permettent d'assurer un niveau de protection suffisant aux données transférées hors de l'Union européenne. En ce sens, elles constituent également une alternative aux principes du *Safe Harbor* pour les transferts vers les États-Unis. Les entreprises concernées sont les multinationales exportant des données depuis leurs entités situées au sein de l'Union européenne vers des pays tiers n'assurant pas un niveau de protection équivalent à celui de l'Union européenne. Le renforcement de ces BCR est au bénéfice de ces entreprises, mais aussi, indirectement, des entreprises qui ne sont pas concernées par les BCR, mais sont concernées par le transfert de données, quotidiennement, vers des solutions ou serveurs américains, le renforcement des BCR pouvant, indirectement, servir de levier pour diffuser de bonnes pratiques jusqu'aux sociétés les plus petites.

Le CESE recommande de promouvoir les BCR comme protocole de base de transfert de données au niveau européen en permettant notamment des mesures de facilités. Le déploiement des BCR doit favoriser et harmoniser les pratiques de protection des données personnelles dans les accords internationaux prévoyant ce type d'échanges.

Il est également indispensable de développer la coopération internationale entre autorités de protection des données en définissant et en soutenant des instruments de collaboration opérationnel et efficace. Aussi le CESE suggère l'institutionnalisation du groupe européen des autorités de protection des données (G29) et le renforcement de ses moyens de fonctionnement.

Renforcer les pouvoirs de régulation et promouvoir la co-régulation

Plus que jamais, la société civile attend une CNIL qui mette en œuvre et qui fasse appliquer effectivement les principes fondamentaux de l'article premier de la loi Informatique et Libertés, selon lequel « l'informatique doit être au service de chaque citoyen. Son développement doit s'opérer dans le cadre de la coopération internationale. Elle ne doit porter atteinte ni à l'identité humaine, ni aux droits de l'homme, ni à la vie privée, ni aux libertés individuelles ou publiques ». Face à l'objectif global de faire de l'univers numérique un espace de droits et de libertés, l'individu a un rôle particulier à jouer et il est essentiel de renforcer ses droits.

A l'occasion du séminaire sur le numérique de février 2013, le Gouvernement a annoncé son intention, au cours de la législature, de déposer un projet de loi sur le numérique. C'est une opportunité pour que la protection des données et la maîtrise de leurs usages que l'activité de co-régulation et les travaux prospectifs de la CNIL soient renforcée légalement et que les moyens dédiés à ces actions soient développés.

Renforcer les pouvoirs de régulation de la CNIL

Face à l'objectif global de faire de l'univers numérique un espace de droits et de libertés, l'individu a un rôle particulier à jouer. Pour cela il est essentiel de renforcer ses droits qui peuvent d'ores et déjà être retenues à cadre européen constant. Dans cette perspective, le CESE recommande en tout premier lieu l'amélioration de la loi Informatique et Libertés de 1978, révisée en 2004.

☐ Renforcer le droit d'accès par un droit à la transparence des données

Parmi les droits actuellement reconnus, le droit d'accès apparaît comme peu utilisé, alors qu'il est « premier » en ce qu'il permet à tout individu de savoir ce qu'un responsable de traitement possède comme information sur lui. Ce droit - qui pourrait être renommé « droit à la connaissance de ses données » ou « droit à la transparence des données » - doit être rendu plus effectif. Par ailleurs, il pourrait être utilement renforcé à la fois dans son contenu et dans ses modalités. **Le CESE suggère de modifier dans son contenu, l'article 39 de la loi du 17 juillet 1978 pour donner aux individus, sur demande effectuée auprès du responsable de traitement, un accès aux informations relatives aux durées de conservation et, de manière plus systématique, sur l'origine des données.**

S'agissant des modalités, le CESE propose d'introduire explicitement, dans une logique de simplification, la possibilité pour les individus d'exercer les droits conférés par les articles 38 à 40 (opposition, accès, rectification) aussi par voie électronique. Une telle possibilité n'ouvrirait pas de risques de fraude supplémentaire, dans la mesure où l'article 92 du décret n° 2005-1309 du 20 octobre 2005 prévoit que toute demande écrite tendant à l'exercice de ces droits doit être accompagnée, pour être recevable, de la copie d'un titre d'identité.

De même, pourrait être introduite l'obligation du responsable de traitement de transmettre aux personnes une preuve de l'exercice de leurs droits afin de faciliter le régime de la preuve (par exemple, permettre aux individus, exerçant leur droit d'opposition via un lien de désabonnement, de recevoir un email prouvant l'exercice de ce droit, constitutif d'une preuve en cas de non-respect de celui-ci).

☐ La protection des mineurs

La loi de 1978 ne comporte aucune disposition propre aux mineurs, alors même que l'immense majorité d'entre eux utilisent les réseaux sociaux, et que les questions de e-réputation sont régulièrement liées à des données mises en ligne avant l'âge de la majorité.

Le CESE propose d'introduire dans la loi la possibilité d'obtenir l'effacement, notamment en ligne, de données à caractère personnel de mineurs, via l'exercice du droit d'opposition. Ce droit pourrait être exercé sur toute donnée collectée, traitée ou mise en ligne avant les 18 ans de la personne concernée. Ceci permettrait ainsi d'exercer un « droit à l'oubli » protecteur de la vie privée des intéressés, qui sont les plus vulnérables dans l'univers numérique.

☐ Simplifier les formalités et les règles applicables pour les entreprises

Dans la logique du projet de règlement et des efforts engagés par la CNIL depuis plusieurs mois, il apparaît opportun d'alléger les formalités pesant sur les entreprises.

Aussi le CESE recommande notamment de simplifier les formalités relatives aux transferts internationaux lorsque les entreprises s'engagent dans un régime de garanties substantielles : les demandes d'autorisation pour les transferts internationaux de données connaissent une forte croissance (près de 1500 autorisations en 2013). En outre, l'outil des « BCR » (*binding corporate rules* ou règles d'entreprise contraignantes), développé par les CNILs européennes, a fait ses preuves, mais ne se traduit pas par une simplification substantielle des formalités : en effet, une entreprise qui adopte des BCR doit continuer à présenter des demandes d'autorisations de transferts auprès de la CNIL, celles-ci faisant simplement l'objet d'un examen allégé. Si les BCR ne semblent pas pouvoir constituer des

autorisations de transferts en tant que telles au regard des termes de la directive de 1995, leur existence juridique pourrait cependant être consacrée dans les textes, et donner lieu à l'adoption systématique d'une autorisation unique délivrée à l'entreprise pour les transferts intervenant dans ce cadre.

Parallèlement, le CESE encourage la CNIL à poursuivre ses efforts en matière de simplification administrative par un travail de concertation avec les différents acteurs économiques concernés par l'application de la loi « informatique et libertés ». Ce travail de simplification doit permettre l'élaboration de nouveaux produits et services à la personne respectueuse de la vie privée et à mieux maîtriser les risques inhérents à une collecte et à des traitements toujours plus massifs à l'ère du numérique.

Renforcer les relations de la CNIL avec les pouvoirs publics

Les relations avec les pouvoirs publics et le contrôle des fichiers publics constitue l'un des enjeux de la loi sur le numérique. Actuellement l'article 11 4°) a) prévoit en effet que la CNIL est saisie pour avis sur « tout projet de loi ou de décret relatif à la protection des données personnelles ».

Le CESE préconise dès lors le renforcement des relations de la CNIL avec les pouvoirs publics en inscrivant dans les textes la possibilité que l'autorité indépendante puisse être saisie sur les propositions de loi. Une telle faculté offerte aux présidents des deux assemblées serait enfermée dans des délais spécifiques afin de ne pas ralentir la procédure parlementaire.

Faire évoluer les règles dans le domaine des fichiers de souveraineté

Dans le contexte « post-Prism », il est nécessaire de donner des garanties supplémentaires au public en matière de contrôle des fichiers de souveraineté. Ces fichiers (DCRI, DGSE...) sont ainsi les seuls, en France, à ne pouvoir faire l'objet d'un contrôle d'une autorité administrative indépendante. Ceux-ci peuvent en effet être, en vertu de l'article 44 de la loi de 1978, exonérés de tout contrôle de la CNIL, autre que l'examen de fiches particulières dans le cadre de l'exercice du droit d'accès indirect.

Afin que l'utilisation de ces fichiers se fasse dans le respect des droits des personnes, le CESE propose que les fichiers de souveraineté des services de renseignement puissent être soumis au contrôle de la CNIL selon des modalités tenant compte de leurs spécificités et avec résultats communiqués au seul ministre de tutelle et au Premier ministre.

Ce contrôle ne porterait que sur le respect de la loi informatique et libertés, dans les conditions de mise en œuvre desdits fichiers, et en aucun cas sur l'activité des services de renseignement.

Renforcer l'efficacité et la crédibilité de la politique de contrôle et de sanction de la CNIL

Face à certaines faiblesses et difficultés constatées, l'adaptation des pouvoirs de la CNIL, notamment en vue de renforcer la crédibilité, l'efficacité et la rapidité de sa politique de contrôle et de sanction s'impose.

Au regard de la dimension mondiale de l'enjeu de la protection des données le CESE propose que la CNIL soit autorisée à échanger avec ses homologues ces informations confidentielles, diligenter des contrôles ou initier des procédures coercitives dans le cadre de ses actions de coopération avec ses homologues non européens comme cela

est d'ailleurs le cas avec les partenaires des Etats membres de l'Union européenne en vertu de l'article 49 de la loi du 6 janvier 1978¹³¹.

Par ailleurs la procédure retenue pour la CNIL, qui distingue les pouvoirs d'instruction (contrôle, mise en demeure, désignation d'un rapporteur pour saisine de la formation restreinte), relevant des pouvoirs propres du président, et les pouvoirs de sanction, relevant de la seule formation restreinte, ont été regardés par le Conseil d'Etat comme conformes aux exigences constitutionnelles par une décision Pages jaunes de mars 2012.

Toutefois **pour éviter qu'un traitement de données à caractère personnel illégal puisse continuer à « vivre » pendant le temps de sa mise en demeure de répondre aux exigences de la loi le CESE propose d'élargir le champ du référé judiciaire pour que la CNIL puisse, de manière générale, saisir le juge des référés de toute demande tendant, notamment, à l'exécution de ses décisions de sanctions ou à la suspension d'un traitement¹³².**

Le CESE préconise également d'augmenter le montant maximal des sanctions de la CNIL : actuellement de 150 000 euros, cette somme peut être pénalisante pour de petites entreprises mais insignifiante pour les géants du numérique tels que les GAFAs. Afin de protéger les citoyens mais également les entreprises vertueuses d'une concurrence déloyale de la part d'acteurs économiques peu respectueux du cadre légal, le CESE recommande de s'inspirer du projet de règlement européen¹³³ qui prévoit une augmentation substantielle du niveau de sanction sur la base du chiffre d'affaire et de prévoir également un plafond en volume à même de garantir la proportionnalité du dispositif par rapport à la capacité financière des entités sanctionnées.

☐ *Autres points d'évolution*

Actuellement, la reconnaissance d'une éventuelle coresponsabilité liée au traitement de l'information, si elle est admise par la directive 95/46, n'a jamais été transposée explicitement en droit interne. Pourtant, elle constituerait une réponse juridique pertinente face à certaines incohérences révélées par l'articulation entre responsables de traitements et sous-traitants.

Le CESE préconise la consécration d'un statut de coresponsabilité qui permettrait ainsi de mieux refléter la réalité de l'implication de différents organismes dans la mise en œuvre d'un traitement « en chaîne ».

Enfin le CESE suggère d'introduire une disposition autorisant la CNIL à fixer une date d'expiration de ses autorisations. Cette recommandation qui répond au souci de

¹³¹ En effet, l'habilitation actuelle est limitée à ces seuls pays, interdisant ainsi une coopération administrative sur des dossiers particuliers avec des autorités tierces, y compris pour les pays reconnus comme offrant une protection adéquate au sens de l'article 25 de la Directive 95/46/CE. Une telle coopération serait subordonnée à des conditions strictes fixées par la loi, et à la conclusion d'une convention bilatérale entre autorités. Il convient de souligner que l'Autorité des marchés financiers, l'autorité de contrôle prudentiel ou l'autorité de la concurrence disposent d'ores et déjà de ce pouvoir de coopération internationale dans des conditions similaires (article L632-7 du CMF ; article L462-9 du Code de commerce, modifié par ordonnance n°2008-1161 du 13 novembre 2008).

¹³² Actuellement la CNIL a la possibilité de saisir le juge des référés, mais uniquement pour que soient mises en œuvre, sous astreinte, les « mesures de sécurité » nécessaires. La suppression des mots « de sécurité » permettrait d'élargir le champ du référé

¹³³ Il convient de rappeler que le projet de règlement à venir est en ce sens, puisqu'il prévoit une augmentation substantielle du niveau de sanction (5 % du chiffre d'affaires mondial dans la limite d'un milliard d'euros dans la version de compromis adoptée par le Parlement européen).

maintenir un degré de protection optimale au fil des évolutions technologiques ne doit pas aboutir à pénaliser les entreprises dans la poursuite de leur traitement.

Afin de répondre à l'ensemble de ses missions et poursuivre la réduction du délai de traitement des demandes d'autorisation, le CESE recommande, à l'instar de son rapport 2014 sur l'état de la France, de renforcer les moyens humains et financiers de la CNIL.

Promouvoir la prospection et la labellisation

D'autres responsables de traitements se montrent sensibles à la mise en œuvre d'une co-régulation et au développement du *privacy by design* et du *privacy by default*. Une protection des données intégrée à des logiciels et outils numériques dès leur conception, de même que le principe du consentement de l'utilisateur à l'utilisation de ses données sont déterminants dans ce travail de restauration de la confiance numérique.

Aussi le CESE préconise pour développer la corégulation notamment au sein des entreprises, de mieux faire connaître la labellisation mise en place notamment par la CNIL. En effet, une autre manière de mettre en œuvre une co-régulation profitable à tous les usagers est de labelliser les bonnes pratiques en matière de protection des données personnelles.

Le CESE préconise également que cette labellisation fasse l'objet de référentiels communs de tous les acteurs du net sur le modèle de celui établi en 2013 sur les coffres forts numériques qui exige un haut niveau de protection sur les données sensibles (santé, vie privée...), la conservation limitée des données, le transfert de données, le chiffrement et les mesures d'authentification.

La CNIL a délivré 29 labels en 2013. **Le CESE préconise que cette notion de labellisation soit accompagnée de moyens de contrôle permettant de vérifier l'effectivité des engagements des entreprises labellisées.**

La diversification des usages doit pour le CESE, à la fois permettre une réflexion sur l'utilisation des données personnelles mais aussi la mise en œuvre d'études prospectives permettant des développements industriels sectoriels. Dans ce cadre, la CNIL doit pouvoir développer sa mission d'information et d'éducation au numérique mais également sa mission prospective notamment en matière de données sensibles (santé, biométrie...)

Revoir l'encadrement des nouvelles données sensibles

Les nouvelles données sensibles sont celles dont nous percevons à présent qu'elles sont désormais susceptibles d'être données par les individus à des interfaces afin d'obtenir des services. Un des secteurs balbutiants, mais qui concentre le plus de risques, est la santé. C'est un secteur exposé car il est potentiellement très lucratif, et les individus sont d'autant plus susceptibles de céder des informations que les contreparties leur semblent désirables : mieux-être quotidien, espérance de vie. On distingue désormais entre « m-santé » (les informations strictement médicales) et « e-santé » (les informations médicales, sociales et médicales moins sensibles qui ont des incidences sur la santé des individus). À proprement parler, la « m-santé » est un secteur moins sensible, en cela que si les informations y sont plus sensibles (ce sont habituellement des informations qui ne sont partagées qu'avec votre médecin), elles sont cependant plus aisées à encadrer. En revanche, le secteur

de l'« e-santé » est plus problématique : si les bénéfices promis par le *Big Data* sont les mêmes que dans le cas de la « m-santé », notamment la prédiction (qui permet, par exemple, la prévention), les données sont gérées par chaque individu et sont donc plus sujettes, à la dispersion, et à la possibilité, à terme de la ré-identification. Là encore, la promesse du *Big Data* est si grande que la pression sur les entreprises (à accumuler des informations) et sur les individus (à transmettre des informations) est immense.

Le CESE recommande de considérer les données dites de « bien-être » issues de la collecte et de l'usage des objets connectés comme des données sensibles au même titre que les données de santé et d'imposer une normalisation européenne de la conception et de l'utilisation de ces objets.

Le CESE préconise également que des études d'impact soient menées concernant ces objets connectés et les algorithmes prédictifs qui y sont liés. Ces études évalueraient les risques pour les parties prenantes de ces écosystèmes.

Plus généralement le CESE recommande de renforcer constamment les procédures de codage et de sécurisation des bases de données de l'assurance-maladie et des autres banques de données médicales, d'assurer une traçabilité de l'accès des personnes habilitées à connaître ces données, d'améliorer la formation et la sensibilisation des personnels médicaux aux enjeux de la protection des données personnelles.

Protéger les données personnelles au sein de l'*Open Data*

L'*Open Data* consiste pour l'État, une collectivité, voire une entreprise, à mettre à disposition pour le public de certaines données qui sont en sa possession. Or, ces données peuvent être des données personnelles collectées par l'établissement qui appellent une attention particulière.

Il est nécessaire de continuer à sensibiliser tous les établissements qui adoptent une politique d'*open data* à cette problématique notamment si le nombre de ces établissements continue de croître, et que leurs moyens diminuent, notamment en raison de leurs tailles parfois modestes. Il convient alors de veiller à l'anonymisation des données et au consentement effectif libre et éclairé des usagers.

Concrètement, cela signifie que les organismes producteurs d'informations publiques ont une responsabilité, y compris du point de vue « Informatique et libertés », quand ils mettent à disposition du public ces informations, et ce quelle que soit la nature de ces informations (données à caractère personnel par nature ou par destination). En effet, « ouverture » des données ne doit en aucun cas signifier absence de contrôle et perte de maîtrise des informations ainsi mises à disposition.

Dès lors, le CESE propose de considérer que les fournisseurs et les réutilisateurs d'informations publiques ont une responsabilité conjointe en matière d'*Open Data*. Il s'agit de faire peser des obligations sur ces deux catégories d'acteurs, tout en leur proposant des solutions concrètes d'accompagnement de leurs projets respectifs.

Même si les risques d'atteinte à la vie privée ne sont pas tout de suite et directement identifiables, au vu des potentialités infinies de l'*Open Data*, il convient d'adopter une approche proactive en la matière et d'anticiper autant que possible la mise en place de projets innovants, dans une optique partenariale. En somme, il s'agit d'appliquer au cas particulier de l'*Open Data* un principe de précaution, en prévoyant dès à présent des moyens

de prévenir toute atteinte importante à la vie privée des administrés, tout autant que des moyens d'action *a posteriori* en cas de survenance d'une telle atteinte.

Le CESE recommande que les projets *Open Data* développés par les organismes publics conservent la maîtrise des données mises à disposition tout en assurant une information pédagogique des administrés sur les modalités d'accès et de réutilisation des informations publiques

Le CESE préconise également d'identifier, parmi ces informations, les données directement ou indirectement identifiantes, et d'anonymiser toute donnée, à l'exclusion des informations nominatives dont la réutilisation est expressément autorisée par une disposition législative ou réglementaire. Sur ce point il peut être recommandé, dès la production de l'information publique, de « marquer » les données à caractère personnel afin de permettre une anonymisation automatisée et donc à moindre coût.

La création d'un véritable catalogue d'informations publiques pour répertorier les catégories de données détenues et produites par les acteurs publics comme l'impose l'article 17 de la loi « CADA » pourrait être envisagé.

Concernant le droit à l'information, le CESE recommande d'informer les personnes dès la collecte de ces données à caractère personnel. Il pourrait être envisagé d'indiquer, de façon claire et pédagogique, sur quels supports et selon quelles modalités pratiques le producteur de l'information publique entend diffuser les données à caractère personnel (adresse du site internet, paramètres de l'indexation par les moteurs de recherche, exercice des droits « Informatique et Libertés », etc.).

Concernant les réutilisateurs, le CESE estime que les projets *Open Data* doivent garantir l'anonymat des informations et interdire les réidentifications de personnes.

Le CESE recommande enfin d'interdire l'utilisation des données publiques à des fins d'enrichissement d'un profil d'une personne. L'ensemble de ces obligations pourraient être intégrées dans des conditions générales d'utilisation ou dans des licences.

Afin de généraliser le recours à cet outil de régulation dans un nouveau contexte et de compléter le contenu de ces licences par de nouvelles recommandations le CESE propose que la CNIL puisse proposer des modèles types de licences, en collaboration avec l'Agence du patrimoine immatériel de l'État (APIE) et la CADA.

Rechercher les voies et moyens pour une maîtrise par les individus de leurs données personnelles

Comme le souligne Daniel Kaplan de la FING, « depuis des décennies les entreprises et les administrations se sont dotées de moyens sans cesse plus performants de capturer, retenir et exploiter les données relatives à leurs clients et usagers. En revanche les individus n'en retire rien de vraiment perceptible ; ni information, ni connaissance, ni capacité nouvelles ». Cette asymétrie est aujourd'hui, plus encore après l'affaire Snowden difficilement supportable par les individus comme par les pouvoirs publics.

La gestion des données devrait être dictée par des principes de collecte et d'utilisation, par l'intermédiaire d'un code de conduite. Dans une stratégie de communication externe,

les entreprises devraient par ailleurs communiquer sur la façon dont les données sont gérées et à quelles fins elles sont utilisées, et publier de manière transparente des indicateurs de performances évaluant la qualité de la gestion des données privées (sécurité, certification de sécurisation des serveurs).

Le CESE encourage l'exploration et le financement de procédures permettant de rendre aux individus le contrôle de l'utilisation de leurs propres données. Chaque individu doit pouvoir posséder la même information que celle dont toute entreprise du net dispose sur lui. Les acteurs économiques peuvent contribuer par une réelle transparence et une loyauté engagée notamment dans la rédaction de leurs conditions générales d'utilisation et de vente à une meilleure maîtrise des données. On peut alors imaginer différents modèles de collecte de données combinant un principe de réciprocité, où l'entreprise pourrait rendre certaines de ses données pouvant servir au bien commun avec un principe de fluidité et portabilité de ces données selon les choix de l'utilisateur du service. On peut par exemple mieux informer la personne connectée sur Google pour qu'elle comprenne comment l'analyse de ses données par le site contribue à générer de la publicité personnalisée et générée par la régie Google. La réciprocité autoriserait que cette même personne ait la possibilité d'agir sur ce processus, en lui offrant la possibilité de changer ses paramètres, ou de sortir du dispositif en désactivant la personnalisation des pubs. Une telle approche doit s'imposer progressivement à l'ensemble des plateformes numériques actuelles et à venir.

Suivant le rapport du Conseil d'État sur les libertés numériques, le CESE recommande que ces plateformes répondent à un principe de loyauté qui induit les obligations suivantes :

- Pertinence des critères de classement et de référencement mis en œuvre par la plateforme au regard de l'objectif de meilleur service rendu à l'utilisateur ;
- Information sur les critères de classement et de référencement ;
- Définition des critères de retrait de contenus licites en termes clairs, accessibles à tous, et non discriminatoires ;
- Capacité de l'utilisateur ayant mis en ligne un contenu en mesure de faire valoir ses observations en cas de retrait de celui-ci ;

En ce qui concerne les utilisateurs commerciaux, notification préalable, avec un délai de réponse raisonnable, des changements de la politique de contenu ou de l'algorithme susceptibles d'affecter le référencement ou le classement.

Comme pour l'ensemble des crises qui peuvent affecter les réseaux, les solutions apportées par la puissance publique ne pourront être « monolithiques » et devront impliquer à la fois les usagers (par des mesures de sensibilisation), les technologies (pour intégrer dès la conception de celles-ci des dispositifs de protection de la confidentialité des échanges) et enfin des mesures juridiques d'encadrement et de régulation.

Le CESE préconise de développer l'apprentissage des principes de chiffrement par les citoyens et de favoriser le développement des solutions conviviales pour rendre effectif le chiffrement des communications afin que celles-ci puissent être accessibles aux « néo-utilisateurs ».

À côté du cadre réglementaire, la co-régulation participe à la responsabilisation des entreprises pour intégrer ces préoccupations « informatiques et liberté » tout en étant pleinement conscientes des responsabilités qui seront les leurs au regard du projet de règlement.

Le CESE préconise la généralisation de tableau de bord (*dashboard*), permettant à l'internaute d'avoir accès à tout moment à une page sécurisée relevant l'ensemble des données récoltées sur lui, celles nécessaires dans le service qui lui est rendu ainsi que les données que l'opérateur s'apprête à délivrer à un tiers. Sur ces différents points et tout particulièrement sur le dernier la personne doit pouvoir exercer son consentement, pour autoriser ou pas la communication à un tiers.

Le CESE recommande également que les fournisseurs de services web permettent d'assurer le blocage de l'accès aux données d'un utilisateur lors d'une suppression de compte et de donner une option de suppression totale des données aux utilisateurs, leur garantissant la suppression pure et simple de toutes leurs données de tous les fichiers, une option permettant d'autoriser les utilisateurs à exporter les données vers un autre service.

Cette démarche conduirait à créer un droit à la portabilité des données autorisant les personnes à sortir des services, à télécharger l'intégralité de leurs données (photos, posts, mails...), de les stocker par elles-même, de les exporter vers d'autres services ou de les supprimer totalement.

Le CESE préconise également de faire de l'*opt-in* par défaut, sur la collecte et l'usage des données de profil, les suggestions, les messages, les photos, les vidéos et pour toutes les évolutions de la vie privée.

Revoir les Conditions générales de vente (CGV) et les Conditions générales d'utilisation (CGU)

Comme le rappelait Antonio Casilli¹³⁴ le *privacy by design* peut également s'entendre comme une amélioration de la compréhension des conditions générales d'utilisation ou de ventes surtout en ce qui concerne l'utilisation des données personnelles et la limitation des phénomènes de cookies (traces numériques) qui permettent une identification des personnes. Le respect de la vie privée et la restauration de la confiance de l'individu passe par cette maîtrise des données et l'établissement d'un consentement éclairé : Pour cela, il faut faire preuve de transparence et rendre plus accessibles et compréhensibles les CGV.

Le CESE préconise la mise en ligne de conditions générales d'utilisation et de vente qui permettrait clairement aux utilisateurs de donner leur consentement à l'utilisation de leurs données pour des finalités énoncées dans lesdites conditions générales.

Considérant sur ce point que les pouvoirs publics ne sont pas démunis¹³⁵ pour faire pression sur les grandes entreprises du web, le CESE recommande de soumettre régulièrement ces acteurs du net à des audits indépendants concernant l'utilisation

¹³⁴ Audition de M. Antonio CASILLI devant la section de l'éducation, de la culture et de la communication du Conseil économique social et environnemental, le 10 septembre 2014.

¹³⁵ La *Federal Trade Commission* est ainsi parvenue en novembre 2011 à imposer, dans le cadre d'un accord amiable avec Facebook, une mise sous surveillance pendant 20 ans du réseau social, qui devra se plier régulièrement à des audits indépendant concernant l'utilisation des données personnelles.

des données personnelles et de les obliger à obtenir le consentement explicite des utilisateurs lors du changement de leurs CGU.

Le CESE encourage sur ce point les initiatives permettant notamment par le biais de concours de développer un outil susceptible de repérer automatiquement d'une part les modifications des CGU et CGV et d'en comparer les versions et d'autre part les clauses qui peuvent s'avérer particulièrement dangereuses et déloyales.

Enfin, le CESE préconise le recours à des licences libres pour garantir que les contenus produits par les utilisateurs, susceptibles d'être réutilisés, puissent ne jamais faire l'objet d'une appropriation exclusive.

Cette démarche globale d'amélioration des CGU et des CGV tant sur la forme que sur le fond doit pouvoir, selon le CESE, comporter une dimension graphique, en recourant comme l'étiquette-énergie¹³⁶ à une étiquette-numérique, fiche destinée au consommateur qui résumerait les caractéristiques d'une plateforme, d'un logiciel, à la fois sur l'accessibilité et la compréhension de ses CGU, mais également sur le degré de risque en matière de protection de la vie privée et de gestion des données personnelles. Le degré de sécurité et de garanties des libertés serait évalué en termes de classes de *Respect des libertés numériques*, de la plus optimale à la moins loyale.

Le CESE soutient également le projet collaboratif *Terms of service; didn't Read* (Conditions d'utilisation ; n'a pas lu)¹³⁷ qui se propose de dispenser les utilisateurs de la lecture fastidieuse des CGU en fournissant des critères d'analyse (propriété, anonymat, export des données,...) sous la forme d'une signalétique couleur (rouge/orange/verte) selon la façon dont les plateformes respectent les droits de leurs utilisateurs.

L'enjeu des CGU est de parvenir à créer un rapport juste et équilibré entre les droits que la plateforme doit se faire céder pour fonctionner et développer un modèle économique, et les droits que les individus doivent garder pour préserver leurs intérêts. Les entreprises doivent concourir à cette recherche d'équilibre au risque de perdre la confiance de leurs clients.

Le CESE recommande d'aider à ce que les droits actuels des particuliers soient plus effectifs, ne serait-ce qu'en rendant effectif le droit d'accès, rectification, opposition, à l'oubli (art. 38 à 40 de la loi du 6 janvier 1978 modifiée). A cette fin le CESE propose que dans le cadre de projet de loi ces droits soient mobilisables en ligne, et qu'il puisse être délivré au particulier qui exerce ce droit une preuve sous la forme par exemple d'un accusé réception ou d'un récépissé.

¹³⁶ Introduit en 1992 pour la plupart des appareils électroménagers, le principe a depuis été étendu à d'autres domaines comme l'automobile et l'immobilier pour permettre au consommateur de comparer plus facilement les performances environnementales d'un produit et l'inciter à se tourner vers les moins énergivores. L'efficacité énergétique de l'appareil est évaluée en termes de classes d'efficacité énergétique notées de A+++ à D ou G. La classe A+++ est celle au rendement optimal, G la moins efficace).

¹³⁷ Projet communautaire qui vise à analyser et classer les termes de politiques de service et la vie privée des principaux sites et services Internet. Chaque aspect d'une politique de protection des renseignements personnels CGU est évalué comme positif, négatif ou neutre. Les services sont classés de A (meilleure) à E (pire) - <https://tosdr.org/> - Source Wikipédia

De la récupération au partage des données, le rôle des tiers de confiance

À terme, le partage d'informations entre entreprise et individu peut être source de progrès et d'une consommation plus réfléchie. En conservant les informations que détiennent des entreprises sur lui, chaque consommateur peut avoir accès à ses dépenses, son alimentation, son bilan carbone. On peut envisager des consommations différentes, plus respectueuses de la santé, de l'environnement. Collectivement, les consommateurs ayant les mêmes besoins peuvent alors peser sur les propositions commerciales qui leurs sont faites. L'ensemble de ces données peut également permettre la création de nouveaux services, privés mais aussi collectifs comme par exemple la gestion des données de consommation de biens et services dans une ville dite intelligente. Si un tel mouvement se met en place, les citoyens auront besoin de conserver leurs données personnelles dans des coffres forts numériques dont la nécessaire labellisation a été évoquée précédemment. Si la collecte de nos données est parfois confiée à un tiers, qui nous transmet en retour une incitation commerciale sans qu'on n'ait rien demandé, la logique de « souveraineté offensive », suppose de développer des agents intermédiaires au service des personnes. Ces agents manageurs de données personnelles assureraient une protection dans l'écosystème des données numériques et offrirait un potentiel de service très important, en tant que tiers de confiance pour aider à la communication, au transfert et à la gestion de nos données personnelles (consommation, finances, communication, formation et emploi, santé et bien être, énergie, mobilité) avec l'écosystème des services autour des données personnelles.

Le CESE recommande de suivre et d'analyser les différentes expériences en cours sur ce sujet dont le projet « Mes Infos » porté par la Fondation internet nouvelle génération¹³⁸ où l'enjeu est de redonner à l'individu la maîtrise de son « sillage numérique ».

Dans ce mouvement de réappropriation des données, le CESE propose également de réfléchir à la création de plateforme publique de type « entrepôt de données personnelles » pour assurer la gestion de données sensibles telles que les données de santé. Cette démarche devra s'accompagner de toutes les garanties en matière de sécurisation pour prévenir tous risques d'interconnexion à l'aide du numéro de sécurité sociale (NIR).

Le CESE propose également d'étudier la mise en place de régies locales chargées de conserver et de gérer les données personnelles utiles par exemple à l'amélioration des services d'une ville. Ces régies seraient administrées par l'ensemble des parties prenantes d'une ville (habitants, collectivités locales, entreprises, associations) et pourraient notamment sous le régime de l'économie sociale et solidaire participer à l'émergence de tiers de confiance.

Le CESE préconise que ces tiers de confiance soient labellisés par la CNIL et fassent l'objet régulier d'audits externes comme le suggère la Fédération nationale des tiers de confiance (FNTC).

¹³⁸ *Mes Infos*, Cahier d'exploration, FING, Mars 2013.

Déclaration des groupes

Agriculture

Le monde agricole se sent tout à fait concerné par les enjeux soulevés par l'avis. Les nouvelles technologies sont depuis longtemps présentes dans les exploitations mais aujourd'hui le mouvement s'accélère. En effet, les professionnels de l'agriculture sont de plus en plus nombreux à utiliser des technologies connectées et toujours plus adaptées à l'exercice de leur métier.

Pour la vie quotidienne d'une exploitation, nous utilisons des outils d'alerte météorologique, des logiciels de gestion des parcelles, des capteurs de vélage dans les stabulations, des compteurs d'eau intelligents. Pour mieux gérer les productions, nous avons également accès à toutes sortes de données sur l'évolution des différents marchés nationaux et internationaux, au jour le jour, offrant ainsi aux exploitants une meilleure réactivité économique.

Vous l'aurez compris, le monde agricole produit et reçoit un nombre considérable de données numériques, parfois d'importance stratégique. Les grandes firmes qui approvisionnent notre secteur l'ont bien compris, la profession agricole y est très sensible et organise des actions pour alerter les agriculteurs. Nous partageons donc tout à fait les préoccupations exprimées dans ce texte sur l'indispensable maîtrise des données.

Le groupe de l'agriculture soutient tout à fait la proposition de l'avis, d'encourager une éducation au numérique. Cette éducation doit se faire dès le plus jeune âge mais doit également être diffusée, à tous les âges de la vie. Chacun doit pouvoir être maître de ses propres données, chacun doit pouvoir être informé des risques qu'il court lors de ses connexions, tant dans ses usages personnels que professionnels.

Et surtout, il est essentiel que chacun comprenne, même de manière simple, la technologie de la production numérique.

L'éducation au numérique ne peut pas se résumer à un code de bonne conduite sur internet, ce doit être, comme le propose le texte, une matière scientifique enseignée à tous les niveaux, y compris dans les cursus de formation continue.

Le groupe de l'agriculture approuve l'ensemble des préconisations faites dans cet avis mais souhaite souligner le fait que cette évolution du numérique n'est pas toujours accessible pour les habitants du monde rural. En effet, pour des raisons de rentabilité moindre des investissements dans les zones de faible densité, les équipements sont souvent moins nombreux et plus onéreux en zone rurale.

Le groupe apprécie la nécessaire attention que méritent les zones rurales car c'est un problème essentiel. La profession agricole se mobilise d'ailleurs sur ces questions ; des partenariats entre les organisations agricoles et les opérateurs téléphoniques devraient favoriser des investissements privés beaucoup trop faibles jusqu'à présent dans ces zones délaissées.

Le groupe de l'agriculture a voté l'avis.

Artisanat

Le numérique fait désormais partie intégrante de notre quotidien et devrait à l'avenir continuer à transformer nos modes de vie et de comportements.

Cette évolution est porteuse d'opportunités considérables, liées notamment à l'essor des appareils connectés, en termes d'innovation et d'emplois, de mobilités, d'accès à la connaissance et aux soins, de gestion des consommations énergétiques etc...

Néanmoins, à côté de ces opportunités, émerge toute une série de risques liés à l'explosion de la circulation des données personnelles, et face auxquels il importe de se prémunir.

Cela appelle une meilleure maîtrise du numérique par les citoyens et les entreprises, ainsi qu'une vigilance accrue sur la diffusion et l'exploitation des données.

Afin que chacun soit partie prenante de notre société connectée, le défi est double : permettre à tous d'une part, d'accéder aux outils et ressources numériques, et d'autre part, d'en maîtriser l'usage.

Cela exige tout d'abord une politique déterminée en faveur de la couverture internet haut-débit de l'ensemble du territoire, et des établissements scolaires en particulier.

Cela implique également de déployer une éducation au numérique pour apprendre à être critique sur le contenu de l'information et comprendre le fonctionnement de ces technologies en ayant conscience des risques qui y sont liés. Cette culture du numérique doit donc s'imposer dès l'école et dans toutes les disciplines; elle doit se poursuivre dans l'enseignement supérieur quelles que soient les filières et enfin s'étendre à toutes les catégories sociales au niveau des territoires.

Il importe par ailleurs de bâtir une politique publique du numérique visant à la fois le développement de l'innovation et la protection des données collectées et utilisées par les entreprises ou les administrations.

A ce titre, il est essentiel d'encourager l'utilisation du numérique par les TPE-PME, tous secteurs d'activité confondus. En effet, ces technologies permettent non seulement d'améliorer leur potentiel de développement économique (accéder à de nouveaux marchés, optimiser les processus de production, améliorer les services aux clients, la commercialisation des produits et la communication ...), mais aussi de sécuriser leur système informatique. La numérisation de leurs activités doit donc être facilitée par des prêts de la Banque publique d'investissement. Cet appui financier s'articulerait avec l'accompagnement proposé par les chambres consulaires et organisations professionnelles.

Du côté des administrations également, le numérique est un atout, en termes de simplifications pour les usagers et d'efficacité des services.

Que ces organisations soient privées ou publiques, elles doivent mettre en place une politique de sécurité des données dont elles disposent, afin d'assurer leur performance et préserver la confiance de leurs salariés, clients ou usagers.

S'agissant enfin de la multitude de données personnelles collectées (de comportements, d'opinions...) à partir d'internet ou d'objets connectés, il apparaît essentiel de prévoir des instruments juridiques permettant de renforcer le contrôle lié à leur utilisation, alors qu'elles sont souvent recueillies à l'insu des individus et exploitées à des fins commerciales.

Le groupe de l'artisanat approuve donc les propositions de l'avis visant à développer, dans les entreprises, les bonnes pratiques et la co-régulation avec la CNIL.

Plus généralement, il partage l'objectif de construire, au niveau français comme européen, un cadre réglementaire qui devra nécessairement concilier des objectifs de protection de la vie privée avec des impératifs de sécurité nationale et d'ordre public dont l'actualité récente est venue nous rappeler toute l'importance.

Le groupe de l'artisanat a voté l'avis.

Associations

Alors que nous vivons dans un environnement où le numérique s'est développé au point d'être présent dans la plupart des aspects de notre quotidien, la question des données numériques ne s'est jamais posée de manière aussi évidente et transversale.

La navigation sur internet, le stockage de données dans le *cloud*, les objets connectés ou encore le développement des villes intelligentes sont autant d'opportunités de production et d'échange de données. Parce que l'espace numérique ne saurait se concevoir sans logiques de domination, s'y mouvoir requiert une capacité de compréhension et de maîtrise des données qui nous entourent, capacité centrale pour une participation réelle de tous à la vie économique, sociale, culturelle et politique.

Tout d'abord, concernant la participation citoyenne, l'avènement du numérique a profondément bouleversé la production, le recueil et l'archivage des données, et a transformé notre rapport à l'information. Or, face à la quantité d'informations et la difficulté à les ordonner et les analyser, on constate trop souvent des discours anxiogènes. Si la vigilance et la protection face à certains contenus sont nécessaires, il nous semble essentiel de rappeler ici, à l'instar de l'avis, que des actions d'éducation au numérique sont au moins aussi pertinentes puisqu'elles s'inscrivent dans une logique de responsabilisation et d'autonomisation des publics, quels qu'ils soient. La fracture d'usage qui touche toutes les générations doit pouvoir être diminuée par de telles actions permettant aux acteurs de mieux comprendre le fonctionnement de l'univers numérique, la part qu'ils y jouent et les outils à leur disposition pour en tirer le meilleur parti. Pour ce faire, cette éducation au numérique doit être pensée de manière transversale et au-delà de la seule approche technique.

Dans cette éducation au numérique, les acteurs associatifs occupent une place de choix. En effet, les nombreuses modalités permises par l'émergence de nouveaux types d'ateliers (tels les *coding* goûters), de lieux d'échanges et de production (tiers lieux, *fablabs*) sont autant d'exemples qui démontrent la réelle mobilisation citoyenne pour la nécessaire construction partagée de cette société numérique. Au-delà d'un simple constat, il s'agit d'un enjeu éminemment politique pour ne pas confiner les citoyens dans le seul rôle d'utilisateurs du numérique. Rendre maîtrisables et accessibles les données et les services d'internet à tous, c'est faire vivre la démocratie et combattre en faveur de l'égalité, et ce sur l'ensemble du territoire. À ce sujet, la proposition visant à renforcer les Espaces publics numériques pour en faire des lieux de proximité, de sensibilisation et de médiation dans une perspective d'éducation populaire constitue une réponse pertinente.

Donner de nouveaux moyens d'agir à tous les citoyens en termes de débat public, en leur permettant de peser sur la prise de décision (via l'e-inclusion) est également un enjeu

majeur alors qu'une partie de la population semble se détourner des modes de participation traditionnels.

Ensuite, d'un point de vue économique, l'ampleur de la valorisation des données des utilisateurs pour la publicité ou le développement de nouveaux services, ainsi que les risques avérés d'exploitation des données personnelles, ne sont plus à démontrer. Pourtant, l'innovation peut s'appuyer sur les données numériques. L'*open data* constitue ainsi une dynamique très intéressante, comme le souligne l'avis. Si là encore il convient d'être vigilant au caractère potentiellement non personnel des données, au format de leur diffusion et aux modalités de leur utilisation, l'*open data* permet, pour les acteurs qui s'engagent dans cette voie, de s'inscrire dans une logique de transparence accrue et d'être source d'inspiration pour les acteurs économiques mais aussi pour la société civile.

Le groupe des associations salue le travail du rapporteur qui a su identifier les principaux enjeux liés aux données numériques pour mieux déterminer les pistes d'action dans une perspective éducative, citoyenne et responsable. Il a voté l'avis.

CFDT

À lui seul le titre de l'avis évoque l'étendue d'une problématique qui s'inscrit elle-même dans un champ plus vaste encore. En effet, parler de données numériques renvoie à notre capacité à appréhender ce que l'on appelle communément la révolution numérique. Pour la section, l'exercice s'est avéré à la fois passionnant et compliqué.

En effet, si l'importance du sujet est indéniable, les défis que le développement du numérique posent à notre société sont immenses et complexes.

Dans ce cadre, le rapporteur a eu raison de circonscrire le sujet à la question des données numériques comme enjeu d'éducation et de citoyenneté mais l'avis n'évite pas l'écueil du trop-plein. Pour la CFDT, la question de la place et du rôle d'un rapport trouve ici toute sa pertinence.

La prise de conscience des bouleversements induits par le numérique demande à se déployer et à se diffuser plus largement dans la société. Pour ce qui concerne l'avis examiné aujourd'hui, les enjeux d'éducation et de citoyenneté sont bien ciblés mais leur traitement est trop inégal.

L'avis préconise à juste titre de renforcer l'éducation au numérique à toutes les étapes de la vie pour lutter contre la fracture numérique et sensibiliser aux bonnes pratiques, déroulant de fait le fil d'une éducation à la citoyenneté dans une société numérisée. Les pouvoirs publics à commencer par l'Ecole doivent en effet développer leurs actions, tout comme les structures associatives qui contribuent à favoriser un usage innovant et responsable des données numériques. Toutes les organisations de la société civile, dont les syndicats et les entreprises, ont le devoir de s'impliquer dans cette démarche, chacune dans son champ professionnel pour la prise en compte et l'anticipation des mutations.

Dans la seconde partie, concernant les données numériques enjeu de citoyenneté, la sensibilisation des citoyens mais aussi des entreprises et des pouvoirs publics à l'égard des enjeux liés à la production et l'exploitation des données publiques ne donne pas suffisamment de perspectives stratégiques.

En effet, le mouvement d'*open data*, c'est-à-dire l'ouverture et le partage des données publiques offre des opportunités nouvelles pour l'action citoyenne, de même la création

récente de la base de données unique dans l'entreprise doit contribuer à promouvoir un dialogue social de qualité et donc contribuer au développement de la démocratie sociale.

L'avis préconise à juste titre d'utiliser le levier réglementaire, de mettre en œuvre un cadre de protection des données personnelles et de renforcer les pouvoirs de la CNIL. Pour la CFDT, il faut autre chose à côté de la loi. Il faut une régulation des usages par les citoyens eux-mêmes. C'est par la co-régulation que les individus pourront participer à la maîtrise de l'utilisation de leurs données personnelles.

Dans une société où les outils numériques prennent de plus en plus de place dans nos pratiques quotidiennes, où chacun recherche l'information tout de suite tout en exprimant le besoin d'une plus grande maîtrise de leurs données personnelles, l'apprentissage du monde numérique est un enjeu de démocratie majeur qui implique une prise de conscience individuelle et collective.

Cet avis y contribue et malgré les quelques réserves exprimées, la CFDT l'a voté

CFTC

Faire progresser la société vers l'usage massif du numérique consistait, il y a quelques années, à doter le plus possible de personnes d'ordinateurs connectés à internet. On s'émerveillait de voir les plus jeunes manifester une grande dextérité dans le maniement du numérique. Mais la « *petite poucette* » de Michel Serres est depuis devenue un objet d'inquiétude. C'est le propos de cet excellent avis qui, fort heureusement, sait aussi discerner les aspects positifs des « progrès » du numérique.

La CFTC considère que l'usage du web et de réseaux sociaux nécessite l'urgence d'une éducation scolaire insistante. On s'exprime sur *facebook*, mais aussi on s'y expose jusqu'à la dépossession de son identité, car ce que j'écris sur le « mur » des autres ne s'efface pas à ma discrétion. De plus, le réseau d'amis est quasi infini et je ne sais jusqu'où peut aller mon message.

Dépossession aussi de la diffusion des œuvres artistiques ou scientifiques, dépossession encore du discernement des bonnes adresses du web. Le web 2.0 met nos jeunes en relations interactives aussi bien avec les « *Je suis Charlie* » qu'avec les réseaux manipulateurs de tous les extrémismes.

L'avis insiste davantage sur la dépossession à son insu de ses données, récupérées par les GAFAs (Google, Apple, Facebook, Amazon) et remixées dans des logiciels propres au *big data* pour soi disant les mettre à notre service (connaître nos besoins pour les satisfaire) mais surtout pour le marketing des divers marchés. La violation de la vie privée est le sport favori du numérique.

L'avis se penche avec pertinence sur des canalisations, régulations, voire interdictions. Mais il est conscient que face à la puissance informatique et financière des GAFAs, les États sont souvent mis en échec.

Les services de Google semblent pour l'essentiel gratuits. En effet, nous en sommes pour la plupart restés à l'idée que les services se paient avec des avoirs. Mais c'est avec de l'être, notre être intime, que se paient les services des GAFAs et non avec de l'avoir monétaire. Nous payons en donnant sans trop le savoir des données multiples, précieuses et massives dont le flux a une grande valeur marchande pour les multinationales qui les brassent afin d'en dégager les rationalités nouvelles de nos comportements. Pour la CFTC, ce passage de

l'échange par nos avoirs à l'échange par nos êtres est une atteinte industrielle à la dignité de la personne humaine qui s'apparente à une nouvelle traite des êtres humains.

Notre aliénation est telle que les ordinateurs qui organisent les milliards de milliards de données, le font, comme le dit l'avis, par des calculs de probabilités et non par déduction cartésienne.

Ainsi, par exemple, les études de l'INSEE et de l'OCDE traitent souvent les données dans cette méthode probabiliste et personne par ailleurs ne vérifie leurs calculs (car sinon à quoi servirait la vitesse de traitement des ordinateurs ?). Et ces instituts servent de prospective aux politiques économiques des Etats et des entreprises !

Heureusement la perspective de l'interconnexion des objets (web 3.0) ouvre des horizons positifs sur des diagnostics et des thérapies instantanés de chaque personne en particulier.

Le numérique peut le meilleur et le pire, mais le pire, pour la CFTC, est que l'homme soit instrumentalisé et perde la maîtrise de son destin.

Même si tout n'est pas résolu quant à l'avenir du numérique, cet avis ouvre les bonnes questions et les bonnes pistes : la CFTC l'a voté.

CGT

La CGT tient d'emblée à souligner la pertinence de l'argumentation et des préconisations. Le rapporteur a su refuser le piège technophobe sans pour autant sombrer dans la technolâtrie : opportunités et risques font donc l'objet d'un traitement équilibré ; nous vivons bien un changement de paradigme : le consommateur devient producteur de données qui doivent être protégées et les modes d'éducation, les formes de souveraineté et de citoyenneté sont transformés.

Le groupe de la CGT insiste sur trois points.

Le premier porte sur la lutte contre la fracture numérique sociale et territoriale. C'est toute la société qui doit être éduquée : du plus jeune âge jusqu'aux séniors, car il s'agit bien d'un enjeu d'émancipation, de capacité à maîtriser son environnement et donc d'agir en citoyens éclairés. Nous approuvons vos préconisations sur l'éducation au numérique de l'école à l'université, dans la cité, sur les territoires, tout au long de la vie et sur la redynamisation des espaces publics numériques mais nous restons dubitatifs sur les moyens qui vont être réellement consacrés à ces objectifs : lutter contre la fracture numérique d'équipement et d'usage en marche qui touche particulièrement les milieux populaires et les personnes en situation de précarité nécessite une volonté et des politiques publiques très ambitieuses : on a vu ici même à travers deux avis que l'école était devenue plus inégalitaire encore ces quinze dernières années ; vous pointez d'ailleurs bien le risque de l'exclusion numérique lorsque vous dites la nécessité « *d'une action publique continue et globale* ».

Le second point traite du partage de la valeur : les géants du net captent l'essentiel de la valeur en marchandisant les données personnelles : les quatre GAFAM pèsent l'équivalent des 40 entreprises du CAC 40 ! Ils ne peuvent plus échapper à toute régulation et doivent contribuer fiscalement tout comme les *data brokers* dans les Etats où ils agissent ; en effet, les distorsions fiscales en cours pénalisent fortement les entreprises françaises et européennes.

Le troisième point s'intéresse à la protection des données et à l'exercice des libertés : si les réseaux numériques accélèrent les échanges et le partage d'informations, le risque d'une

intrusion dans la vie privée existe car avec les objets connectés, nos comportements, nos préférences jusqu'aux détails de notre vie sont captés ; nous ne pouvons pas nous contenter d'une simple autorégulation, nous devons mettre en œuvre une véritable politique publique du numérique au plan national, européen et international : régulation par la protection intégrée de la vie privée dès la conception du logiciel (*privacy by design*), droit des citoyens au silence des puces, etc. tout en restant vigilants sur la tendance de certains États à censurer ou réduire la transparence. Dans l'entreprise, nous sommes d'accord avec les préconisations sur la formation des instances représentatives du personnel sur les enjeux de la gestion de la protection des données.

Le groupe de la CGT a voté favorablement l'avis.

CGT-FO

Les événements qui ont frappé la France ces derniers jours témoignent de l'équilibre fragile sur lequel repose notre démocratie. Liberté d'expression, liberté de la presse, laïcité, sont des fondamentaux qui ont été mis à mal.

Cet attentat tragique rend l'avis que nous avons examiné aujourd'hui d'une grande acuité, que ce soit en termes de surveillance des activités réalisées dans un univers aux enjeux bien réels, que de protection des données personnelles.

Nul ne pouvait anticiper le déluge de données auquel nous sommes collectivement confrontés. En effet, aujourd'hui, il nous suffit de quelques minutes pour produire autant d'informations que durant plusieurs millénaires, sans pour autant nous inquiéter de leurs répercussions, ni de leur véracité. Pourtant, des événements tels que l'affaire PRISM ou les révélations d'Edward Snowden ont fait prendre conscience de l'hyper-surveillance en cours sur les réseaux, cela justifiant pour FO la plus grande prudence et la nécessité pour l'État de se positionner en garant des libertés fondamentales.

Pour FO, ainsi que le souligne l'avis, cette asymétrie de l'information entre les grands opérateurs d'Internet et les citoyens-utilisateurs réside majoritairement dans un défaut de sensibilisation permettant à chacun de mesurer pleinement les opportunités ou les risques induits par ses actions.

Dans une période de crise où les inégalités sont croissantes, les disparités de formation au numérique accroissent les fractures qu'elles soient territoriales ou générationnelles. Il est donc nécessaire, comme le préconise l'avis, que l'État favorise l'accès à Internet sur l'ensemble du territoire, en particulier dans les zones rurales et périurbaines, et mette l'accent sur le soutien à l'éducation au numérique.

Pour FO, face à la domination des acteurs économiques notamment américains et à la captation de la valeur produite en France qui en découle, la question de l'indépendance économique et politique est posée. Sans offre de notre part, c'est à la fois des pans entiers de nos industries qui en souffriront et une approche de la gestion des données à l'opposé de nos exigences éthiques qui l'emportera, avec des risques en matière notamment d'atteintes à la vie privée dont nous apercevons seulement les prémices.

Pour FO, les besoins de confiance, de sécurité et de protection des citoyens créent des exigences nouvelles pour les entreprises et les administrations. FO partage donc la préconisation de l'avis visant à construire un cadre collectif juridique et éthique à cet

écosystème numérique qui soit en mesure de garantir à tous les acteurs les mêmes droits et une défense effective de leurs libertés.

L'avis a le mérite d'alerter l'ensemble des pouvoirs publics d'estimer à leur juste niveau les enjeux du numérique en insistant particulièrement sur la nécessité de protéger les droits fondamentaux en ligne et hors ligne. Parce que le groupe partage l'ensemble des préconisations de l'avis et face au travail considérable effectué par le rapporteur, il votera ce texte sans réserve.

Coopération

De même qu'internet a bouleversé les modes de communication entre individus, la manière dont la société traite l'information se trouve radicalement transformée. Sur les cinq dernières années, le stock d'information généré a atteint un niveau équivalent à celui accumulé au cours des 50 années précédentes. Site web, réseaux sociaux, objets connectés, media, météo, satellite, les sources et la nature des données se multiplient, tout comme les dispositifs de traitement. Cette révolution numérique génère opportunités et risques.

L'avis souligne ainsi les risques engendrés par ce nouveau paradigme, sur notre vie privée bien sûr, mais également sur notre libre arbitre et nos choix individuels, face à une « dictature » potentielle de la prévision. Les risques sont également économiques avec un impact possible sur la liberté d'entreprendre du fait d'une concentration autour d'un ou plusieurs acteurs prééminents et sur le droit de la propriété intellectuelle. Le groupe de la coopération soutient l'ensemble des propositions qui vise à construire une véritable culture numérique, via l'éducation et la formation et une protection des données efficace. Le développement d'une offre de formation couvrant l'intégralité de la chaîne de métiers reliés au *Big Data* est essentiel.

Pour le groupe de la coopération, notre pays doit saisir les formidables opportunités générées par le numérique. Santé, industrie, commerce, marketing, le *Big Data* se développe partout et génère des mutations importantes. La section de l'aménagement durable du territoire travaille d'ailleurs actuellement sur la révolution numérique dans le secteur des transports. Dans le secteur agricole, la montée en puissance de l'agriculture de précision s'appuie en particulier sur l'observation satellitaire pour connaître et agir avec précision sur l'état des cultures, analyser les phénomènes climatiques, gérer les prévisions de récoltes et les marchés. En France, Invivo, première union de coopératives agricoles veut créer le champion français du *Big Data* agricole en fusionnant les données de ses 241 coopératives adhérentes dans une même société. La coopérative vient d'être sollicitée par le ministère de l'Agriculture pour fédérer les *start-up* du secteur. Cela va dans le sens de la proposition de créer un écosystème favorable à l'émergence et à l'essor de *start-up* susceptibles de devenir les champions numériques de demain.

La révolution numérique impacte la politique industrielle qui doit reposer sur une dynamique de l'innovation et de l'entrepreneuriat, ainsi que la capacité à croître vite et à l'international. Au regard des défis à relever, le groupe de la coopération partage pleinement la proposition d'intégrer les enjeux numériques dans les contrats de filière. Cela passe notamment par la mobilisation des crédits de la BPI sur les enjeux du numérique en appui notamment aux PME, comme cela est proposé.

L'avis pointe les enjeux liés au numérique qui sont autant sociétaux et économiques, que politiques et stratégiques.

Le groupe de la coopération a voté en faveur de l'avis.

Entreprises

Avant toutes choses, Monsieur le Rapporteur, nous tenons à souligner la qualité de votre travail sur ce sujet vaste et pointu et vous remercier de votre écoute aux propositions de notre groupe.

Néanmoins, celui-ci s'interroge sur la pertinence de cet avis s'agissant de sa forme, à savoir que sur un sujet si complexe, la section aurait dû faire œuvre de pédagogie en proposant un texte plus resserré, précédé en amont d'un rapport qui aurait permis de poser un constat partagé; dès lors, il lui aurait été plus aisé de formuler des préconisations fortes et concises, l'objet de l'avis.

De surcroît, plus que dans d'autres occasions, nous aurions apprécié que cet avis volumineux comporte une synthèse qui aurait permis une lecture plus aisée à ceux qui veulent aller à l'essentiel.

Ceci étant dit, le groupe des entreprises partage l'essentiel des éléments du constat que vous avez fait. Il est clair que la question du stockage et indirectement celle de la protection des données numériques nous concernent tous en notre qualité de citoyen.

S'agissant des préconisations de l'avis, le groupe des entreprises souhaiterait en aborder quelques-unes sous l'angle des entreprises.

Disons-le d'emblée, l'affaire Snowden ne doit pas être un raccourci pour jeter l'opprobre sur les entreprises en général. Les entreprises françaises sont très rigoureuses dans la gestion des données numériques. Or, faire accroire ainsi que le texte le suggérait dans sa version initiale que le numérique peut être un instrument de surveillance des salariés pour nombre d'entreprises n'était pas admissible et vous l'avez bien compris Monsieur le rapporteur.

Nous préférons, comme le suggère le rapporteur, qu'il y ait une information objective des salariés, voire des formations adaptées des instances représentatives du personnel aux enjeux de la gestion de la protection des données numériques. Car dans ce domaine c'est par de la pédagogie que nous sensibiliserons l'ensemble des acteurs de l'entreprise à l'importance de la préservation des données numériques.

La CNIL préconise que dans chaque entreprise soit nommé un Correspondant Informatique et Libertés compte tenu de la complexité des sujets. Certes l'intention est louable et c'est déjà une réalité dans quelques grandes entreprises. Mais gardons-nous d'en faire une obligation pour les petites et moyennes entreprises et que celles qui souhaitent nommer un CIL puissent partager cette fonction avec le titulaire d'une autre fonction RH ou juridique par exemple pour une meilleure optimisation des ressources.

Dans le même ordre d'idée, et même si la protection des libertés et des droits fondamentaux relève d'abord de la loi, nous soutenons les propositions de la Commission visant à encourager les initiatives en matière d'autoréglementation (codes de conduite). Car une fois de plus, à vouloir tout régir par la loi, on rajoute de nouvelles contraintes au fonctionnement des entreprises.

Or, nos PME/TPE ont elles aussi besoin d'une réelle sécurité qui n'est pas aujourd'hui toujours à leur portée.

Le groupe ne peut s'empêcher de revenir sur l'amalgame qui est quelques fois fait, à tort, entre le comportement des GAFAs et celui des entreprises françaises.

Notre groupe a exprimé des réserves concernant la préconisation qui consiste à augmenter le montant maximal des sanctions de la CNIL et à les indexer sur le chiffre d'affaires. Nous avons fait prévaloir, ainsi qu'il a été dit précédemment, que les entreprises françaises pour l'essentiel sont vertueuses en matière de traitement de données à caractère personnel. Il conviendrait donc de ne pas les assimiler aux géants américains du numérique notamment. Nous vous remercions, Monsieur le Rapporteur, d'avoir précisé cette différenciation.

Enfin pour conclure le groupe des entreprises tient à rappeler qu'il est essentiel de trouver l'équilibre entre la sécurité des citoyens et la protection de leurs données personnelles.

Le groupe des entreprises a voté favorablement l'avis.

Environnement et nature

La question des données numériques est perçue comme un véritable enjeu économique, avec bien sûr des implications sociales et environnementales, mais son impact sur les enjeux de gouvernance, de transparence et de citoyenneté pose question. Le développement du secteur numérique s'est fait sans cadre réglementaire adapté. En s'affranchissant des frontières, il bouleverse et continuera de bouleverser nos habitudes, notre manière d'être en société, accélère la mondialisation, offre de nouvelles opportunités, mais aussi fragilise les droits de l'individu, et est source de nouvelles inégalités.

En préalable, une question de forme : le format très long de cet avis risque d'être un frein à sa diffusion dans la société civile. Nous le regrettons car il aurait fallu se donner les moyens de rendre accessible à tous la richesse du contenu de ce travail.

Le groupe environnement et nature se retrouve cependant dans la plupart des propositions. Nous retenons particulièrement celles qui vont dans le sens de la sensibilisation de tous aux enjeux positifs et négatifs du numérique comme développer l'esprit critique du citoyen vis-à-vis de toutes ces innovations ou réduire la fracture numérique d'accès mais aussi d'usage. L'exploitation de données numériques pertinentes va devenir incontournable pour tout ce qui a trait au développement durable. On pense notamment à l'évolution de nos modes de consommation et de transport, la protection de la biodiversité ou la lutte contre les changements climatiques. Pour autant, les politiques de confidentialité, et les réglementations en vigueur ne nous protègent pas suffisamment d'une captation privée de toutes ces données personnelles. Beaucoup reste à faire dans ce domaine.

Le groupe environnement et nature estime que la question de la citoyenneté et des débats de société n'a pas été suffisamment prise en compte d'une manière globale. Aujourd'hui, le développement de l'économie numérique se fait essentiellement au fil des innovations et des opportunités, et non au regard des services rendus à la collectivité. Ainsi, le développement d'applications numériques, sans prise en compte des besoins réels des populations et de leur capacité à s'approprier les outils, nous semble une erreur. Le groupe environnement et nature regrette que la mise en place préalable de débats publics de qualité sur l'évolution de notre vivre ensemble afin d'enrichir la réflexion et la décision politique, n'ait pas été retenue. Restaurer la confiance des citoyens et des consommateurs, qui est le fil rouge de cet avis, sera à ce prix !

En remerciant le rapporteur pour ce travail enrichissant et captivant, et malgré les réserves émises, le groupe environnement et nature a voté cet avis.

Mutualité

La révolution numérique liée à une explosion du volume des données est une révolution culturelle et économique qui peut avoir des conséquences politiques et démocratiques considérables si elle n'est pas maîtrisée et encadrée.

Il est indispensable de promouvoir une éducation au numérique. Cette éducation, qui doit toucher tous les âges et tous les publics, doit permettre non seulement de favoriser l'acquisition d'une éducation à l'esprit critique mais également de maîtriser les techniques numériques.

Ainsi, aujourd'hui, Netflix ou Amazon menacent la diversité culturelle car ils ne proposent que les œuvres les plus consultées ou achetées.

La question de la fracture numérique est également essentielle pour le groupe de la mutualité, car cette révolution numérique ne sera un progrès que si elle est partagée par tous. Cette fracture est à la fois sociale, territoriale et générationnelle. Les préconisations de l'avis répondent à cet enjeu.

La protection des données personnelles est devenue un véritable enjeu de société ; l'exemple des données de santé est à ce titre révélateur.

S'il faut en effet renforcer le contrôle et la protection dans l'utilisation des bases de données, l'ouverture des données publiques aux acteurs de la société civile pourrait renforcer notre système de santé. Trois raisons y poussent : améliorer les connaissances sur la prise en charge sanitaire de la population pour la rendre plus performante, satisfaire l'exigence toujours plus forte de transparence sur l'action publique et permettre la création de nouveaux services, et donc de nouveaux emplois, en valorisant ces données.

La capacité de la société civile à tirer le meilleur parti de ce capital immatériel collectif que constituent les données de santé publique est réelle et pourrait jouer un rôle majeur, notamment d'alerte, dans le domaine de la santé dans notre pays. Les derniers scandales sanitaires en sont malheureusement pour les victimes des exemples concrets. Ils ont démontré qu'il importait qu'un large panel d'acteurs ait accès aux données de santé publique dans l'intérêt des citoyens.

Pour le groupe de la mutualité, l'analyse des données de santé anonymisées est la clé pour mieux comprendre et améliorer notre système de santé, réduire les inégalités tarifaires, les inégalités d'accès aux soins et identifier les pratiques les plus efficaces pour les patients. C'est pourquoi, il est indispensable de confier la gouvernance des données de santé à un acteur indépendant.

Or, alors que la société civile est aujourd'hui présente au sein de l'Institut des données de santé (IDS), créé en 2004 pour favoriser l'accès aux données de santé publique, le projet de loi de santé prévoit de confier la gouvernance et l'hébergement des données de santé à la CNAMTS. Pour jouer véritablement son rôle, ce dispositif doit être piloté par un acteur indépendant (qui ne serait pas à la fois producteur et organisateur de ces données) et laisser une place réelle à l'ensemble des acteurs impliqués – assurance maladie et pouvoirs publics, mais aussi complémentaires santé, professionnels de santé, associations de patients...

Enfin, s'il faut anticiper les risques de l'*open data* par l'éducation de tous en renforçant les pouvoirs de régulation, le groupe de la mutualité s'interroge sur la place du facteur humain, de la curiosité et du hasard dans un monde qui serait géré par des algorithmes.

Le groupe de la mutualité a voté en faveur de l'avis.

Organisations étudiantes et mouvements de jeunesse

L'avis met en avant les progrès permis par le numérique et l'immensité des opportunités ouvertes par les nouveaux moyens dont nous disposons désormais, qu'il s'agisse de fonctionnalités techniques ou de l'amélioration de nos connaissances par le traitement des données. Dans le domaine de la santé, de la maîtrise énergétique, de la gestion des mobilités, ou encore de l'économie collaborative, les apports du numérique sont indéniables, et notre groupe se félicite que l'avis en ait fait une présentation équilibrée.

Ces évolutions s'accompagnent cependant de nouveaux risques et nous imposent de repenser la protection de nos libertés en tenant compte de ces nouveaux paramètres. Si l'*open data* a pu participer à un mouvement de relative transparence de nos institutions, les données collectées d'une façon générale peuvent également entrer en confrontation avec la liberté de maîtrise de nos données personnelles et de protection de notre vie privée. Les données numériques peuvent également être sources de détournements quand elles sont récupérées dans le cadre des dérives consommatrices et sécuritaires de notre société.

Dans ce contexte, l'éducation aux usages du numérique apparaît comme un des principaux piliers et l'avis en fait le cœur de ses préconisations. Nos modes de vie d'une façon générale et notre marché du travail plus particulièrement, sont et seront largement transformés par l'économie de la connaissance. Aussi la maîtrise du numérique et de l'ensemble de ses usages doit-elle impérativement faire partie du socle commun des citoyens. Nous soutenons les propositions de l'avis relatives au renforcement de l'éducation au numérique au sein de l'éducation nationale et de l'enseignement supérieur par l'irrigation de l'ensemble des disciplines du parcours scolaire. Au-delà des enjeux d'équipement, l'avis montre bien l'importance de former les enseignants au couple numérique/pédagogie.

Enfin, il nous paraît important de briser le mythe des *digital natives*. La réduction de la fracture numérique, que l'avis appelle de ses vœux, concerne également les jeunes, qui, s'ils sont certes nés avec les outils numériques, n'ont pas pour autant la science infuse. À cet égard, nous souhaitons souligner le rôle des associations et de l'éducation populaire. Des expérimentations sont également en cours au sein de missions locales d'insertion pour améliorer la littératie numérique des jeunes, ces initiatives doivent être encouragées et favorisées.

Le groupe des organisations étudiantes et mouvements de jeunesse a voté en faveur de l'avis.

Outre-mer

À l'heure du *big data*, l'avis met en évidence l'importance des enjeux auxquels nos sociétés sont aujourd'hui confrontées dans la valorisation et l'utilisation des données numériques.

En matière d'éducation au numérique et de protection des données personnelles, beaucoup reste encore à faire au niveau national et européen pour bâtir un véritable cadre juridique réaliste et adapté.

Mais, d'une certaine manière, il s'agit là de réflexions qui concernent les sociétés parfaitement intégrées et connectées au numérique et au très haut débit. Ce qui est encore très loin d'être le cas aujourd'hui dans les outre-mer !

Pour rappel, en 2012, seuls 5 à 20% des foyers ultramarins bénéficiaient du haut-débit, à des tarifs parfois scandaleux et en tout cas bien plus élevés que dans l'hexagone !

Cet avis nous donne donc l'occasion de rappeler que la fracture territoriale numérique est malheureusement une réalité et un frein quotidien au développement des collectivités ultramarines alors que le numérique est un extraordinaire moyen de briser un handicap structurel de l'Outre-mer extrêmement pénalisant, celui de l'isolement et de l'éloignement.

La suppression des distances permise par le développement des échanges numériques est, en effet, une grande chance pour les Outre-Mer confrontés à cet isolement et cet éloignement.

Il s'agit là d'un puissant et incontournable vecteur de continuité territoriale.

La mise en œuvre du très haut débit fixe et mobile est un élément primordial pour la compétitivité de nos appareils productifs et le développement des collectivités ultramarines avec notamment l'émergence de la télémedecine, téléformation, télé administration etc.

Dans ce domaine, le retard important en termes d'infrastructures rend nécessaire un engagement des pouvoirs publics par notamment un soutien fiscal aux investissements et une volonté au niveau local d'encourager un certain nombre de projets. Outre-Mer, dans ce secteur du désenclavement numérique, il y a urgence à agir !

Le groupe de l'Outre-Mer félicite le rapporteur pour la qualité de son travail et la clarté de son exposé. Partageant l'ensemble des préconisations formulées dans l'avis, il l'a voté.

Personnalités qualifiées

M. Aschieri : « Je tiens à remercier notre rapporteur pour nous avoir entraînés dans ce travail où, comme la plupart d'entre nous, j'ai beaucoup appris et qui a fait avancer notre réflexion collective sur un sujet qui est à la fois d'actualité et relativement inhabituel pour notre assemblée. En votant ce texte nous allons donner une bonne illustration de notre mission de réflexion prospective.

Dans cet avis très riche, je souhaite mettre en avant trois aspects importants à mes yeux. D'abord son analyse équilibrée des potentialités et des risques : ne cédant ni à un optimisme béat ni à la tentation d'un repli frileux, il fonde sa démarche sur la défense des droits, il fait des propositions qui à la fois postulent et montrent que l'innovation n'est pas contradictoire avec la protection et il avance une notion selon moi fondamentale, celle d'éthique du numérique, qui vaut autant pour les entreprises que pour les administrations.

En second lieu, j'apprécie le fait que, tout en proposant des mesures législatives et réglementaires visant à créer un cadre nouveau de protection, il met l'accent sur la nécessité de donner à l'utilisateur les moyens d'exercer pleinement ses responsabilités : il place ce dernier au centre de la stratégie de protection des droits dans une démarche qu'on peut qualifier de citoyenne.

Et le troisième point est que cette démarche accorde une place centrale à l'éducation et à la formation, qu'il s'agisse d'éducation informelle ou formelle ; et en matière scolaire où nombre de questions font encore débat, l'avis a le mérite de donner des directions – par

exemple l'idée que l'éducation au numérique ne doit pas être systématiquement liée à la formation scientifiques - sans pour autant trancher définitivement ces débats.

Cet avis intervient dans un ensemble de travaux divers sur la question, qu'il s'agisse de ceux du Conseil national du numérique ou du Conseil d'Etat : son apport est sans doute de s'appuyer sur ce qui fait l'originalité de notre assemblée, la confrontation d'acteurs les plus divers.

« Ce sont pour toutes ces raisons que je le voterai ».

Professions libérales

Depuis le début des années 2000, nous vivons une révolution silencieuse, celle de la donnée personnelle, de sa collecte et de son exploitation à titre personnel ou à visée d'intérêt général. Dans le passé, l'oubli était la règle et la mémoire, l'exception. Les technologies numériques ont transformé ce rapport à l'information en permettant la collecte et la conservation massive de données, en réduisant les coûts de stockage et de traitement des informations ; mais comme toute révolution, il est difficile d'en saisir toutes les opportunités ou d'en mesurer tous les risques !

La maîtrise des données numériques est devenue un élément crucial de la participation de chaque individu à la vie en société. L'enjeu fondamental à nos yeux est le respect des libertés, le droit à la confidentialité des données personnelles et à la capacité d'échapper au fichage d'un « *big brother* » dont on ne perçoit pas les arcanes.

D'où l'urgence de développer l'éducation au numérique, au-delà même de la simple utilisation des outils. Aujourd'hui les données ont tendance à refléter nos comportements marketing sur Internet et sur les mobiles, demain apparaîtra une prochaine génération de données, encore plus intimes, celles de notre santé, qui seront collectées par des objets connectés. Il faut anticiper cette tendance et lister les risques que comporte l'*Open Data* et favoriser une éducation à la critique, à la recherche ou la réutilisation des données.

La santé est un exemple intéressant avec d'un côté l'imagerie médicale qui permet une meilleure compréhension du vivant ou une détection précoce de pathologies, de l'autre côté, l'accès à des données médicales personnelles ultrasensibles. Aujourd'hui, les données médicales de chaque patient englobent ses consultations, ses prescriptions, ses examens, ses actes médicaux, ses séjours à l'hôpital. Seule la CNAM les détient. Mais avec l'arrivée des dispositifs connectés, la frontière des données médicales est poreuse... selon la définition que l'on en retiendra et l'usage que l'on voudra en faire, jusqu'où doit s'arrêter l'exploitation des données médicales ? Les compagnies d'assurance par exemple ne seront-elles pas tentées demain d'individualiser leurs primes ? On devine les choix qui en découleraient ! Comment concilier progrès de la médecine et protection de la vie privée ? L'équation est complexe !

Pour autant en termes de sécurité sanitaire, l'accès pour les pharmaciens d'officine au fichier de remboursement des prestations pharmaceutiques permettrait d'éviter nombre de iatrogénies médicamenteuses et notamment chez les patients migrants. On regrette que ce service déjà mis à disposition des médecins, ne le soit pas dans les mêmes conditions pour les pharmaciens, alors que ce sont eux qui abondent ce même fichier.

Plusieurs problèmes hypothèquent l'avenir, l'anonymat ne pouvant être garanti à 100%. La loi actuelle est dépassée, il faudra sans doute l'adapter. La protection des données est un

droit fondamental non monnayable, il faut veiller au respect des trois principes fondamentaux de la loi de juillet 1978, rappelés dans l'avis : finalité, loyauté et proportionnalité... Et veiller également au respect du droit à l'oubli, qui est une garantie fondamentale des libertés. Il passe par un droit d'opposition ou de consentement à l'utilisation de ses données personnelles pour chaque individu. La marchandisation des données personnelles est un autre risque, et non des moindres. L'avis préconise entre autres de promouvoir une éthique numérique seule capable de rétablir une confiance dans le numérique, et préconise de renforcer les sanctions pour protéger les citoyens mais également les entreprises.

Toute personne doit devenir co-architecte de cette nouvelle société numérique qui se profile à l'horizon. C'est le message principal porté par l'avis. Le groupe des professions libérales l'a voté.

UNAF

L'informatique a ouvert de gigantesques chantiers et opportunités. Il en ressort l'urgence d'une stratégie en faveur d'une véritable culture numérique et d'une protection des données efficiente. Sous l'angle des données personnelles, l'avis présente le sujet de façon positive : ce que le groupe de l'UNAF souligne.

Le rôle essentiel de la famille dans ce domaine est justement mis en lumière. C'est la raison pour laquelle les parents, comme tous les citoyens ont besoin d'une véritable éducation, leur permettant d'accompagner leurs enfants. Toute initiative de plateforme collaborative assortie de tutoriels est une réponse intéressante à ce besoin. Il faut accompagner les familles pour qu'elles comprennent mieux les enjeux du numérique et ne se retrouvent pas démunies face à l'exploitation dommageable de photos ou de données relatives à leurs enfants.

Pour le groupe de l'UNAF, deux questions restent en suspens.

- concernant la labellisation des meilleurs sites, quels en seront les critères et la méthodologie de mise en place ?
- les interventions en milieu scolaire élémentaire ne sont pas toutes réussies du fait de l'approche préventive et parfois trop défensive des risques de l'Internet.

Pour l'UNAF, l'éducation au numérique est essentielle pour les familles. Il faut donc rappeler que l'éducation au et par le numérique vont de pair. De nouvelles pratiques pédagogiques doivent être proposées et nous regrettons que l'avis ne soit pas plus abouti sur ce point.

Le groupe de l'UNAF rappelle que les Espaces publics numériques (EPN) ou les espaces socio-culturels sont des lieux au service de l'acculturation, la compréhension, la maîtrise, l'innovation, la créativité devant permettre à chacun de trouver sa place dans la société numérique.

Le groupe de l'UNAF soutient les préconisations de redynamisation des politiques publiques sur les territoires car comment faire avancer cette culture du numérique sans connexion de bonne qualité, ni infrastructure, notamment dans les territoires ruraux. La revitalisation de monde rural en dépend.

Enfin, le projet de règlement européen sur les données personnelles, dans son approche de la protection des données comme un droit fondamental de chaque individu reconnaissant un « droit à l'oubli », doit être défendu par les pouvoirs publics français.

Le groupe de l'UNAF a voté l'avis.

L'accroissement des données produites par tous - entreprises, particuliers, scientifiques, institutions publiques - et des objets connectés qui débouchera sur le web 3.0 d'ici à 2020, ainsi que le perfectionnement des outils d'analyse sont comparés aujourd'hui à un phénomène de révolution aussi importante que l'imprimerie en son temps.

Les réels enjeux issus de l'analyse en temps réel de ces données massives, tels que notamment les enjeux de sécurité au niveau national et mondial, le traitement plus efficace des pathologies, le développement de la recherche et la prévention de catastrophes, le développement de nouvelles technologies et de nouveaux emplois ou encore l'organisation plus efficiente de services ou l'optimisation de l'offre commerciale doivent se conjuguer au respect de la vie privée, de la confidentialité, du libre-arbitre, de l'éthique, du libre choix, de l'égalité entre tous les citoyens.

Les informations disponibles sur le net n'ont pas de frontières, le cadre juridique doit évoluer pour les dépasser afin d'engager toutes les parties prenantes sur un même socle de droits et devoirs.

Le *Big Data* entraîne des évolutions de modèles économiques pour les entreprises et les nations, mais aussi une évolution des modes d'apprentissage, de structuration de la pensée et d'analyse personnelle.

L'accès aux informations disponibles sur le net est devenu un facteur d'intégration social et économique, la fracture numérique concerne l'Etat mais aussi nos entreprises.

La France doit être un acteur dynamique pour capter au niveau national le potentiel économique et les retombées en matière de création d'emplois. Aujourd'hui, ce sont les GAFA (Google, Apple, Facebook, Amazon) qui captent hors de la France la valeur économique des données que nos institutions et nos citoyens mettent à disposition sur la toile.

A cet effet, l'UNSA est attachée au développement d'une filière *big data*, l'une des « sept ambitions pour une France innovante et dynamique », génératrice d'emplois qualifiés et garantie d'un traitement des données et d'une gestion des risques à la française.

La France s'est emparée de ces questions en nommant un administrateur général des données et en investissant dans le développement des analyses, des outils de stockage et des moteurs de recherche nationaux, dans la mise en œuvre de la normalisation des données et de la sécurisation des échanges, ainsi que dans le recrutement et la formation des analystes de données massives qui nécessitent des compétences multiples.

Mais peu de choses semble fait pour l'éducation à l'usage du numérique au profit des citoyens, des entreprises et des administrations. C'est ce à quoi s'attache cet avis et à cet effet, l'UNSA partage les préconisations dans sa volonté d'englober l'ensemble de la société, de l'école aux entreprises, afin de former des citoyens éclairés et vigilants.

Pour l'UNSA, il est important de rappeler que la dématérialisation de l'apprentissage et la mise à disposition de savoirs sur le net ne doit pas engendrer la généralisation de l'isolement des « apprenants ». Il est primordial pour la construction de la pensée de nos jeunes qui seront les citoyens de demain, de leur capacité à raisonner, à hiérarchiser l'information, à l'analyser que les enseignements du parcours initial restent interactifs dans un cadre collectif et présentiel.

Les français entretiennent un rapport paradoxal sur le sujet numérique se dotant massivement d'objets connectés tout en se manifestant préoccupés par les questions de protection de leurs données personnelles.

L'environnement personnel de tous les citoyens étant connecté, ces derniers doivent avoir les moyens de prendre la mesure des enjeux mais aussi des risques. Il s'agit de faire respecter la loi Informatique et Libertés qui prévoit le droit à être informé de la collecte et de l'utilisation de ses données, le consentement explicite et le droit à l'oubli. Prendre le temps de comprendre, savoir paramétrer, se poser les bonnes questions n'ont jamais été aussi essentiels. Trop peu de citoyens y sont sensibilisés et préparés.

Pour limiter les dérives, les questions notamment de l'incitation à transmettre des données personnelles, du consentement et encore du détenteur des données et de leur marchandisation doivent être encadrées et adaptées aux besoins.

Les préconisations restent à l'aube des réflexions sur ces sujets appelés à se développer et se transformer à la mesure de la rapidité de la croissance des données, du développement des outils d'analyse et des usages qui en seront faits.

L'ensemble de la vie citoyenne doit se saisir de la question du numérique et développer les outils opérants à son échelle.

Ainsi, pour une école de la citoyenneté innovante, l'éducation nationale se doit par exemple de réfléchir au BYOD (*Bring Your Own Device*) ou AVEC (Apportez Votre Equipement personnel de Communication) en contexte scolaire, au filtrage d'internet dans les établissements, à l'interdiction de l'usage des téléphones mobiles en primaire et au collège qui met en infraction les enseignants qui autorisent des usages pédagogiques pertinents, ou encore à la réforme des examens dans un monde connecté.

L'UNSA a voté l'avis.

Scrutin

Scrutin sur l'ensemble du projet d'avis

Nombre de votants 187

Ont voté pour 187

Le CESE a adopté.

Ont voté pour : 187

<i>Agriculture</i>	M. Bastian, Mmes Bernard, Bonneau, MM. Choix, Cochonneau, Mme Dutoit, M. Giroud, Mme Henry, MM. Lefebvre, Pelhate, Roustan, Mmes Serres, Sinay, M. Vasseur.
<i>Artisanat</i>	Mme Amoros, MM. Bressy, Crouzet, Mmes Foucher, Gaultier, MM. Griset, Le Lann, Liébus, Martin, Mme Sassano.
<i>Associations</i>	M. Allier, Mme Arnoult-Brill, M. Da Costa, Mme Jond, M. Leclercq, Mme Prado, M. Roirant.
<i>CFDT</i>	M. Blanc, Mme Boutrand, MM. Cadart, Duchemin, Gillier, Mmes Hervé, Houbairi, MM. Le Clézio, Mussot, Mme Nathan, M. Nau, Mmes Pajères y Sanchez, Pichenot, Prévost, MM. Quarez, Ritzenthaler.
<i>CFE-CGC</i>	M. Artero, Mme Couturier, MM. Dos Santos, Lamy, Mme Weber.
<i>CFTC</i>	M. Coquillion, Mme Courtoux, MM. Ibal, Louis, Mme Parle.
<i>CGT</i>	Mmes Cailletaud, Crosemarie, M. Delmas, Mme Dumas, M. Durand, Mmes Farache, Geng, Hacquemand, MM. Mansouri-Guilani, Marie, Michel, Naton, Teskouk.
<i>CGT-FO</i>	Mme Baltazar, MM. Bellanca, Lardy, Mmes Medeuf-Andrieu, Millan, M. Nedzynski, Mme Nicoletta, M. Peres, Mme Perrot, MM. Pihet, Porte, Veyrier.
<i>Coopération</i>	MM. Argueyrolles, Lenancker, Mmes Rafael, Roudil, M. Verdier.
<i>Entreprises</i>	Mme Bel, M. Bernasconi, Mmes Castera, Dubrac, Duhamel, Duprez, Frisch, M. Gailly, Mme Ingelaere, MM. Jamet, Lebrun, Lejeune, Marcon, Mariotti, Mongereau, Placet, Mme PrévotMadère, MM. Ridoret, Roger-Vasselin, Mme Roy, M. Schilansky, Mmes Tissot-Colle, Vilain.
<i>Environnement et nature</i>	MM. Beall, Bonduelle, Bougrain Dubourg, Mmes de Béthencourt, Denier-Pasquier, Ducroux, MM. Genest, Genty, Guérin, Mmes de Thiersant, Laplante, Mesquida, Vincent-Sweet, M. Virlouvét.
<i>Mutualité</i>	MM. Andreck, Davant.
<i>Organisations étudiantes et mouvements de jeunesse</i>	MM. Djebara, Dulin, Mmes Guichet, Trelu-Kane.
<i>Outre-mer</i>	MM. Arnell, Grignon, Janky, Omarjee, Osénat, Mme Romouli-Zouhair.

<i>Personnalités qualifiées</i>	MM. Aschieri, Bailly, Mme Ballaloud, M. Baudin, Mmes Brishoual, Brunet, Chabaud, MM. Corne, Delevoye, Mmes Dussaussois, El Okki, M. Etienne, Mme Flessel-Colovic, MM. Gall, Geveaux, Mmes Gibault, Grard, Graz, MM. Guirkinge, Hochart, Jouzel, Mme de Kerviler, MM. Khalfa, Le Bris, Mme Levaux, MM. Lucas, Martin, Mmes de Menthon, Meyer, M. Obadia, Mmes d'Ormesson, Ricard, MM. Richard, de Russé, Soubie, Terzian.
<i>Professions libérales</i>	MM. Capdeville, Gordon-Krief, Noël, Mme Riquier-Sauvage.
<i>UNAF</i>	Mme Basset, MM. Damien, Farriol, Feretti, Fondard, Joyeux, Mmes Koné, L'Hour, Thery, M. de Viguerie.
<i>UNSA</i>	M. Grosset-Brauer.

Annexes

Annexe n° 1 : composition de la section de l'éducation, de la culture et de la communication

✓ **Président** : Philippe DA COSTA

✓ **Vice présidentes** : Claire GIBault et Claire GUICHET

Agriculture

✓ Monique BERNARD

Artisanat

✓ Monique AMOROS

Associations

✓ Philippe DA COSTA

✓ Bérénice JOND

CFDT

✓ Adria HOUBAIRI

✓ Xavier NAU

✓ Albert RITZENTHALER

CFE-CGC

✓ Jean-Claude DELAGE

CFTC

✓ Bernard IBAL

CGT

✓ Claude MICHEL

CGT-FO

✓ Françoise NICOLETTA

✓ Éric PERES

Entreprises

✓ Geneviève BEL

✓ Danielle DUBRAC

✓ Sophie DUPREZ

Environnement et nature

✓ Jacques BEALL

Organisations étudiantes et mouvements de jeunesse

- ✓ Azwaw DJEBARA
- ✓ Claire GUICHET
- ✓ Marie TRELLU-KANE

Outre-mer

- ✓ Marie-Claude TJIBAOU

Personnalités qualifiées

- ✓ Rachel BRISHOUAL
- ✓ Laura FLESSEL-COLOVIC
- ✓ Claire GIBAULT
- ✓ Marie-Aleth GRARD
- ✓ Alain TERZIAN
- ✓ Gérard ASCHIERI (Rattaché administrativement au groupe)

UNAF

- ✓ Henri JOYEUX
- ✓ Christiane THERRY

Personnalités associées

- ✓ Amewofofo ADOM'MEGAA
- ✓ Joël BATTEUX
- ✓ Nadia BELLAOUI
- ✓ Nora HUSSON
- ✓ Marie-Françoise LEFLON
- ✓ Anaïg LUCAS
- ✓ Jean-Marc MONTEIL

Annexe n° 2 : liste des personnes auditionnées

- ✓ **Mme Maryse ARTIGUELONG**
Ligue des droits de l'Homme
- ✓ **M. Dimitri BARCLAIS**
rapporteur-adjoint au CNum
- ✓ **M. Frédéric BARDEAU**
Simplon.co
- ✓ **M. Bernard BENHAMOU**
maître de conférences à l'Institut d'études politiques de Paris
- ✓ **Mme Amandine BRUGIERE**
directrice de projet à la Fondation internet nouvelle génération
- ✓ **M. Antonio CASILLI**
maître de conférences en humanités numériques à Telecom Paris Tech
- ✓ **Mme Marie CAMIER**
Media éducation
- ✓ **M. Nicolas COLIN**
The Family
- ✓ **M. Alexandre DESROUSSEAUX**
Conseil régional Nord Pas de Calais
- ✓ **M. Stéphane DISTINGUIN**
responsable de Fabernovel
- ✓ **M. Samuel GOETA**
Open Knowledge Foundation
- ✓ **Mme Laure KALTENBACH**
directrice générale du Forum d'Avignon
- ✓ **M. Jean-Marc MANACH**
journaliste au journal Le Monde
- ✓ **M. Marc MOSSE**
directeur des affaires juridiques et des affaires publiques de Microsoft
- ✓ **M. Lancelot PECQUET**
Will Strategy
- ✓ **Mme Sophie PENE**
membre du Conseil national du numérique (CNum) et pilote du Groupe éducation
- ✓ **M. Nicolas SEYDOUX**
président du Forum d'Avignon
- ✓ **M. Henri VERDIER**
directeur d'Etalab
- ✓ **Mme Sophie VULLIET-TAVERNIER**
directeur des études, de l'innovation et de la prospective de la Commission nationale informatique et libertés

Annexe n° 3 : glossaire

Big Data

Donnée massive

Cloud

Nuage

Cloud computing

Informatique en nuage

Data Center

Centre de conservation des données

Open Data

Donnée ouverte

Profiling

Récolte de données

People based

Stockage basé sur les données personnelles

Software based

Stockage basé sur un logiciel

Quantified self

Méthode de mesure de ses données personnelles

Patient care and insights

Soins centrés sur le patient

Smart grid

Réseau de distribution électrique « intelligent »

Mooc

Cours en ligne ouvert et massif

Flipped classroom

Classe inversée

Wiki

Application web qui permet de créer et modifier de façon collaborative

Wikipedia

Encyclopédie collaborative

Crowdfunding

Financement participatif

FabLabs

Laboratoires de fabrication

Makerspaces

Espace de travail exploité en communauté

Chief data officer

Directeur des données

Computer illiteracy

Analphabétisme de l'ordinateur

Information illiteracy

Analphabétisme de l'information

Privacy paradox

Paradoxe de la vie privée

Privacy framework

Structure logicielle de protection des données personnelles pour un individu

Cross border privacy rules

Système de règles de confidentialité transfrontalières

Recognited accountability agent

Applications pour servir de moyen de responsabilisation

Rules and guidelines

Règles et programmes

Privacy by design

Protection intégrée de la vie privée dès la conception d'un logiciel

Do not track by default

Application informatique permettant de ne pas traquer un utilisateur sans son consentement

Closed circuit

Circuit fermé de caméras de surveillance

Patriot act

Loi antiterroriste des Etats - Unis

National Security Agency

Agence pour la sécurité nationale aux Etats-Unis

Open SSL

Boîte à outils de chiffrement

Right to be left alone

Droit de rester seul

Crowdsourcing

Externalisation ouverte

Data scientist

Spécialiste de la donnée en matière de statistique et d'analyse

Data broker

Courtier de données

Smart disclosure

Divulgateur intelligente de données

Coworking

Travail partagé

Bring your own device (BYOD)

Apportez vos appareils personnels à votre travail

Bring your own access

Apportez vos applications à votre travail

Soft Law

Droit mou ou droit souple

Opt in

Option d'adhésion

Chief technology officer (CTO)

Directeur de la technologie

Chief data officer (CDO)

Directeur de la technologie

Safe harbor

Sphère de sécurité

Dashboard

Tableau de bord

Empowerment

Développement du pouvoir d'agir

Points Cyb

Espaces jeunes numériques

Peer to peer

Pair à pair

Data driven

Diriger par les données

Data mining

Exploration de données

Annexe n° 4 : table des sigles

APEC	<i>Asia Pacific Economic Cooperation</i>
APIE	Agence du patrimoine immatériel l'Etat
ANSA	Association nationale des sociétés par actions
B2i	Brevet informatique et internet
BCR	Règles internes d'entreprises (binding corporate)
BYOD	<i>Bring Your Own Device</i> : apporter nos appareils personnels
BYOA	<i>Bring Your Own Application</i> : utiliser ses propres applications informatiques
CADA	Commission d'accès aux documents administratifs
CBPR	<i>Cross Border Privacy Rules</i>
C2i	Certificat informatique et internet
CCI	Chambre de commerce et d'industrie
CCTV	<i>Closed-circuit television</i> (vidéosurveillance)
CEDH	Convention européenne des droits de l'Homme et des libertés fondamentales
CEPD	Contrôleur européen de la protection des données
CNIL	Commission nationale de l'informatique et des libertés
CNIS	Conseil national de l'information statistique
CDC	Caisse des dépôts et consignation
CEA	Commissariat à l'énergie atomique et aux énergies
CESI	Centre des études supérieures de l'industrie
CGPME	Confédération générale du patronat des petites et moyennes entreprises
CGU	conditions générales d'utilisation
CGV	Conditions générales de vente
CIGREF	Réseau des grandes entreprises
CREDOC	Centre de recherche pour l'étude et l'observation des conditions de vie
CTI	Commission des titres d'ingénieur
DC	<i>Data Center</i>
ECM	Entreprises content management (gestion de contenu)
ENT	Espaces numériques de travail
EPN	Espaces publics numériques
ESPE	Ecoles supérieures du professorat et de l'éducation
FED	Réserve fédérale des Etats-Unis
FING	<i>Fédération Internet Génération</i>
FNSEA	Fédération nationale des syndicats d'exploitants agricoles
GAFA	Google, Apple, Facebook, Amazon
GENES	Groupe des écoles nationales d'économie et statistiques
INED	Institut national d'études démographiques
INSEE	Institut national de la statistique et des études économiques
MEDEF	Mouvement des entreprises de France
MOOC	<i>Massive Online Courses</i> (cours massifs en ligne)
NSA	Agence nationale de sécurité des Etats-Unis
ONU	Organisation des Nations unies
OCDE	Organisation de coopération et de développement économiques
PME	Petites et moyennes entreprises
RFID	<i>Radio Frequency Identification</i>
TICE	Technologies de l'information et de la communication pour l'enseignement
TPE	Très petite entreprise
UNAF	Union nationale des associations
UPA	Union professionnelle artisanale

Annexe n° 5 : bibliographie

Library of Congress 25 avril 2012 « A “Library of Congress” Worth of Data: It’s All In How You Define It »

<http://blogs.loc.gov/digitalpreservation/2012/04/a-library-of-congress-worth-of-data-its-all-in-how-you-define-it/>

Oxford Economics et Citybank, 2011

http://www.citibank.com/transactionservices/home/docs/the-new_digital_economy.pdf

http://www.arcep.fr/uploads/tx_gspublication/rapport-credoc-diffusion-tic-2012.pdf

Thomas Khun, La structure des révolutions scientifiques. Ed Flammarion Collection Champs 2008

Viktor Mayer-Schonberger, Kenneth Cukier, .- Big Data. Editions Robert Laffont, Paris 2013, p.17

Fabrice Coquoio <http://pro.01net.com/editorial/605472/>

<http://www.globalsecuritymag.fr>

Christophe Brasseur, op.cit.

Présentation détaillée dans « Data Center et Développement Durable », juin 2011, Syntec Numérique

Data Center et Développement Durable, juin 2011, Syntec Numérique

Glanz, New York Times, 22/09/2012

Christophe Brasseur, Enjeux et usages du Big Data, technologies, méthodes et mise en œuvre, Lavoisier, Hermès Science, 2013

Commissariat général à la stratégie et à la prospective, Internet : prospective 2030, note d’analyse n°2, juin 2013

Report of the 2007 Rueschlikon Conference on Information Policy By **Kenneth Cukier**

<http://www.cukier.com/writings/Rueschlikon2007-infogov-cukier.pdf>, il est aussi l’auteur de Big Data, la révolution des données est en marche par Kenneth Cukier et Viktor Mayer-Schonberger (Lafont février 2014).

Talend, Gartner Group et Deloitte

Transparency Market Research « Big DataMarket – Global Scenario, Trends, Industry Analysis, Size, Share and Forecast 2012-2018 »

Henri Verdier, Nicolas Colin, L’âge de la multitude, Entreprendre et gouverner après la révolution numérique. Editions A.Colin 2012

INRIA, rapport 2012

Le mariage du numérique et de l’énergétique : vers un Internet de l’énergie <http://www.scenarios2020.com/2012/05/le-mariage-du-num%C3%A9rique-et-de-l%C3%A9nerg%C3%A9tique-vers-un-internet-de-l%C3%A9nergie.html>

Smart Grid - Interview intégrale de **Jeremy Rifkin** - FUTUREMAG – ARTE - <http://www.youtube.com/watch?v=OhWNUUKHahc>

Conseil économique, social et environnemental, Pour un renouveau des politiques publiques de la culture, avis présenté par Claude Michel au nom de la section de l’éducation, de la culture et de la communication, avril 2014

Compte-rendu du Conseil des ministres du mercredi 17 septembre 2014

Agence nationale des solidarités actives, L’accès aux télécommunications pour tous, la parole aux personnes en situation de précarité, avril 2012

<http://www.observatoire-du-numerique.fr/usages-2/grand-public/equipement>

Tech executives to Obama: NSA spying revelations are hurting business (Washington Post 17/12/2013) <http://wapo.st/1kfMSAZ>

Editorial de **Mark Zuckerberg** posté sur Facebook le 13/03/2014 <http://on.fb.me/1nVf2Cc>

Social Media and the 'Spiral of Silence' (Etude PewResearch - août 2014)

<http://www.pewinternet.org/2014/08/26/social-media-and-the-spiral-of-silence/>

<http://www.wired.co.uk/news/archive/2014-02/06/tim-berners-lee-reclaim-the-web>

Rapport au nom de la mission commune d'information sur l'accès aux documents administratifs et aux données publiques présidé par **M. Jean-Jacques Hyst**, Sénateur, présenté par **Mme Corinne Bouchoux**, Sénatrice, juin 2014.

MIT TechnologyReview 15 septembre 2014)

<http://www.technologyreview.com/news/530671/smartphone-movements-could-reveal-empty-parking-spots/>

20 % des grandes entreprises investissent dans l'Internet des objets (Proxima Mobile - 21 août 2014)

<http://www.proximamobile.fr/article/20-des-grandes-entreprises-investissent-dans-l-internet-des-objets>

<http://www.proximamobile.fr/article/une-cartographie-mondiale-de-l-internet-des-objets>

<http://www.newsweek.com/2013/06/26/body-data-craze-237656.html>

<http://research2guidance.com/the-market-for-mhealth-app-services-will-reach-26-billion-by-2017/>

Eric Topol on the Future of Medicine – Wall Street Journal 7 juillet 2014)

<http://online.wsj.com/articles/eric-topol-on-the-future-of-medicine-1404765024> voir

aussi son ouvrage The Creative Destruction of Medicine (Eric Topol- Ed. Basic Books - janvier 2012).

Wearable Tech Is PluggingIntoHealthInsurance (Forbes 19 juin 2014)

<http://www.forbes.com/sites/parmyolson/2014/06/19/wearable-tech-health-insurance/>

<http://www.proximamobile.fr/article/le-ministre-anglais-de-la-sante-demande-aux-medecins-d-inciter-leurs-patients-utiliser-des-a>

Patrick Arnoux, Le Nouvel Economiste - 5 août 2014

<http://www.lenouveleconomiste.fr/e-sante-les-technologies-les-mentalites-pas-en-core-23635/>

How Much Is Your Privacy Worth ? (MIT TechnologyReview, 26 août 2014)

<http://www.technologyreview.com/news/529686/how-much-is-your-privacy-worth>

« Le droit sur les données personnelles, un droit à l'autodétermination plutôt qu'un droit de propriété », étude annuelle 2014 du Conseil d'Etat : Le numérique et les droits fondamentaux (p264)

[http://www.ladocumentationfrancaise.fr/rapports-publics/144000541-etude-annuelle-2014-du-conseil-d-etat-le-numerique-et-les-droits-fondamentaux \)](http://www.ladocumentationfrancaise.fr/rapports-publics/144000541-etude-annuelle-2014-du-conseil-d-etat-le-numerique-et-les-droits-fondamentaux)

The creepside of data mining: Selling "sick" lists (CBS Moneywatch 11 septembre 2014)

<http://www.cbsnews.com/news/the-creepy-side-of-data-mining-selling-sick-lists/>

<http://www.theguardian.com/technology/2014/aug/29/apple-health-data-privacy-developers-advertisers>

The Feds Stall Self-Driving Cars (Wall Street Journal - 24 août 2014)

<http://online.wsj.com/articles/gordon-crovitz-the-feds-stall-self-driving-cars-1408919700>

Big Data Can Be Used for Good in the Community (New York Times 6 août 2014 <http://www.nytimes.com/roomfordebate/2014/08/06/is-big-data-spreading-inequality/big-data-can-be-used-for-good-in-the-community>)

Predictive Policing' Technology Lowers Crime In Los Angeles (Huffington Post Greg Risling 7 janvier 2012)

http://www.huffingtonpost.com/2012/07/01/predictive-policing-technology-los-angeles_n_1641276.html

Valérie Peugeot.- Données personnelles : sortir des injonctions contradictoires. Vecam. 13/04/2014

Marine Albarède, René Francou, Daniel Kaplan.- Mes Infos : cahier d'exploration. FING. Mars 2013

<http://assistance.orange.fr/securiser-le-mobile-de-vos-enfants-avec-le-controle-parental-mobile-1788.php> <http://petitlien.fr/CESEnum1>

Conseil économique, social et environnemental, L'alternance dans l'éducation, étude présentée par **M. Jean-Marc MONTEIL** au nom de la section de l'éducation, de la culture et de la communication, 2014

<http://www.proximamobile.fr/article/une-initiative-americaine-pour-maitriser-la-consommation-electrique-depuis-les-mobiles> <http://petitlien.fr/CESEnum2>

États-Unis : un concours pour créer un appareil mobile mesurant l'impact de la pollution sur la santé (Proxima Mobile - 6 octobre 2012)

<http://www.proximamobile.fr/article/etats-unis-un-concours-pour-creer-un-appareil-mobile-mesurant-l-impact-de-la-pollution-sur-l> <http://petitlien.fr/CESEnum3>

Cass Sunstein

(The Law of Group Polarization- University Of Chicago Law School 1999)

http://www.law.uchicago.edu/files/files/91.CRS_Polarization.pdf <http://petitlien.fr/CESEnum4>

Why teaching grandmothers to code isn't a crazy idea (Washington Post 15/8/2014)

<http://www.washingtonpost.com/blogs/innovations/wp/2014/08/15/why-teaching-grandmothers-to-code-isnt-a-crazy-idea> <http://petitlien.fr/CESEnum5>

Pascal Buffard. Président du CIGREF

Hervé Collignon – associé **d'A.T.Kearney**, coauteur d'une étude sur le secteur de la haute technologie en Europe – Février 2014.

<http://www.theguardian.com/commentisfree/2013/sep/05/government-betrayed-Internet-nsa-spying> <http://petitlien.fr/CESEnum7>

The Internet after Snowden : New threat model army (The Economist, 11/11/2013) <http://econ.st/1r5U71J> <http://petitlien.fr/CESEnum8>

Panel recommends NIST declare independence from NSA (FCW - 14 juillet 2014) <http://petitlien.fr/CESEnum9>

<http://fcw.com/articles/2014/07/14/nist-panel-on-nsa.aspx>

http://www.ssi.gouv.fr/IMG/pdf/NP_Ordiphones_NoteTech.pdf

Laurent Cytermann, rapporteur général adjoint du Conseil d'Etat, Audition rapport d'information – L'Europe au secours de l'Internet, n°696 – Tome II, 2013-2014 – Sénat

Les mutations économiques, sociales et politiques de l'Internet des objets (**Bernard Benhamou** - Cahiers de la Documentation Française – décembre 2012)

<http://www.netgouvernance.org/IOT%20Cahiers%20DOC%20FRANCAISE.PDF>

Rapport au nom de la mission commune d'information sur l'accès aux documents adminis-

tratifs et aux données publiques présidé par **M. Jean-Jacques Hyest**, Sénateur, présenté par **Mme Corinne Bouchoux**, Sénatrice, juin 2014

http://www.redressement-productif.gouv.fr/files/20140306_rapport_tariq_krim.pdf

L'accès aux télécommunications pour tous : la parole aux personnes en situation de précarité (Étude ANSA – avril 2012)

http://www.solidarites-actives.com/pdf/ANSA_TIC_contribution_15_acces_telecoms.pdf

Glanz, New York Times, 22/09/2012

<http://iet.jrc.ec.europa.eu/energyefficiency/ict-codes-conduct/data-centres-energy-efficiency> <http://petitlien.fr/CESEnum11>

<http://www.greenit.fr/article/acteurs/hebergeur/data-center-quels-impacts-sur-le-territoire-5057> <http://petitlien.fr/CESEnum12>

Conseil économique social et environnemental, Internet : pour une gouvernance ouverte et équitable, étude présentée Mme Nathalie Chiche au nom de la section des affaires européennes et internationales, 2013

Architecture et Gouvernance de l'Internet par **Bernard Benhamou** (Revue Esprit mai 2006)

www.netgouvernance.org/ArchitectureEsprit.pdf <http://petitlien.fr/CESEnum13>

Pervasive Monitoring Is an Attack (RFC 7258 IETF mai 2014)

<http://tools.ietf.org/html/rfc7258> <http://petitlien.fr/CESEnum14>

Liberty And Security In A Changing World, Report and Recommendations of The President's Review Group on Intelligence and Communications Technologies (décembre 2013)

http://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf
<http://petitlien.fr/CESEnum15>

Comment le logiciel nous influence – **Hubert Guillaud** InternetActu, le 29 août 2014

<http://Internetactu.blog.lemonde.fr/2014/08/29/comment-le-logiciel-nous-influence/>

<http://petitlien.fr/CESEnum16>

<https://tosdr.org/> - Source Wikipedia



Dernières publications de la section de l'éducation, de la culture et de la communication

- *Pour un renouveau des politiques publiques de la culture*
- *L'alternance dans l'éducation*
- *Pour une politique de développement du spectacle vivant : l'éducation artistique et culturelle tout au long de la vie*
- *Avant-projet de loi d'orientation et de programmation pour la refondation de l'école de la République*
- *Réussir la démocratisation de l'enseignement supérieur : l'enjeu du premier cycle*
- *La mobilité des jeunes*

LES DERNIÈRES PUBLICATIONS DU CONSEIL ÉCONOMIQUE, SOCIAL ET ENVIRONNEMENTAL (CESE)

- *Rapport annuel sur l'état de la France en 2014*
- *Combattre les violences faites aux femmes des plus visibles aux plus insidieuses*
- *Agir pour la mixité des métiers*
- *Tourisme et développement durable en France*
- *L'impératif d'une ambition pour le climat*
- *La protection maternelle et infantile*
- *L'influence de la France sur la scène européenne et internationale par la promotion du droit continental*

**Retrouvez l'intégralité
de nos travaux sur
www.lecese.fr**

Imprimé par la direction de l'information légale et administrative, 26, rue Desaix, Paris (15^e)
d'après les documents fournis par le Conseil économique, social et environnemental

N° de série : 411150001-000115 – Dépôt légal : janvier 2015

Crédit photo : 123RF



LES **AVIS**
DU CONSEIL
ÉCONOMIQUE,
SOCIAL ET
ENVIRONNEMENTAL



La révolution du numérique a ouvert de gigantesques chantiers et opportunités dans notre vie quotidienne et domestique et dans de multiples domaines (santé, prévention, gestion intelligente des espaces publics, facilitant du quotidien, pratique démocratique etc.).

Tant les citoyens, les entreprises que les États et leurs administrations participent pleinement à cet univers numérique sans toutefois en mesurer pleinement les opportunités ou les risques induits. Ce défaut de sensibilisation renforce l'asymétrie d'information entre les grands opérateurs d'internet et les citoyens-utilisateurs et conduit le CESE à appeler de ses vœux la construction d'un cadre collectif juridique et éthique à cet écosystème numérique qui soit en mesure de garantir à tous les acteurs les mêmes droits et une défense effective de leurs libertés.



CONSEIL ÉCONOMIQUE, SOCIAL
ET ENVIRONNEMENTAL

9, place d'Iéna
75775 Paris Cedex 16
Tél. : 01 44 43 60 00
www.lecese.fr

N° 41115-0001 prix : 25,70 €

ISSN 0767-4538 ISBN 978-2-11-138653-2



Diffusion
Direction de l'information
légale et administrative
Les éditions des Journaux officiels
tél. : 01 40 15 70 10
www.ladocumentationfrancaise.fr