



Béatrice Galinon-Melenec et Sami Zitni (dir.)

## Traces numériques De la production à l'interprétation

CNRS Éditions

---

# Protection des identités numériques personnelles : des futurs incertains

Jacques Perriault

---

DOI : 10.4000/books.editions-cnrs.21723

Éditeur : CNRS Éditions

Lieu d'édition : Paris

Année d'édition : 2013

Date de mise en ligne : 16 juillet 2019

Collection : CNRS Alpha

EAN électronique : 9782271130136



<http://books.openedition.org>

### Référence électronique

PERRIAULT, Jacques. *Protection des identités numériques personnelles : des futurs incertains* In : *Traces numériques : De la production à l'interprétation* [en ligne]. Paris : CNRS Éditions, 2013 (généré le 16 novembre 2023). Disponible sur Internet : <<http://books.openedition.org/editions-cnrs/21723>>. ISBN : 9782271130136. DOI : <https://doi.org/10.4000/books.editions-cnrs.21723>.

---

Le texte seul est utilisable sous licence . Les autres éléments (illustrations, fichiers annexes importés) sont « Tous droits réservés », sauf mention contraire.

# Protection des identités numériques personnelles : des futurs incertains

*Jacques Perriault*

Les problèmes que pose la protection de l'identité personnelle dans sa version numérique croissent à mesure que se développent à la fois le nombre des utilisateurs d'Internet et ce qu'ils en font, entre autres dans les pratiques de recrutement. Notre laboratoire<sup>1</sup> a découvert cela très tôt, dès 2002, du fait de sa forte implication dans les travaux de construction de standards et de normes pour l'apprentissage en ligne dans le cadre de l'*International Standard Organization* (ISO) et de l'Afnor. Cela fera l'objet d'un rappel, dans une première partie, de la lente et progressive construction d'une problématique, compliquée par des difficultés croissantes. Dans une seconde partie nous tenterons de caractériser l'évolution de la protection des identités numériques personnelles, en anglais : *privacy*<sup>2</sup>. Nous reformulerons dans un troisième temps, la question de l'identité numérique personnelle en termes de politique publique pour terminer, en quatrième partie, par la présentation d'un processus de régulation en cours de réalisation, utile, ambitieux, mais difficile à mettre en place.

## UNE CONSTRUCTION TRÈS PROGRESSIVE

La commission ISO à laquelle nous faisons ici référence, est un comité permanent (*standing committee*) qui porte le sigle SC36 et l'intitulé « *Information Technologies for Learning, Education and Training* ». En juillet 2001, les comités nationaux ont été saisis par les États-Unis d'une

---

1. Laboratoire CRIS de Paris-Ouest Nanterre, aujourd'hui dénommé TACTIC (EA 1738).

2. Le terme anglais *privacy* comporte en lui-même une idée de défense. Mais les organisations internationales, comme ISO, parlent de *privacy protection principles*.

demande d'adoption en urgence – sans discussion – d'un projet d'identifiant personnel pour tout internaute accédant à des services de formation en ligne. Le projet précisait que cet identifiant devrait permettre d'apprécier les compétences intellectuelles et physiques des intéressés, de même que leurs préférences culturelles. Le Japon et la France furent les seuls à refuser d'emblée, cette dernière arguant du fait que chaque citoyen avait un identifiant, le code Insee, et que par ailleurs la directive européenne 95/46/CE de 1995 réservait strictement aux parlements le droit d'associer un code numérique à une identité personnelle (ARNAUD, JUANALS et PERRIAULT, 2002).

Par nature, l'apprentissage en ligne accumule des données sur les utilisateurs du fait des incessantes interactions entre l'apprenant et la machine : ses réponses, ses notes, son profil d'apprentissage construit à partir de ses interventions, etc., et enrichit de ce fait le contenu de ce qui peut facilement être associé à un identifiant, appelé ici *simple human identifier*. Essayons de clarifier cette question :

- un identifiant numérique personnel renvoie à la notion d'identité au sens classique du terme. Il inclut les composantes habituelles de celle-ci, c'est-à-dire : nom, adresse, date de naissance, etc. Même s'il n'est pas explicitement lié à l'identité dans ce dernier sens, il l'est indirectement dans la plupart des cas par le truchement de l'adresse de courrier électronique ou bien encore, dans les transactions commerciales, par le truchement de la carte de crédit ;

- les identifiants se retrouvent dans les bases de données les plus diverses : administratives, commerciales, bancaires, éducatives. En regard de chaque identifiant lié à un individu s'accumulent les traces de ses actions sur les réseaux. Il en ignore beaucoup ; il se doute de l'inscription numériques de certaines, telles que ses achats, ses interactions avec un tuteur dans un cours en ligne, par exemple. Et il en crée lui-même délibérément, de plus en plus, par ses interventions sur les réseaux sociaux (FABRE, 2009) ;

- il est donc possible, à l'aide de logiciels adaptés de constituer des sortes de grappes de traces associées à un individu. Des logiciels en accès libre, tels que *Touchgraph* ou *Agx Page* permettent pour une personne dont on connaît le nom et le mail, d'obtenir la carte du réseau des relations qu'elle entretient par Internet et, dans le cas de *Agx Page*, par des *tweets*, dont on peut connaître les contenus ;

- en raison de cette évolution, l'identité numérique personnelle est devenue une question plus large qu'à l'origine, compte-tenu de ces grappes de données et de traces qui sont attachées à l'identifiant original et qui ne cessent d'augmenter.

Identifiants et stocks de traces n'ont cessé de proliférer (PERRIAULT et VAGUER, 2012). Ce n'est plus le privilège d'une institution mandatée que de pratiquer de tels exercices. Le projet américain de *simple human identifier* ne fut pas retenu par ISO, pour une raison intéressante : lors d'une réunion à Adélaïde (Australie), une conseillère d'État, membre de la délégation française, rappela la directive européenne de 1995 – de ce fait, les représentants des pays de l'Union Européenne ne prirent pas part au vote et la décision fut rejetée.

### Difficultés croissantes

Dans la dernière décennie, de nombreuses difficultés ont émergé à propos des identifiants. La première, qui a été mise en évidence du fait des attentats du 11 septembre 2001, a été l'émergence d'un conflit toujours non résolu entre liberté et sécurité. La doctrine américaine fut, dans les années qui suivirent, de tracer systématiquement tout utilisateur d'Internet, afin de pister le terrorisme. La contrepartie en est une généralisation du contrôle et, par conséquent, une restriction des libertés.

La seconde difficulté vient du fait que tout individu peut enregistrer et inspecter les activités de tout internaute, approfondissant ainsi la connaissance de son identité. La géolocalisation est installée dans tous les *smart-phones* et le traçage d'un individu est devenu aujourd'hui monnaie courante. Les données que l'on peut recueillir sur Facebook sont souvent très instructives et de nombreuses firmes trouvent qu'elles sont souvent plus parlantes qu'un CV (BREDUILLIARD et CORDELIER, 2011).

La troisième difficulté et non la moindre vient du fait que les utilisateurs contribuent à exposer publiquement leurs données personnelles. On a ainsi appelé « extimité » ce phénomène. Blogs et réseaux sociaux contribuent à cette extension et ainsi à la construction d'une réputation numérique. Une industrie de la réputation s'est développée en parallèle, et il ne semble pas que cet engouement soit un effet de mode. Deux catégories d'arguments étayent ce qui, pour l'instant, n'est qu'une conjecture :

- ce qu'on appelle la génération Y – globalement, les moins de trente-cinq ans – sont nés dans un environnement fortement numérisé et trouveraient « naturelle » cette extimité, point sur lequel les avis divergent, à la seule exception de l'expérience acquise mais de façon inégale par la pratique des jeux informatisés ;

- la connectivité des personnes entre elles relèverait d'une problématique de régénération du lien social par la recherche de la considération par autrui pour renforcer l'estime de soi (GRANJON 2011 ; PERRIAULT, 2010).

On observe des tentatives sporadiques de limitation des excès. Des firmes telles que Bouygues ou Total font signer à leurs employés des chartes de confidentialité qui leur interdisent d'aborder dans leurs échanges sur les réseaux des informations liées à leur activité professionnelle (BREDUILLIARD et CORDELIER, 2011). De ce constat ressortent les enseignements suivants :

- chaque intervenant sur Internet est désormais au cœur d'une galaxie de données numériques innombrables, dont celles qu'il produit lui-même : question étudiée sous la dénomination de *user generated content* ;
- dans l'état actuel des choses, l'anonymisation des données personnelles paraît difficile à réaliser ;
- *a fortiori*, le droit à la déconnection, le droit à l'oubli, apparaissent sous cet éclairage comme des utopies.

Mais un processus de régulation est en route. Il devra reprendre les choses à zéro, ce qui ne va pas de soi.

## UNE PROTECTION PROCÉDURALE

L'identité numérique personnelle et sa protection (*privacy*)<sup>3</sup> sont des notions encore floues et fragiles. Deux préalables préfixent la réflexion en cours. Ce sont :

- le rapport entre diffraction et agrégation des données. Deux options sont intéressantes à considérer, formulées par des spécialistes. Daniel Kaplan, avocat français, se demande s'il faut prendre en considération la multiplicité des identités numériques liées à une personne ou bien celle des modes de présentation. Renaud Fabre, expert français, et Jake Knoppers, expert canadien, membres d'ISO, mettent en doute la notion de standard fixe au profit de celle de standard évolutif, ce dernier étant plus apte à se caler sur les changements technologiques (2012). Ils distinguent par ailleurs des standards orientés vers les exigences des utilisateurs et d'autres relatifs au soutien de services ;

- la propriété des identifiants et la réappropriation par les intéressés. En effet, aujourd'hui, ces profils ne nous appartiennent pas. Par exemple,

---

3. « “Privacy protection” is a human right, i.e. only natural persons have privacy protection right. Organizations and public administrations are “legal persons” and do not have privacy protection rights » FABRE et KNOPPERS, 2012. [La “protection de la vie privée” est un droit de l'homme, c'est-à-dire que seules les personnes physiques ont accès à sa protection. Les organismes et administrations publiques sont des « personnes morales » et n'ont pas le droit à la protection de la vie privée.]

Facebook revendique la propriété des données sur ses réseaux. Les utilisateurs sont très loin d'avoir accès aux données les concernant et on observe une prise de conscience émergente à ce sujet. Cela conduit à considérer les réflexions sur les choix institutionnels en matière de protection et passe par une réflexion en cours qui s'inscrit dans la problématique de la médiation, ici en matière d'information et de communication, entre des personnes physiques et des données numériques. L'interrogation porte sur la nature et le rôle du médiateur. Une fonction importante qui lui serait confiée est celle d'agrégateur central des données, dénommé « tiers de confiance » dans les réflexions en cours. Michel Arnaud (2011) plaide il y a quelques temps pour la constitution d'institutions tierces de confiance, sorte d'officiers ministériels du numérique, qui détiendraient la clé d'accès aux données identitaires en cas de besoin impérieux, et autorisés légalement à les mettre en regard des données comportementales, correspondant aux transactions de la vie courante effectuées sur les réseaux numériques. Une série de questions découlent de la métaphore de l'officier ministériel : la plus importante est de loin le pouvoir discrétionnaire que lui conférerait cette médiation, le mode de gestion du patrimoine numérique, du portefeuille et de sa transmission en cas d'héritage.

Dans cette hypothèse, resterait à définir :

– qui ou quelle institution pratiquerait ce recueil et cette agrégation ? Il y aurait lieu de distinguer identification et authentification. Le principe de ce qu'on appelle *cartes d'identité blanches* serait d'attester que la prestation demandée est licite sans que toutefois l'identité du demandeur soit communiquée ;

– comment seraient traitées des questions de sécurité et de confiance ? Les vides juridiques sont en effet nombreux : traces *post mortem* ; avatar (injures racistes, responsabilité pénale).

En tout état de cause, l'identité numérique, aujourd'hui galactique, est devenue problématique à définir et, *a fortiori*, à gérer. Un changement radical de perspective devrait s'imposer. Comme les données elles-mêmes, leur protection traverse l'espace public et l'espace privé. Nous rejoignons Bernard Miège, quand il indique que l'espace public est devenu une logique sociale (2010), ici nous dirions le territoire virtuel d'une logique procédurale. Nous assistons en effet à une dynamisation et à une mise en procédure des notions identitaires : se connecter une fois par jour à Facebook pour consulter son compte est ainsi une procédure composante de l'identité numérique. Nous constatons ainsi une évolution de la *protection* vers le statut procédural, ce qui converge avec la conception par Renaud Fabre et Jake Knoppers de standards évolutifs, rappelée en début d'article. Nous retrouvons le même constat chez Emmanuel Kessous à propos des normes de recrutement : « Dans cette acception, la *privacy* se construit au

fur et à mesure d'un sentier d'usages des services Web (et *a fortiori* d'autres services numériques) où les individus délivrent des informations les concernant » (KESSOUS, 2007).

## Régulations et politiques publiques

Au cours de la décennie, de nouvelles questions sur l'identité numérique se sont précisées. L'information sur la personne a une valeur, que démontrer l'intense utilisation qu'en fait le marketing. Selon Renaud Fabre (2009), la personne est devenue un *document* et est traitée comme tel. Quatre questions émergent à ce sujet et pèsent sur les travaux en cours :

- la personne virtuelle se superpose-t-elle au double numérique ?
- comment définir et protéger les contours d'un profil personnel ?
- quelle attitude adopter face aux administrations qui achètent désormais des données individuelles en ligne ?
- comment normer les conditions de l'interopérabilité, de l'adaptabilité et de l'extensibilité des systèmes (ce qui n'est plus un luxe mais une nécessité), au fur et à mesure que les gens (par exemple travailleurs, étudiants, etc.) ont de plus en plus besoin d'apprendre et de travailler dans différents endroits, fuseaux horaires, et différentes infrastructures technologiques ?

Ces interrogations rappellent que l'identité numérique est non seulement dynamique mais qu'elle fait surgir au fil du temps de nouvelles questions. À la clé se trouve l'enjeu important de faciliter la communication pour vivre ensemble (WOLTON, 2012). Certes, la préoccupation relative à la protection des données personnelles dans les bases de données est ancienne. Dans les années 1980, l'OCDE et le Conseil de l'Europe s'en saisissent ; dans les années 1990, c'est au tour de l'ONU. En 1995, le Parlement européen adopte la directive dont il a été question plus haut. Mais dans des conditions sociétales et technologiques différentes, par exemple quant à la nomadité des acteurs et à l'utilisation des réseaux. La mobilisation institutionnelle s'accélère une dizaine d'années plus tard. En 2008, la commission 36 de l'ISO ouvre un chantier sur cette question. Elle vient d'en publier la norme en 2012<sup>4</sup>. Par ailleurs, la commission 27 de

---

4. R. Fabre, J. Knoppers, ISO/IEC JTC1 SC36 Information technology – *Identification of Privacy Protection requirements pertaining to Learning, Education and Training (LET)* – Part 1: Framework and Reference Model, ISO/IEC FDIS 29187-1: 2012 (E), 29 02 2012

l'ISO centralise travaux et questions sur l'identité numérique<sup>5</sup>. En juin 2009, la Charte de Lisbonne stipule dans son article 8 que « toute personne a droit à la protection des données personnelles la concernant ». En 2009, le G29 met en chantier « le processus de Madrid »<sup>6</sup> devant produire des standards internationaux pour cette protection. Le G29 ou encore Groupe de travail (article 29) sur la protection des données est un organe consultatif européen indépendant (auquel s'ajoutent deux pays non européens) sur la protection des données et de la vie privée. Son organisation et ses missions sont définies par les articles 29 et 30 de la directive 95/46/CE, plusieurs fois citée, dont il tire sa dénomination, et par l'article 14 de la directive 97/66/CE. Il est présidé par Alex Türk. En mai 2010, le Parlement européen demande qu'une charte des droits des citoyens et des consommateurs sur Internet soit adoptée avant 2012. Toujours la même année, est lancée à Jérusalem une convocation internationale afin que ces standards soient mis au point pour 2012.

## Processus de Madrid : principes

Trois sources font actuellement référence pour la protection des données personnelles :

- Les lignes directrices de l'OCDE sur la protection de la vie privée et les flux transfrontières des flux de données à caractère personnel ;
- La directive 95/46/EC du Parlement Européen, déjà citée ;
- Le APEC Privacy Framework de 2005<sup>7</sup>.

Les 29 pays participant au processus de Madrid ont établi les principes de la protection de l'identité numérique personnelle, définissant ainsi un cadre lui-même normatif pour de futures politiques publiques dans ce domaine. Ces six principes, dont la norme ISO 29187 tient le plus grand compte, sont les suivants :

- licéité et loyauté – respect des droits, absence de discrimination : « Les Données Personnelles doivent être traitées loyalement, dans le respect de la loi nationale applicable et également des droits et libertés des

---

5. JTC1/SC27. Work and Projects in ISO/IEC JTC 1/SC 27/WG 5 « *Identity Management & Privacy technologies* » 2011-04-15 *ITSC Seminar International Standards for Information Security Singapore*. Convener WG 5[kai.rannenberg@m-chair.net] Kai Rannenberg, Goethe Frankfurt 1 Université de Francfort, Allemagne.

6. États et ONG (ISO, par exemple) se sont réunis à Genève début décembre 2011

7. Pour de plus amples renseignements, voir FABRE et KNOPPERS, *op. cit.*

individus, conformément au présent Document et en conformité avec les objectifs et principes de la Déclaration Universelle des Droits de l'Homme et du Pacte international relatif aux droits civils et politiques » ;

- détermination des finalités – les données personnelles sont recueillies et traitées pour une seule finalité, sauf autorisation des personnes concernées : « Le traitement de données personnelles devrait être limité à la réalisation des finalités spécifiques, explicites et légitimes de la personne responsable... » ;

- proportionnalité – traitement pour le minimum nécessaire : « Le Traitement de Données Personnelles devrait être limité aux Traitements adéquats, pertinents, et non excessifs au regard des finalités fixées dans l'article précédent » ;

- qualité des données – données exactes, tenues à jour puis effacées ou rendues anonymes ;

- transparence – transparence, information des personnes concernées sur la finalité du traitement ;

- *Accountability* – rendre compte de l'observance des principes ;

- légitimité – préalable du consentement des personnes concernées : « [...] D'une manière générale, les Données Personnelles ne peuvent être traitées que dans l'une des situations suivantes :

- a) Après obtention du consentement libre, non ambigu et éclairé de la Personne Concernée ;

- b) Lorsque l'intérêt légitime de la Personne Responsable justifie le Traitement, dès lors que les intérêts légitimes, droits et libertés de la Personne Concernée ne prévalent pas ;

- c) Lorsque le Traitement est nécessaire au maintien ou à l'exécution d'une relation juridique entre la Personne Responsable et la Personne Concernée ;

- d) Lorsque le Traitement est nécessaire pour être en conformité avec une obligation imposée à la Personne Responsable par la législation nationale applicable, ou est mené par une autorité publique dans l'exercice de ses pouvoirs.

- e) Quand il existe des circonstances exceptionnelles qui menacent la vie, la santé ou la sécurité de la Personne Concernée ou d'une autre personne ».

L'énumération de ces principes, rapportée à la tâche immense en constante évolution d'encadrer les données relatives aux utilisateurs, montre à la fois la difficulté de l'exercice et la gravité de l'enjeu. Il y a au départ une pétition de principe sur la place du numérique dans la société. La société est-elle numérisée dans son essence – ce que pense sans doute une bonne partie de la génération dite Y ? Ou bien, est-il possible de délimiter encore une ligne de partage entre les fonctions de la société et leurs versants numé-

riques ? Plus que jamais, il est urgent de prendre position et ce devrait être une tâche impérative des institutions parlementaires. Car du choix qui aura été retenu dépendra la forme de la régulation à mettre en place.

En tout état de cause, un dispositif et une politique de médiation en découleront, ne serait-ce que pour des raisons de surcharges informationnelles inutiles. Mais comment en définir les critères ? Plusieurs facteurs entravent cette évolution, notamment la généralisation de la carte bancaire et l'achat sur *smartphone* à l'aide de *flashcodes* qui indiquent le numéro téléphonique ou le mail de l'acheteur, donc son identité. L'hypothèse du tiers de confiance semble s'éloigner aujourd'hui d'une réalisation proche sauf à ce que sortent des travaux du G29 une politique de médiation dont il est difficile de percevoir les contours.

Un concept qui sera d'utilité dans ces travaux est celui de *politique publique*. Nous assistons encore à une confusion urgente à dissiper, entre régime de l'application numérique et politique publique. On a commencé dans l'histoire de l'informatisation par des applications, puis ce furent des projets. Mais quand une collectivité territoriale, une entreprise fait un « projet » d'ampleur qui a des conséquences économiques, sociales, en termes d'emploi, il ne s'agit plus d'un projet mais d'une politique ; s'il s'agit de l'État, d'une politique publique. Cela signifie que doivent être posés et négociés en premier les objectifs dont découleront les modalités, y compris les principes de normalisation numérique. C'est peut-être dans cette inversion, mettant la finalité et le sens au premier plan, qu'il faudra rechercher une issue autre que celle de la protection de l'identité comme finalité première.

Pour clore cette réflexion, signalons deux alternatives à la recherche de l'identité, l'une complémentaire : le renforcement de l'identifiant, l'autre totalement différente, dénommée Singularité technologique. Les tenants de cette école de pensée estiment que le souci de préserver sa vie privée n'est plus une norme et que la transparence totale s'impose. Jusqu'au changement d'identité, si nécessaire après « banqueroute de la réputation » (TÜRK, 2011). L'autre alternative a été annoncée personnellement par le président Barack Obama. Relisons sa déclaration du 18 avril 2011 : « Cet identifiant sécurisé est le principal élément sorti d'un an de travail sur une nouvelle Stratégie nationale pour des identités en confiance dans le cyberspace (NSTIC). Le programme serait géré par le secteur privé, et accessible aux internautes souhaitant les utiliser, sans obligation. Il supprimerait la nécessité de mémoriser de multiples mots de passe ».

« Le résultat est que le consommateur peut utiliser son identifiant pour se connecter sur n'importe quel site Internet, avec plus de sécurité que ce qu'apportent les mots de passe », a assuré la Maison Blanche dans son commentaire en poursuivant : « Les consommateurs peuvent utiliser leur

identifiant pour prouver leur identité quand ils font des transactions sensibles, par exemple avec une banque, et sinon peuvent rester anonymes. »

Reste peut être un autre espoir. Des travaux en cours dans notre laboratoire relèvent que la génération des quinze ans est nettement plus circonspecte sur la question de l'identité à protéger et du risque à cet égard de la dissémination des traces numériques (TINGRY, 2011). Une sagesse serait-elle en train d'émerger ?

## CONCLUSION

Le futur de la protection de l'identité personnelle paraît aujourd'hui encore incertain. Le travail sur ces questions appelle une forte contribution de la recherche. Les premières disciplines à s'engager dans ce domaine furent le droit, l'économie des conventions et les sciences de l'information et de la communication (SIC). Le droit poursuit son investigation autour de la notion de procéduralisation contextuelle (LENOBLE, 2002). Lenoble explore depuis de nombreuses années la conceptualisation d'une construction de la règle juridique qui tiendrait compte de la complexité des contextes et de celle de leur évolution. Il plaide pour une réflexivité intense à ce sujet enveloppant son élaboration. Nous retrouvons la même contrainte dans le cas présent. Cela suggère deux choses : d'une part une régulation que l'on pourrait qualifier de glissante, qui s'ajusterait aux contextes au fur et à mesure qu'ils évoluent ; d'autre part, la construction de passerelles entre le droit et la normalisation numérique – la protection de l'identité numérique personnelle ne pouvant pas être traitée sans rapport fort et constant entre les deux univers concernés, celui de la norme juridique et celui de la norme numérique. Un tel va-et-vient constant est indispensable et, avec Renaud Fabre, nous avons entrepris un travail en ce sens. Ce qui permet de souligner au passage le caractère interdisciplinaire de cette recherche. L'économie des conventions a joué un rôle majeur dans ce champ en y introduisant le concept d'investissement de forme, et en montrant que les normes et les standards techniques en sont un. Peut-être, à propos du thème traité ici (celui de la personne), une relecture des *Économies de la grandeur* serait-elle opportune. Enfin, les sciences de l'information et de la communication sont convocables à de multiples entrées. Notre laboratoire travaille depuis 1999 sur les questions de standards pour l'accès au savoir en ligne, sans quoi sa circulation numérique – grand thème Infocom – serait impossible. Techniques documentaires, métadonnées, profils d'application, tous outils qui en relèvent, sont ici employés à la construction de dispositifs et à la modélisation

des conduites d'utilisateurs – modèles discutés servant à la construction de normes. Enfin la question posée ici, celle d'un espace public au sens d'une logique sociale procédurale et de la médiation qui s'y exercerait, devrait retenir l'attention des chercheurs en SIC, compte tenu de la nouveauté des problématiques et des enjeux de société.

## Références bibliographiques

- ARNAUD M., JUANALS B., PERRIAULT J., « Les identifiants numériques humains. Éléments pour un débat public », *Les Cahiers du numérique*, n° 2, 2002, p. 169-182.
- ARNAUD M., « Entre droit d'auteur et liberté des échanges : les métadonnées, objets informatiques, objets économiques », dans Jacques PERRIAULT et Céline VAGUER (dir.), *La norme numérique, savoir en ligne et Internet*, Paris, Éditions du CNRS, 2011.
- BREDUILLIEARD P., CORDELIER B., « Conditions de performativité des chartes d'utilisation des médias socionumériques en entreprise », Actes du Colloque, *In-formation et communications organisationnelles: entre normes et formes*, Colloque International PREFics, Rennes, 8-9 septembre 2011, p. 141-149.
- FABRE R., « La personne : une régulation par les normes ? », *Hermès*, n° 53, 2009, p. 175-181.
- FABRE R., KNOPPERS J., *Information technology – Identification of Privacy Protection requirements pertaining to Learning, Education and Training (LET)*, Part 1, Framework and Reference Model, ISO/IEC FDIS 29187-1, 2012.
- GRANJON F., « De quelques pathologies sociales de l'individualité numérique : exposition de soi et auto-réification sur les sites de réseaux sociaux », *Réseaux*, vol. 29, n° 167, 2011, p. 75-103.
- KESSOUS E., « La *privacy*, du substantiel au procédural : quels enjeux de normalisation ? », dans Céline VAGUER, Jacques PERRIAULT (dir.), *La norme numérique. Savoir en ligne et Internet*, Paris, CNRS Éditions, 2012.
- LENOBLE J., « L'Efficiencia de la gobernanza por el Derecho. Para una proceduralización contextual del derecho », *La Revue Canadienne Droit et Société (RCDS/CJLS)*, n° 1, 2002, p. 1-37.
- MIÈGE B., *L'Espace public contemporain. Approche info-communicationnelle*, Grenoble, PUG, 2010.
- PERRIAULT J., « Jeunes générations, réseaux et culture numérique », dans Thierry Gaudin (dir.), *Comment les techniques changent les sociétés*, Actes de colloque, Paris, L'Harmattan, 2010.

- PERRIAULT J., VAGUER C. (dir.), *La norme numérique. Savoir en ligne et Internet*, Paris, CNRS Éditions, 2012.
- RANNENBERG K., « Identity Management & Privacy technologies », *ITSC Seminar International Standards for Information Security*, Singapour, 15 avril 2011.
- TINGRY N., « La ville apprenante virtuelle », *Spécificités*, n° 3, 2011, p. 241-250.
- TÜRK A., *La vie privée en péril. Des citoyens sous contrôle*, Paris, Odile Jacob, 2011.
- WOLTON D., *Indiscipliné. Trente ans de recherche en communication*, Paris, Odile Jacob, 2012.