INTERNATIONAL JOURNAL OF **DIGITAL AND DATA LAW**

REVUE INTERNATIONALE DE DROIT **DES DONNÉES ET DU NUMÉRIQUE**

Vol. 3 - 2017

ISSN 2553-6893

IMODEV
LES ÉDITIONS

International Journal of Digital and Data Law
Revue internationale de droit des données et du numérique

Direction :
Irène Bouhadana & William Gilles

ISSN : 2553-6893

IMODEV
49 rue Brancion 75015 Paris – France
www.imodev.org
ojs.imodev.org

Les propos publiés dans cet article n'engagent que leur auteur.

The statements published in this article are the sole responsibility of the author.

À PROPOS DE NOUS

La **Revue Internationale de droit des données et du numérique (RIDDN)/ the International Journal of Digital and Data Law** est une revue universitaire créée et dirigée par Irène Bouhadana et William Gilles au sein de l'IMODEV, l'Institut du Monde et du Développement pour la Bonne Gouvernance publique.

Irène Bouhadana, docteur en droit, est maître de conférences en droit du numérique et droit des gouvernements ouverts à l'Université Paris 1 Panthéon-Sorbonne où elle dirige le master Droit des données, des administrations numériques et des gouvernements ouverts au sein de l'École de droit de la Sorbonne. Elle est membre de l'Institut de recherche juridique de la Sorbonne (IRJS). Elle est aussi fondatrice et Secrétaire générale de l'IMODEV.

William Gilles, docteur en droit, est maître de conférences (HDR) en droit du numérique et en droit des gouvernements ouverts, habilité à diriger les recherches, à l'Université Paris 1 Panthéon-Sorbonne où il dirige le master Droit des données, des administrations numériques et des gouvernements ouverts. Il est membre de l'Institut de recherche juridique de la Sorbonne (IRJS). Il est aussi fondateur et Président de l'IMODEV.

IMODEV est une organisation scientifique internationale, indépendante et à but non lucratif créée en 2009 qui agit pour la promotion de la bonne gouvernance publique dans le cadre de la société de l'information et du numérique. Ce réseau rassemble des experts et des chercheurs du monde entier qui par leurs travaux et leurs actions contribuent à une meilleure connaissance et appréhension de la société numérique au niveau local, national ou international en en analysant d'une part, les actions des pouvoirs publics dans le cadre de la régulation de la société des données et de l'économie numérique et d'autre part, les modalités de mise en œuvre des politiques publiques numériques au sein des administrations publiques et des gouvernements ouverts.

IMODEV organise régulièrement des colloques sur ces thématiques, et notamment chaque année en novembre les *Journées universitaires sur les enjeux des gouvernements ouverts et du numérique / Academic days on open government and digital issues*, dont les sessions sont publiées en ligne [ISSN : 2553-6931].

IMODEV publie deux revues disponibles en open source (ojs.imodev.org) afin de promouvoir une science ouverte sous licence Creative commons CC-**BY-NC-ND** :

1) la *Revue Internationale des Gouvernements ouverts (RIGO)/ International Journal of Open Governments* [ISSN 2553-6869] ;

2) la *Revue internationale de droit des données et du numérique (RIDDN)/International Journal of Digital and Data Law* [ISSN 2553-6893].

ABOUT US

The **International Journal of Digital and Data Law / Revue Internationale de droit des données et du numérique (RIDDN)** is an academic journal created and edited by Irène Bouhadana and William Gilles at IMODEV, the Institut du monde et du développement pour la bonne gouvernance publique.

Irène Bouhadana, PhD in Law, is an Associate professor in digital law and open government law at the University of Paris 1 Panthéon-Sorbonne, where she is the director of the master's degree in data law, digital administrations, and open governments at the Sorbonne Law School. She is a member of the Institut de recherche juridique de la Sorbonne (IRJS). She is also the founder and Secretary General of IMODEV.

William Gilles, PhD in Law, is an Associate professor (HDR) in digital law and open government law at the University of Paris 1 Panthéon-Sorbonne, where he is the director of the master's degree in data law, digital administration and open government. He is a member of the Institut de recherche juridique de la Sorbonne (IRJS). He is also founder and President of IMODEV.

IMODEV is an international, independent, non-profit scientific organization created in 2009 that promotes good public governance in the context of the information and digital society. This network brings together experts and researchers from around the world who, through their work and actions, contribute to a better knowledge and understanding of the digital society at the local, national or international level by analyzing, on the one hand, the actions of public authorities in the context of the regulation of the data society and the digital economy and, on the other hand, the ways in which digital public policies are implemented within public administrations and open governments.

IMODEV regularly organizes conferences and symposiums on these topics, and in particular every year in November the Academic days on open government and digital issues, whose sessions are published online [ISSN: 2553-6931].

IMODEV publishes two academic journals available in open source at ojs.imodev.org to promote open science under the Creative commons license CC-**BY-NC-ND**:

1) the *International Journal of Open Governments*/ la *Revue Internationale des Gouvernements ouverts (RIGO)* [ISSN 2553-6869] ;

2) the *International Journal of Digital and Data Law* / la *Revue internationale de droit des données et du numérique* (RIDDN) [ISSN 2553-6893].

L'AMBITION INDIVIDUALISTE DE L'AUTODETERMINATION INFORMATIONNELLE

par **Thomas BIZET**, Juriste à la CNIL, doctorant en droit à l'Université Paris 1 Panthéon-Sorbonne (France).

La doctrine de « Gouvernement ouvert » vise à promouvoir une gouvernance favorisant la transparence et la responsabilisation des gouvernants ainsi que la possibilité aux gouvernés de contrôler, superviser et prendre part aux décisions. Cette doctrine a comme essence un plus large mouvement d'encapacitation (« *empowerment* » ou « *agency* ») des citoyens.

En 1983, la Cour constitutionnelle fédérale allemande forge le concept de l'autodétermination informationnelle (le « *Selbstbestimmungsrecht* ») comme « le pouvoir de l'individu de décider lui-même sur base du concept d'autodétermination, quand et dans quelle mesure une information relevant de sa vie privée peut être communiquée à autrui »[1]. La loi n° 2016-1321 dite pour une « République numérique » a transcrit un droit similaire en France depuis le 7 octobre 2016.

Ainsi après l'alinéa 1 classique de la loi n° 78-17 modifiée, « 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 », un alinéa 2 précise désormais que « Toute personne dispose du droit de décider et de contrôler les usages qui sont faits des données à caractère personnel la concernant, dans les conditions fixées par la présente loi. »

Le rapport d'information déposé par la Commission de réflexion et de propositions sur le droit et les libertés à l'âge numérique, préfigurant notamment la loi Lemaire précitée, précise que le droit à l'autodétermination informationnelle consiste à « donner à l'individu l'autonomie informationnelle et décisionnelle nécessaire à son libre épanouissement dans l'univers numérique »[2].

Toutefois, la proposition issue du rapport précise que « l'individu doit se voir reconnaître de véritables droits d'information et d'action dans la mise en œuvre de ces traitements »[3]. En particulier, le rapport attirait l'attention du législateur sur les

[1] Cour constitutionnelle fédérale, 16 février 1983, *BVerfGE*, tome 62, p. 1 ; Analyse FROMONT, *RD publ.* 1983, p. 954.

[2] C. PAUL & FERAL-SCHUHL, *Rapport d'information déposé par la Commission de réflexion et de propositions sur le droit et les libertés à l'âge du numérique,* p.125, 2015.

[3] *Id.* p. 129

risques que ferait courir la seule inscription de droit, « dépourvu de traduction juridique concrète et de moyens techniques effectifs, il ne permettra pas à l'individu de faire face au fonctionnement des réseaux numériques et d'exprimer une volonté éclairée sur la multitude des utilisations de données auxquelles il s'expose plus ou moins volontairement. »[4]
Il convient alors d'analyser si l'intégration de ce nouveau droit a été accompagnée des moyens juridiques et techniques permettant sa mise en œuvre effective.

§ 1 – L'INTÉGRATION DU NOUVEAU DROIT À L'AUTODÉTERMINATION INFORMATIONNELLE DANS UN SYSTÈME JURIDIQUE PRÉEXISTANT

Le droit à l'autodétermination informationnelle a été intégré dans un ordre juridique existant. Cet ordre juridique est particulier créé en 1978 il a été modifié notamment en 2004 par la transposition de la directive 95/46/CE du 24 octobre 1995.
Les termes de l'alinéa intégré dans l'article 1 de la loi n° 78-18 modifiée renvoient plus particulièrement vers deux principes déjà présents dans le droit applicable : le droit de « décider » des usages qui sont faits des données le concernant et le droit de « contrôler » les usages qui sont faits des données le concernant.
Le droit de « contrôler » les usages semble renforcer les dispositions du droit applicable relatives aux droits « Informatique & Libertés » de la personne concernée, à savoir les droits d'accès, de rectification, d'opposition pour motif légitime – ce qui inclut le droit au déréférencement – et le droit de suppression des données.
Le droit de « décider » des traitements, dans son approche volontariste, se rapporte au consentement de l'individu à un traitement et aux informations préalables nécessaires à la formation de celui-ci.
En ce qui concerne le consentement, les travaux de la Commission de réflexion et de propositions sur le droit et les libertés à l'âge numérique[5] n'ont pas été transcrits dans la loi dite « Lemaire » en même temps que le droit à l'autodétermination informationnelle.
Le droit applicable reste donc celui de l'article 7 de la loi n° 78-17 modifiée[6]. La mise en œuvre d'un traitement de données à caractère personnel est conditionnée au consentement préalable de la personne concernée. À défaut, le traitement doit satisfaire à l'une obligations énumérées : l'exécution d'un contrat auquel la personne concernée est partie ou l'exécution de mesures précontractuelles prises à la demande de celle-ci, le respect d'une obligation légale à laquelle le responsable du traitement est

[4] *Id.*
[5] http://www2.assemblee-nationale.fr/14/autres-commissions/numerique/
[6] Le règlement européen 2016/678 applicable à partir de mai 2018 conserve par ailleurs le cadre de ce droit applicable.

soumis, la sauvegarde de l'intérêt vital de la personne concernée, l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique, dont est investi le responsable ou le destinataire du traitement ou la réalisation de l'intérêt légitime poursuivi par le responsable du traitement ou par le destinataire, sous réserve de ne pas méconnaître l'intérêt ou les droits et libertés fondamentaux de la personne concernée[7].

Le consentement, dans l'environnement numérique actuel, se heurte à de nombreuses limites. Christophe Lazaro et Daniel Le Metayer précisent, dans *Le consentement au traitement des données personnelles : une perspective comparative sur l'autonomie du sujet*[8] :

> « Les développements technologiques de ces dernières années ainsi que les pratiques sociales qu'ils génèrent semblent battre en brèche la capacité, voire même la volonté, des individus d'exercer un véritable contrôle sur leurs données personnelles ».

Le consentement semble bien devenir une fiction dans la plupart des cas, l'utilisateur, même averti, est quasiment dans l'incapacité aujourd'hui de mesurer les conséquences de son choix. Ainsi que l'indiquait Mme Isabelle Falque-Pierrotin, présidente de la CNIL :

> « Dans l'univers actuel des données massives, le principe du consentement est moins évident en raison des multiples échanges qui interviennent bien au-delà de la collecte. »[9]

La Directive de 1995 définit le consentement comme :

> « toute manifestation de volonté, libre, spécifique et informée par laquelle la personne concernée accepte que des données à caractère personnel la concernant fassent l'objet d'un traitement ».

La doctrine juridique en matière de consentement médical a été particulièrement précise pour définir les conditions nécessaires à sa formation[10].

---

[7] Voir dans le cadre de l'intérêt légitime dans la décision nº 2016-007 du 16 janvier 2016 mettant en demeure les sociétés FACEBOOK INC. et FACEBOOK IRELAND où la Commission indique que « l'intérêt économique et commercial de la société ne peut être regardé comme légitime que si le responsable de traitement met à disposition des utilisateurs inscrits des moyens adéquats leur permettant de contrôler la combinaison de leurs données et d'exercer effectivement le droit qui leur est reconnu par l'article 38 de la loi du 6 janvier 1978 modifiée. » Disponible sur : https://www.cnil.fr/sites/default/files/atoms/files/d2016-007_med_facebook-inc-ireland.pdf (consulté le 20 janvier 2017).

[8] C. LAZARO & D. LE METAYER, « Le consentement au traitement des données personnelles : une perspective comparative sur l'autonomie du sujet », *Revue juridique Themis, 43*(3), 768-815, 2015.

[9] Audition du 26 novembre 2014 de I. FALQUE-PIERROTIN devant la Commission de réflexion et de propositions sur le droit et les libertés à l'âge numérique

[10] Voir en ce sens : J. Katz, « Informed consent. A fairy tale? Law's vision », *U. Pitt. L. Rev., 39* (2), 1977, p. 143 et G. DWORKING, *The Theory and Practice of Autonomy*. Cambridge, 1988.

Dans ce cadre, R. Faden et T. L. Beauchamp ont défini plusieurs phases[11] :

1. Information (« disclosure ») : toutes les informations pertinentes doivent être délivrées au patient avant qu'il ne prenne sa décision.
2. Compréhension (« understanding ») : le patient doit comprendre les caractéristiques générales de la pathologie ou du problème médical, les risques et bénéfices du traitement ainsi que les autres options.
3. Volonté (« voluntariness ») : le patient ne doit pas subir de pression ou d'influence déterminante dans sa prise de décision.
4. Capacité (« compétence ») : le patient est censé être responsable (au sens de « en capacité de prendre la responsabilité ») de la prise de décision.
5. Consentement (« consent ») : le patient doit se voir laisser le choix

Le consentement n'est pas une notion autonome, il est dépendant de la mise en capacité de la personne concernée à la former. Il est donc nécessairement lié aux informations prérequises permettant sa formation.

Or, en matière numérique, les informations nécessaires listées à l'article 32 de la loi n° 78-17 modifiée ne permettent pas d'assurer une compréhension des traitements directs ou ultérieurs des données par le responsable de traitement ou les destinataires des données.

L'article 32 de la loi n° 78-17 liste ainsi que la personne auprès de laquelle sont recueillis des données à caractère personnel la concernant est informée, sauf si elle l'a été au préalable, par le responsable de traitement ou son représentant de l'identité du responsable du traitement et, le cas échéant, de celle de son représentant, de la finalité poursuivie par le traitement auquel les données sont destinées, du caractère obligatoire ou facultatif des réponses, des conséquences éventuelles, à son égard, d'un défaut de réponse, des destinataires ou catégories de destinataires des données, des droits qu'elle détient et le cas échéant, des transferts de données à caractère personnel envisagés à destination d'un État non membre de la Communauté européenne.

La loi dite « Lemaire »[12] a ajouté une information supplémentaire relative à la durée de conservation des catégories de données traitées ou, en cas d'impossibilité, des critères utilisés permettant de déterminer cette durée ainsi qu'une information supplémentaire relative aux droits de définir des directives relatives au sort des données après la mort de la personne concernée.

[11] R. FADEN & T. L. BEAUCHAMP, *A History and Theory of Informed Consent,* Oxford University Press, 1986.

[12] Loi n° 2016-1321 du 7 octobre 2016 pour une République numérique.

Le règlement européen 2016/678 ajoute également des informations supplémentaires à partir de mai 2018. Le responsable de traitement devra ainsi fournir à la personne concernée, le cas échéant, les coordonnées du délégué à la protection des données, lorsque le traitement est fondé sur l'intérêt légitime le responsable de traitement devra fournir une information relative à cet intérêt légitime, lorsque le traitement est fondé sur le consentement une mention informant du droit de retirer son consentement, le droit d'introduire une réclamation auprès d'une autorité de contrôle, l'existence d'une prise de décision automatisée, y compris un profilage, et, au moins en pareils cas, des informations utiles concernant la logique sous-jacente, ainsi que l'importance et les conséquences prévues de ce traitement pour la personne concernée.

Le règlement européen précise par ailleurs, en son article 7, les conditions applicables au consentement. Le responsable de traitement devra être en mesure de démontrer que la personne concernée a donné son consentement au traitement de données à caractère personnel la concernant. Par ailleurs, la personne concernée aura le droit de retirer son consentement, ce qui ne sera applicable que pour les traitements effectués après ledit retrait.

Les informations à fournir par le responsable de traitement, ou son représentant sont donc très nombreuses. Toutefois, l'environnement numérique actuel est si dense, si technique, que ces informations, quand bien même elles seraient lisibles par l'individu, ne garantissent pas que la personne puisse saisir de manière claire et prévisible les conséquences de sa « décision » de partage d'informations[13].

La possibilité pour la personne concernée d'effectuer un droit de retrait de son consentement semble adapter en partie le droit à cette réalité en permettant à l'individu de revenir sur sa décision dont il en aurait subi ou perçu des conséquences. En ce sens, le législateur européen prévoit que le consentement doit être aussi simple à retirer qu'à donner. Par ailleurs, le retrait du consentement n'est pas subordonné à un motif comme le droit à l'effacement ou le droit d'opposition.

Malgré cette prise en considération des usages et des problématiques liées à la difficile compréhension par les personnes concernées des impacts sur leur vie privée des traitements, le consentement demeure dans le droit le fondement juridique d'un traitement de données à caractère personnel.

Cette primauté, liée à une conception essentiellement individualiste de la protection de vie privée, implique de ne pas prendre en compte que les données à caractère personnel ne concernant pas une unique personne.

[13] C. LAZARO & D. LE METAYER, "Control over personal data: true remedy or fairy tale?", *Scripted, 12, 2015.*

§ 2 – LES DONNÉES À CARACTÈRE PERSONNEL SONT DE PLUS EN PLUS COLLECTIVES

La primauté du consentement suppose que la personne concernée consent au traitement de ses données à caractère personnel. Or, se faisant, elle soumet au traitement de nombreuses données qui sont également des données à caractère personnel concernant d'autres personnes.

La personne concernée n'est plus dans un fichier plat du XIX[e] siècle, mais dans des bases de données qui peuvent être interconnectées entre elles. Les organismes consommateurs de données non plus seulement besoin de connaître les données concernant une personne, mais ont besoin des données de contexte (famille, contacts, etc.). Ces données peuvent également être utilisées pour construire des modèles permettant de « deviner » des données non fournies par un tiers.

L'évolution des réseaux sociaux permet à chacun de raconter sa propre vie : photographies, géolocalisations, avis laissés, etc. Ce « grand déballage » dépasse la seule vie de celui ou celle qui raconte. Les médias sociaux permettent de raconter aussi l'histoire des proches. Les photographies peuvent être « taguées » pour y faire figurer les noms ou pseudonymes des personnes qui y apparaissent, les points de géolocalisation peuvent de même faire apparaître l'endroit – par exemple le domicile d'une personne – ou les personnes avec qui celui ou celle qui raconte se situe. Les réseaux sociaux permettent de construire le graphe social de chacun, de manière directe en y incluant volontairement les noms/pseudonymes des personnes ou de manière indirecte par recoupement (liste d'amis, de contacts téléphoniques, recoupement de la géolocalisation, etc.).

Ainsi, quand un utilisateur partage une photographie sur le réseau Instagram ou Facebook, il partage ses propres informations contenues dans la photographie, mais les informations de toutes les personnes qui l'entourent et qu'il a « taguées » dans la photographie.

Dans la conception individualiste d'un traitement fondé sur le consentement, les personnes « taguées » n'ont pas nécessairement consenti *a priori*. Quand bien même le réseau Facebook permet par exemple de supprimer une identification *a posteriori*, cette simple possibilité de suppression ne saurait être entendue comme un consentement valable. Le seul consentement provient de la personne qui a publié la photographie et identifié les personnes.

Il convient en outre de rappeler que Facebook dispose de la technologie permettant d'identifier automatiquement des personnes sur des photographies. Cette technologie est devenue une fonctionnalité en 2011 permettant à l'ensemble du réseau d'amis de l'utilisateur de voir les photographies publiées où l'utilisateur « semble apparaître », une modification a été réalisée pour dorénavant suggérer une identification lorsqu'une personne publie une photographie dans le cadre de la « suggestion

d'identification ». Il faut souligner que tout utilisateur peut désactiver cette fonctionnalité depuis les paramètres de confidentialité.

Plus clivant que ces exemples de « réseaux de partage » qui peuvent impliquer autant les tiers que l'utilisateur, des données particulières sont partagées entre les individus. Le type de donnée le plus visible en ce sens est la donnée génétique.

La donnée génétique est une donnée qui est partagée par l'ensemble de la famille génétique. Cette donnée est actuellement au centre d'une course, de grands acteurs comme 23andMe proposent des tests génétiques permettant d'obtenir des informations généalogiques, des informations médicales, mais aussi des rencontres amoureuses, des régimes alimentaires personnalisés sur la base d'une analyse du génome, etc.

Le partage des informations génétiques implique nécessairement de partager – au moins une partie significative – les informations génétiques de ses proches génétiques. Par le biais d'un recoupement généalogique, l'entreprise ou l'administration pourra en déduire les informations génétiques des proches. Or, sur ces données de santé le consentement n'a pas été fourni par les proches, qui par ailleurs ne sont pas mis en mesure d'être informé du partage. Il est tout à fait libre d'imaginer dans un avenir rythmé par le « data marketing » que la famille d'un utilisateur qui aura partagé ses informations génétiques recevra des produits de tests personnalisés (alicaments, etc.).

Plus avant, l'accroissement des technologies d'analyse de données amplifie le travail des spécialistes dans l'analyse des données marketing. Sur la base des informations clients fournies par les courtiers en données, les spécialistes de l'analyse établissent des modèles permettant d'évaluer la chance pour tel ou tel type de personnes de consommer tel ou tel produit. Ces modèles ne peuvent exister que parce que certains ont partagé leurs données. Ces modèles s'appliquent aussi sur ceux qui n'ont pas partagé beaucoup. Grâce aux personnes qui ont beaucoup partagé, les spécialistes vont pouvoir déduire ce que pourraient consommer ceux qui ont moins partagé.

De la même manière, dans le cas où les assurances demanderaient, à titre facultatif, de fournir des informations sensibles supplémentaires, si chaque individu consent à fournir ces informations, de fait l'individu qui n'y consent pas se retrouver heurter à une position moins avantageuse.

Le partage des informations d'un individu a donc une implication sur la vie privée d'un autre individu. Le droit à l'autodétermination informationnelle dépasse le seul individu qui le maîtrise, ou pense le maîtriser.

§ 3 – L'ÉDUCATION À LA VIE PRIVÉE ET AU PARTAGE

Le premier élément vers une gestion des utilisateurs de leur intimité sur les réseaux est la pédagogie, l'éducation au dévoilement sur les réseaux. Si les utilisateurs paraissent

aujourd'hui informés sur les risques de diffusion et de propagation de leurs données personnelles, cette information ne semble pas avoir suffi à inciter des pratiques responsables. Une première solution paraît la promotion d'une éducation à se « faire discret »[14] sur les réseaux. Cette pédagogie de la discrétion, de la pudeur, doit être au cœur du processus de compréhension des stratégies de dévoilement afin de permettre aux utilisateurs de distinguer le simple partage d'informations à propos d'eux de « l'oversharing »[15] ou encore la gestion de sa réputation numérique du « personal branling »[16]. Plus globalement l'ambition est la compréhension des usages, des enjeux et les failles que peuvent présenter le partage d'informations sur les réseaux. Il s'agit des briques élémentaires nécessaires pour que l'utilisateur soit en mesure de développer des stratégies de dévoilement ou de contournement.

Les principales actions de pédagogie mises en œuvre sont des présentations des dangers et des risques liés au numérique. Outre une vision fantasmée de la chose numérique personnifiée comme dévoreuse d'emplois et de données, les enfants découvrent alors dès leur plus jeune âge que l'Internet est peuplé essentiellement de pédophiles[17] et de terroristes sévissant sur le « dark net »[18]. Internet serait ainsi le repaire pour « les psychopathes, les violeurs, les racistes et les voleurs »[19] dans une « sorte de *Far West* »[20]. Dans ces conditions, avec cette conception des réseaux, il est évident que le discours pédagogique ne peut être positif et encourageant.

Cette peur est donc transmise dans la pédagogie, à l'exemple du « Permis Internet au CM2 » lancé par des gendarmes et AXA Prévention le 12 décembre 2013[21]. Armés d'un « Code de bonne conduite sur Internet » les instituteurs devront donc formés des élèves de CM2 qui passeront par la suite leur permis devant des gendarmes. Le terme « permis » est pertinent et semble adéquat avec l'action menée puisqu'il renvoie à une « permission », une

---

14 E. DESPLANQUES, « Éloge de la retenue sur les réseaux sociaux », *Télérama,* 2014. Disponible sur : http://www.telerama.fr/idees/eloge-de-la-retenue-sur-les-reseaux-sociaux,107620.php [consulté au 24/05/2014]

15 Anglicisme désignant le fait qu'une personne délivre trop d'informations personnelles, notamment intimes.

16 Anglicisme dérivé de l'onanisme narcissique du « personal branding », le marketing personnel apparu notamment dans Al RIES, J. TROUT, *The Battle for your Mind,* McGraw-Hill, 1981.

17 Par exemple la campagne de presse de l'organisation « Action Innocence » de 2009 sur les « Nouveaux dangers d'Internet » pour sensibiliser les parents.

18 Dont la terminologie exacte est « Deep web », c'est-à-dire le Web profond, non indexé par les moteurs de recherches grand public. En ce sens A. GUITON, « Qui a peur du grand méchant "DarkNet ?", *Slate*, 2013. Disponible sur : http://www.slate.fr/monde/80471/qui-peur-du-grand-mechant-darknet [consulté au 20/05/2014]

19 Propos de F. LEFEBVRE, disponible sur : http://www.assemblee-nationale.fr/13/cri/2008-2009/20090103.asp [consulté au 24/05/2014]

20 Propos de M. BOUTIH, disponible sur : http://www.nextinpact.com/news/ 84450-selon-malek-boutih-pires-pulsions-galopent-sur-far-west-internet.htm [consulté au 24/05/2014]

21 Une présentation est disponible sur le site de AXA Prévention : http://www.axaprevention.fr/Actualites/Pages/permis-Internet-pour-les-enfants.aspx [consulté au 22/05/2014]

« autorisation » sans laquelle l'élève de CM2 ne pourrait pas naviguer sur Internet. L'action se situe ainsi dans un contexte essentiellement répressif et négatif.

C'est d'ailleurs ce que remarque le député Lionel Tardy en posant une question le 6 mai 2014 au ministre de l'Éducation nationale,

> « en regardant les questions posées, il semble que ce permis repose principalement sur une pédagogie "par la peur", qui n'a aucun intérêt si elle n'est pas accompagnée d'une sensibilisation aux usages du numérique, pour que les élèves acquièrent de réelles compétences en la matière. »[22]

Le Syndicat de l'Inspection de l'Éducation nationale (S.I.EN UNSA) avait aussi émis des critiques en rappelant notamment que

> « les enseignants ont un penchant naturel à privilégier l'intelligence à la norme, la compréhension à la soumission, l'adhésion à la contrainte »[23].

Le CSA est allé plus loin dans sa vision d'un « nettoyage » de l'Internet en proposant dans son rapport annuel de créer un label « site de confiance » aux sites Internet qui signeront une convention et tous les sites non labellisés seraient alors filtrés et bloqués.[24] Toutefois, cette idéologie ne semble pas respecter le droit fondamental qu'est la liberté d'accès au réseau[25] et en sus elle paraît radicalement contre-productive dans l'objectif de responsabiliser les utilisateurs des réseaux.

L'éducation au dévoilement doit être conçue comme une pédagogie prenant en compte les nouveaux usages. L'ambition doit être une sensibilisation des enfants et de leurs parents en présentant les avantages et les inconvénients de l'outil qu'est l'Internet sans le figurer tel un monstre. Par ailleurs, ces cours pourraient très bien s'intégrer dans le cadre des cours de code informatique actuellement en préparation[26].

L'image des cours sur le numérique ressemble fortement à la vision des premiers cours d'éducation sexuelle où les adolescents apprenaient les noms des maladies sexuellement transmissibles et à se protéger sans jamais parler de l'acte lui-même, de ce qu'il peut représenter et de ce qu'il peut contenir de positif. Dans cette perspective, en ne présentant uniquement que les aspects négatifs, la seule suite logique est la peur, le rejet puis l'étreinte. Or, l'objectif d'une éducation n'est pas de susciter la peur, mais d'élever, en

---

[22] L. TARDY, *Question nº 54941*

[23] S. I. E. N. UNSA, *Non au permis Internet Gendarmerie, AXA*, 2014. Disponible sur : http://www.sien-unsa-education.org/images/stories/documentation/actions/Non_au_permis_Internet_Gendarmerie_AXA.pdf [consulté au 24/05/2014].

[24] G. CHAMPEAU, *Le CSA veut un label « site de confiance » pour censurer le Web,* Numerama, 2014. Disponible sur : http://www.numerama.com/magazine/29070-le-csa-veut-un-label-site-de-confiance-pour-censurer-le-web.html [consulté au 24/05/2014].

[25] Conseil constitutionnel, 10 juin 2009, nº 2009-580 DC.

[26] M. BAUMARD, « Faut-il enseigner le code informatique à l'école ? », *Le Monde,* 2014. Disponible sur : http://www.lemonde.fr/education/article/2014/05/23/faut-il-enseigner-le-code-informatique-a-l-ecole_4424397_1473685.html [consulté au 24/05/2014] ou encore D. BARCLAIS, « L'inévitable enseignement des sciences de l'informatique », Droitnumérique-sorbonne.fr, 2014. Disponible sur : http://www.droitnumerique-sorbonne.fr/enseignementinformatique.html consulté au 24/02/2014]

présentant les bienfaits et les risques, et en responsabilisant. Mais pour responsabiliser, il convient de donner l'ensemble des éléments pour faire naître la compréhension. Mais s'il convient d'effectuer ces efforts pédagogiques en primaire, des opérations de sensibilisation doivent aussi être mises en œuvre en continu de la scolarité afin d'informer et de former l'ensemble de la population[27]. L'incompréhension du numérique n'est pas le monopole d'une génération[28].

Car le risque d'une population ne comprenant pas les usages, dans la société informationnelle, est lourd de conséquences. Le juriste Daniel J. Solove prend l'exemple de Kafka et de la bureaucratie pour analyse des conséquences d'une société qui ne saisiraient pas l'importance de l'utilisation des données, ainsi « le problème que saisit la métaphore de Kafka est différent de celui que cause la surveillance. Il relève du processus de traitement de l'information (le stockage, l'utilisation ou l'analyse des données) plutôt que de sa collecte. Le problème ne réside pas tant dans la surveillance même des données, mais dans l'impuissance et la vulnérabilité créée par une utilisation de données qui exclut la personne concernée de la connaissance ou de la participation dans les processus qui le concernent. Le résultat est ce que produisent les bureaucraties : indifférences, erreurs, abus, frustrations, manque de transparence et déresponsabilisation. Un tel traitement affecte les relations entre les gens et les institutions d'un État moderne. Il ne se limite pas à frustrer l'individu en créant un sentiment d'impuissance, mais il affecte toute la structure sociale en altérant les relations que les gens ont avec les institutions qui prennent des décisions importantes sur leur existence. »[29]

Le Parlement européen, notamment dans sa recommandation du 26 mars 2009 à l'intention du Conseil sur le « renforcement de la sécurité et des libertés fondamentales sur Internet », dont le point j) recommande

> « d'encourager des programmes visant à protéger les enfants et à éduquer leurs parents comme indiqué dans la législation communautaire concernant les nouveaux dangers d'Internet et fournir une étude d'impact sur l'efficacité des programmes existant à ce jour ; il convient, dans cette optique, d'accorder une attention particulière aux jeux en ligne ciblant principalement les enfants et les jeunes et d'intégrer les jeux vidéo et informatiques dans le programme *Safer Internet.* »[30]

---

[27] Voir en ce sens, D. BAHU-LEYSER, « Une éthique à construire », *Hermès. La Revue*, 2009/1 (nº 53), pp. 161-166.

[28] Voir en ce sens, G. JACQUINOT-DELAUNAY, « On ne naît pas internaute, on le devient… », *Hermès, La Revue,* 2011/1, nº 59.

[29] Daniel J. SOLOVE, *«* I've got nothing to hide and other misunderstandings of privacy *»,* (trad. H. GUILLAUD), *San Diego Law Review*, Vol. 44, p. 745, 2007. Disponible sur :http://papers.ssrn.com/sol3/papers.cfm?abstract_id=998565 [consulté au 24/05/2014]

[30] Parlement européen, Renforcement de la sécurité et des libertés fondamentales sur Internet, 2009. Disponible sur : http://www.europarl.europa.eu/sides/getDoc.do?pub

Le projet du programme « *Safer Internet* »[31] est de sensibiliser pour un « Internet sans crainte », « plus responsable et plus sûr ». Ce programme a le mérite de disposer d'une plateforme de signalement en ligne des contenus choquants et d'un numéro national d'assistance. Par ailleurs ce programme permet l'éclosion d'initiatives institutionnelles et citoyennes autour de l'éducation au numérique, à l'image du collectif « EducNum ». Ces initiatives développent des projets d'éducation à une utilisation responsable et positive des réseaux qui ne peuvent qu'être salués.

C'était par ailleurs l'ambition de faire de l'éducation au numérique une grande cause nationale en 2014 permettant de dispenser une véritable « culture générale du numérique permettant à chacun de disposer des clés de compréhension de cet univers, aussi bien en termes scientifiques, informatiques, juridiques, mais aussi économiques, sociaux ou encore éthiques »[32].

Ref=-//EP// TEXT+TA+P6-TA-2009-0194+0+DOC+XML+V0//FR [consulté au 24/05/2014]

[31] Disponible sur : http://www.saferinternet.fr/[consulté au 24/05/2014]

[32] Disponible sur le site du collectif EducNum : http://www.educnum2014.fr/ [consulté au 24/05/2014]