



**HAL**  
open science

# CHRONIQUE DU PROFIL IDENTITAIRE CONTINGENT

Claire Noy

► **To cite this version:**

Claire Noy. CHRONIQUE DU PROFIL IDENTITAIRE CONTINGENT. Les Cahiers du numérique, A paraître, 7 (1), p75-85. <10.3166/lcn.7.1.75-85>. <hal-04103954>

**HAL Id: hal-04103954**

**<https://hal.science/hal-04103954v1>**

Submitted on 12 Jun 2023

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire HAL, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.



HAL Authorization

# CHRONIQUE DU PROFIL IDENTITAIRE CONTINGENT

CLAIRE NOY

Nous proposons de travailler sur ce qui est construit ou induit à partir des éléments existants sur le web. On appellera *identité contingente* d'un individu, le profil nominatif qui découle d'une recherche sur ledit web. La contingence résulte de la prise en compte de nombreux paramètres afférents aux capacités du « chercheur », à son intentionnalité et ses pratiques. Le *profil identitaire contingent* (PIC), devient alors la caractéristique incontournable de l'individu, qu'il pratique le web ou non. Nous procédons à un repérage du PIC en nous basant sur une approche décrivant, en trois systèmes, le potentiel identitaire. Ensuite nous envisageons les quatre postures d'usage potentielles du web afin de les situer dans ces systèmes.

## Identité numérique et profil contingent

Nous proposons de nous interroger sur ce qui est construit (ou induit) au travers de ce concept d'identité numérique, à partir des éléments existants sur le web. Nous partons d'une identité numérique qui résulte d'une construction en partie auto-alimentée, tantôt interprétée, tantôt masquée, médiatisée par l'outil internet. « On pourrait la définir comme toute la sphère d'information, de contenu qui est rattaché à l'identité, la personnalité, l'édification d'une personne. Ce qui va, je dirais de l'identifiant de la personne, ce qui la désigne, à tous les contenus qui lui sont rattachés, notamment toutes les traces que la personne qui utilise un service numérique va provoquer (...)»<sup>1</sup>.

On appelle *identité contingente*, le profil nominatif qui découle d'une recherche sur le web. La contingence est induite par de nombreux paramètres et, en premier, par l'étendue du savoir-faire du « chercheur », de son projet et des ses usages. Ainsi entre l'internaute béotien qui introduit un nom dans son moteur de recherche pour retrouver un copain d'école et le chasseur de tête expert qui tente de profiler un cadre international, il existe un écart incommensurable. Le *profil identitaire contingent* ou PIC, devient une caractéristique incontournable de l'individu, qu'il pratique le web ou non. Le développement tentaculaire du web (et du web 2) provoque l'irruption de ce potentiel individuel d'informations plus ou moins accessibles, plus ou moins précises, plus ou moins maîtrisées, voire plus ou moins connues par l'acteur concerné.

Il est courant aujourd'hui d'entendre que l'on s'est fait googler ! Se faire googler<sup>2</sup> n'est déjà pas banal puisque selon la qualité de la recherche effectuée qui peut aller de la simple entrée de vos nom et prénom dans le moteur de recherche à un véritable data mining organisé via des métamoteurs.

Nous proposons de procéder à un repérage dudit PIC. Nous nous basons sur une approche décrivant, en trois systèmes, le potentiel identitaire. Ensuite nous envisageons les quatre postures d'usage potentielles du web afin de les situer dans ces systèmes.

### Les trois systèmes du PIC et ses composantes

Nous postulons que le PIC est nourri de trois système sources : les systèmes normé, interprétatif et putatif (masqué).

Au-delà des données classiquement répertoriées dans les champs de bases de données autorisées et dont la signification est en général assez explicitée, on assiste à la multiplication de données à caractère personnel d'une nature beaucoup plus informelle : productions et expressions diverses d'un individu, messages, contacts, relations et liens, jugements de ou à propos de la personne, commentaires, images, rumeurs, traces de passage ou d'usage... autant de "grains"

---

1. Entretien avec Nicolas Nova. Identité numérique mobile. <http://idn.ensad.fr/?p=1113>

2. Googler : verbe intransitif. Néologisme décrié par la société Google elle-même pour des questions de propriété intellectuelle. Acte de rechercher une information sur une personne (ou simplement effectuer une recherche) sur le moteur de recherche Google. <http://www.dicodunet.com/definitions/google/googler.htm>

d'information, jusqu'ici difficilement exploitables à grande échelle, mais dont la forme numérique permet désormais de faire plus aisément usage <sup>3</sup>.

Dans un article récent (août 2010), Bruce Schneier <sup>4</sup> fournit une taxonomie des données : données de service, données divulguées, données confiées, données accidentelles, données comportementales et données produites.

Partant de cette taxonomie, nous la complèterons avec de nouvelles formes de données contextualisées dans trois systèmes et permettant de voir ce processus dynamique de construction des identités numériques.

### ***Le système normé***

Il comprend toutes les données à faible variété, c'est-à-dire des informations factuelles qui ne peuvent entraîner que des déviations d'interprétation nulles ou faibles. Par exemple les données biométriques, le nom, le sexe... toutes les données officiellement enregistrées (pérennes) et non ambiguës. Lorsqu'un individu cherche à cerner son propre PIC, cet ensemble peut paraître simple à définir, mais demande en réalité un inventaire approfondi et pertinent. Ainsi on éliminera les données pouvant induire des interprétations. « Marié » offre peu de variété interprétative à l'inverse de divorcé deux fois, par exemple. Les sources de ces données sont plurielles, et vont de l'individu lui-même aux fournisseurs patentés d'informations (vente de fichiers nominatifs), en passant par des tiers officiels (état civil, justice, immigration,...), la presse (récit de faits divers, palmarès,..) ou non.

On peut trouver diverses catégories de données normées :

– Les « données de repérage » : les données que l'utilisateur confie à un site interactif afin de l'utiliser. Ces données peuvent inclure votre nom légal, votre âge, le numéro de votre carte de crédit.

– Les « données illustratives », données que l'utilisateur publie sur ses pages: billets de blogs, photographies, croquis, schéma, messages, commentaires.

– Les « données errantes », données que l'utilisateur publie sur les pages des autres. Ce sont le même type de données que les données divulguées, à la différence qu'une fois qu'elles sont postées, quelqu'un d'autre en a le contrôle.

– Les « données allogènes » sont celles que d'autres personnes publient à propos de l'utilisateur pour informer, rapporter des agissements connus, retracer des faits et gestes.

– Les « données de traçabilité » sont celles que le site recueille sur l'utilisateur en surveillant ce qu'il fait et avec qui il le fait. Il peut s'agir de jeux auxquels il joue, de sujets sur lesquels il écrit, des articles auxquels il accède.

– Les « données dérivées 1 » sont des données concernant l'utilisateur issues de toutes les autres données, sans interprétation sinon une extrapolation simple. Par exemple, si 80 % de vos

---

<sup>3</sup>. Kaplan D., « Le nouveau paysage des données personnelles: quelles conséquences sur les droits des individus ? *Comptes rendus Droits numériques, gouvernance de l'internet*, Identité numérique identités actives ». <http://www.internetactu.net/2009/04/03/>

<sup>4</sup>. [http://www.schneier.com/blog/archives/2010/08/a\\_taxonomy\\_of\\_s\\_1.html](http://www.schneier.com/blog/archives/2010/08/a_taxonomy_of_s_1.html).

A Revised Taxonomy of Social Networking Data, august 2010, Scheier B.

Schneier B., Ferguson N., Kohno T., *Cryptography Engineering: Design Principles et Practical Application*, Ed. John Wiley et Sons Ltd, 2010.

amis repérés s'auto-identifient comme francs maçons, on induira que vous êtes susceptible d'être franc maçon aussi.

Ces deux dernières catégories sont, pour nous, marginales sécantes du système suivant.

### ***Le système interprétatif***

Il donne à voir tous les éléments qui pourront être déstructurés et restructurés par les tiers, avec un potentiel de variété important. Il rajoute certains types de données telles que les données diffuses et constituées qui construisent une réalité augmentée dérivée :

– Les « données constituées », données mises en scène par l'auteur via photos, vidéos, illustration, mise en page, expression de goûts, playlist... et publiées en accès libre (sans contrôle d'accès ou mot de passe).

– Les « données dérivées 2 » : détournées ou interprétées comme nous venons de le voir ci-dessus, mais fusionnées avec des éléments extérieurs, eux-mêmes constitués d'informations alimentées par des tiers conscients (opinion des autres, récits incluant l'individu...).

– Les « données diffuses » faisant apparaître le nom à l'occasion d'un fait quelconque auquel la personne concernée a participé volontairement (liste, palmarès, pétition...) mais dont le domaine d'origine (sport, parti politique, syndicat, forum,...) connotera fortement le PIC.

### ***Le système putatif***

Il se veut réservoir d'information masquée. Lesdites informations ne sont rattachables à la personne en cause qu'après « investigation », « bidouillage » ou « espionnage ». En effet elles se réfèrent à une identité « rideau », sciemment mise en place par l'utilisateur, cachant ou floutant la vraie.

Ainsi l'usage de pseudonymes, d'avatars, de mots de passe... cherche à soustraire de l'accès public ces informations pour les réserver à un usage personnel ou à un cercle d'ayants droit. Toutefois, le verrouillage fiable des données exige un niveau de compétence supérieure à celle qu'exerce l'utilisateur lambda. Sans forcément évoquer les hackers, la seule utilisation des cookies, invisibles pour les béotiens, permet d'accéder à des données que l'individu souhaite garder secrètes.

Cette question de la sécurité du masquage d'items et de sa fiabilité ne doit pas être occultée, d'autant plus que les technologies évoluent vite et les enjeux de piratage peuvent s'avérer précieux. Le droit, qui est censé protéger l'individu contre ces ingérences indues, à lui-même du mal à suivre (voire précéder) les montages intrusifs plus ou moins malveillants.

Tout ce qui vient d'être dit, l'a été « ici et maintenant » selon un contexte socio juridique donné. L'idée de contingence impose que le PIC soit constamment (re)évalué à l'aune du changement dudit environnement.

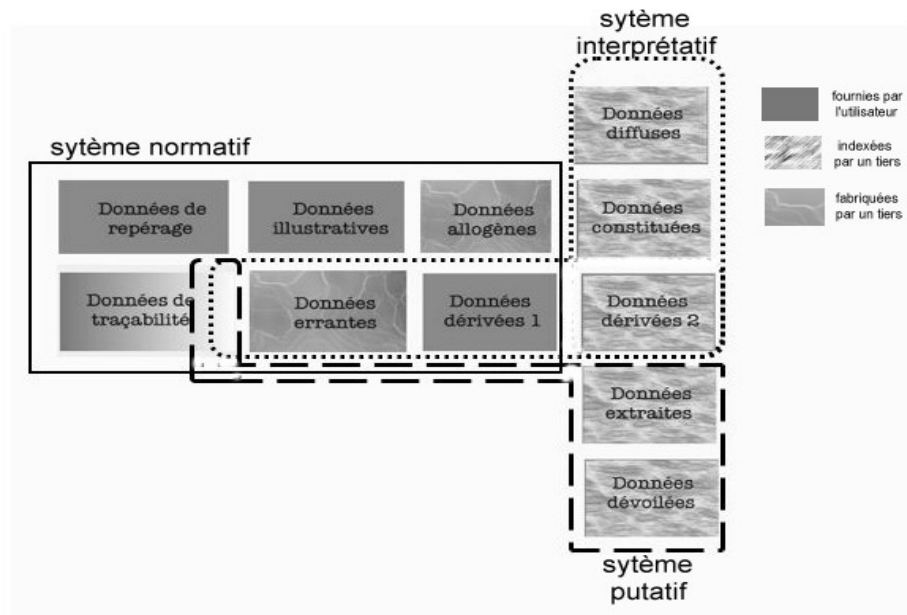


Figure 1. Systèmes et types de données

## Les postures potentielles d'usage du PIC

Nous envisageons quatre postures potentielles d'usage du potentiel identitaire contingent.

### *Usage réfractaire*

Certains individus, souvent non initiés à l'informatique en général ou à l'utilisation d'internet, certains non connectés au réseau, affichent un refus net des usages afférents. En partant du plus « simple », disons qu'un nombre d'individus non négligeable désirent s'exclure du web volontairement. Leur motivation première résulte d'une incompétence assumée vis-à-vis de l'outil et des dispositifs liés.

Une autre motivation s'inscrit dans la peur des conséquences mises en lumière par la presse tout public, concernant des problèmes liés au piratage des cartes bleues ou les avanies découlant de Facebook. Ce refus s'avère le plus souvent velléitaire puisque la possession d'un compte mail devient quasiment indispensable à ce jour et que par cette entrée, l'identité numérique va se constituer. À l'extrême, même des non utilisateurs stricts (non connectés, non producteurs de données) n'échappent pas à « la toile » via les données diffusées. Ne pas intervenir ce n'est pas ne pas exister en termes de PIC comme le croient trop de personnes mais exister passivement (identité numérique passive).

### *Usage inexpérimenté*

La sécurisation velléitaire situe une posture intermédiaire d'un usage désirant empêcher au maximum une « exploitation mauvaise ou malveillante » de son identité potentielle (identité numérique active). Or, la maîtrise experte de l'outil ordinateur, du dispositif réseau, des logiciels afférents, de la logistique des sites utilisés, du droit relatif au domaine... n'est pas une mince affaire. Elle commence par un certain nombre de recommandations minimales et une parcimonie d'usage des données du second système. Par exemple, éviter au maximum toutes les informations qui prêtent à interprétation (quasiment toutes !) en imaginant l'usage déviant qui peut en être fait.

Cette visibilité sociale numérique est vécue par ce type d'individus comme intrusive, passive, manipulable. Soit il va tenter de bloquer ladite visibilité par divers stratagèmes que permettent les sites de web 2. C'est ce que D. Cardon<sup>5</sup> appelle « le paravent ». Soit il décide de tracer une limite entre les informations tout public et les informations privées, réservées à un cercle étroit d'ayants droit. Ces dernières étant protégées par des barrières logicielles (mots de passe notamment). Ce « clair-obscur »<sup>6</sup> vaut ce que vaut la sécurisation d'accès. Au-delà de ce travail de précaution, le suivi de l'existant doit se faire périodiquement. L'individu concerné doit se préoccuper fréquemment de l'état et de l'évolution de son PIC et, le cas échéant faire corriger les atteintes à la qualité de ce dernier (mise à jour, suppression de situations inexacts, fermetures de pages...) en allant, le cas échéant, jusqu'à l'action judiciaire.

Pour inclure la dimension contingente concernant à la fois l'environnement, le contexte, mais aussi son projet, l'utilisateur doit se poser un nombre minimum de questions : que désirais-je pour mon e-réputation ? Dans quel but second (trouver un travail, trouver un partenaire, me faire valoir, avoir des contacts...) ? Ce questionnement induit que selon le moment de sa vie on peut avoir envie de changer profondément son PIC. Ce ne sera pas immédiat et il faudra s'y atteler progressivement, sciemment, en effaçant autant que possible les traces handicapant la nouvelle identité souhaitée. Des documentations nombreuses sont maintenant disponibles pour guider la sécurisation de son image numérique et de sa e-réputation. Ce peut être aussi l'occasion privilégiée pour faire appel à un véritable expert en la matière.

### *Usage narcissique*

D'autres internautes se veulent « un phare »<sup>7</sup> dans le web. Ce phare est souvent démultiplié par l'effet cumulatif des « amis » comme dans Facebook. Se retrouvent dans ces usages des personnes désirant utiliser le web pour « s'exposer », voire s'exhiber. Dans le premier cas se retrouvent à la fois les personnes qui usent de la possibilité de « s'exposer » en se googlisant elles-mêmes, celles qui « communiquent visuellement à distance », et celles qui usent des réseaux pour se mettre en évidence, en scène.

L'estime de soi, surtout quand elle ne résulte pas d'une évidence sociale, représente un besoin fort de nos sociétés. Selon les strates démographiques elle se manifeste de plusieurs façons. Pour faire simple, disons que chez les « juniors » elle se traduit par un affichage de performances et une affirmation de soi. Chez les seniors, elle consiste plutôt à un exercice de mémoire (exposé de souvenirs, de faits historiques, de photos d'antan). Se montrer sous des formes jugées valorisantes compense souvent un manque de « visibilité publique ». Ce peut être tout bonnement l'exposé de son quotidien : « Avec le lancement de Twitter on avait déjà passé un certain stade puisque certains

---

5. Le design de la visibilité : un essai de typologie du web 2.0. Dominique Cardon  
<http://www.jeunesse-vie-associative.gouv.fr/IMG/pdf/typo.pdf>.

6. Idem.

7. D. Cardon, idem.

n'hésitent pas à utiliser cette plateforme de micro-blogging pour annoncer qu'ils viennent de se lever, vont prendre une douche, vont aux toilettes, de quelle couleur et consistance... ! Bref, ça devient quasiment de l'exhibitionnisme électronique ! »<sup>8</sup>. Ces individus fournissent délibérément un très grand nombre d'informations sur eux-mêmes, afin de se faire valoir, de montrer une (ou plusieurs) de leurs points jugés forts, de se doter d'un réseau de relation, etc. Ainsi, au lieu de se protéger, un très grand nombre d'internautes sont engagés dans une débauche de visibilité. Axel Honneth pointe le manque fréquent de reconnaissance dans nos sociétés qu'il assimile à une « pathologie sociale », c'est-à-dire à « des relations ou des évolutions sociales qui portent atteinte aux conditions de réalisation de soi »<sup>9</sup>.

D'autres personnes se servent du réseau pour communiquer avec des tiers à distance. Cela peut aller des photos des enfants montrées à la famille jusqu'aux échanges érotiques. Enfin il existe une part non négligeable d'exhibitionnisme sur le web. La frontière qui sépare les narcissiques de ces derniers est ténue. Peut-être peut-on avancer que les exhibitionnistes s'adressent plus particulièrement à des voyeurs ? R. Redeker, dans *Medias*<sup>10</sup>, avance : « Une familiarisation avec ce réseau fait rapidement ressortir une autre caractéristique, moins reluisante que la socialisation : Facebook est surtout un média d'exhibition à laquelle la socialisation sert de masque. ». Il existe même une dialectique qui rend le narcissique ductile aux sollicitations des voyeurs en le transformant par petites touches en un « exhibitionniste passif ». Pastinelli (2007) décrit cette dialectique à la perfection : « Il y a du voyeurisme sur l'intimité des autres, un jeu de révélations. Mais aussi un consentement à avoir une certaine transparence, ou une prétention de transparence vis-à-vis des autres ». Le curseur intentionnel va ainsi du narcissisme naïf à l'exhibition manipulée. Tout cela génère des flux considérables. Uniquement en termes de photos, les chiffres parlent d'eux-mêmes... 750 millions de photos postées sur Facebook pour le nouvel an 2011, 6 milliards de photos chargées par mois, 60 milliards de photos fin 2010, 100 milliards de photos à l'été 2011 (estimation)<sup>11</sup>.

### ***Usage exploitant***

Les individus concernés fournissent délibérément un grand nombre d'informations sur eux-mêmes, mise en forme pour un projet bien particulier et maîtrisé. Par exemple un site en ligne comme Soovox<sup>12</sup> se propose de fournir à l'internaute intéressé son « score » social classé en sept échelons (Newbie, Legit, Emcee, Socialite, Transcender, Cultuforce, Mogul) en se basant sur votre environnement social, vos compte sur le web2 (et autres réseaux à venir) et la « buzzsphere ». Cette exploitation de rentabilisation d'image, aussi appelée *personal branding*, consiste à tenter de se démarquer pour susciter de l'intérêt en valorisant son PIC (personnalité, expériences, valeurs, talents, etc.) à l'instar d'une marque commerciale et en le diffusant de façon maîtrisée. « C'est un processus qui permet de clarifier et de communiquer sur ce qui vous rend unique. Comprendre vos caractéristiques, atouts, valeurs et passions. C'est aussi simple (en apparence) que d'être Soi dans une société où nous avons été entraînés à gommer nos différences et à entrer dans des moules ! »<sup>13</sup>.

---

<sup>8</sup>. Exhibitionnisme 2.0 : extensions Firefox et sites sociaux pour partager son historique web. 22 Septembre 2008 <http://www.business-garden.com>

<sup>9</sup>. Honneth A. La société du mépris – Vers une nouvelle théorie critique. Paris, La Découverte, collection Armillaire, 2006, p. 179.

<sup>10</sup>. <http://www.revue-medias.com/facebook-narcissisme-et,594.html>

<sup>11</sup>. Source : Pixable, <http://www.pixable.com/blog/2011/02/14>

<sup>12</sup>. <http://soovox.com/>

<sup>13</sup>. Définition *Personal Branding*, <http://www.blogpersonalbranding.com>

La procédure peut revêtir deux stratégies opposées : soit la stratégie « post it »<sup>14</sup>, soit la stratégie « vitrine ». La première consiste à semer de nombreuses marques ou références qui permettront à un googliseur de reconstruire une image très positive de l'individu, d'autant plus crédible qu'il l'aura lui-même (apparemment) confectionné comme un puzzle. La seconde, moins risquée, tend à canaliser le googliseur vers un site personnel riche et valorisant, la vitrine de l'individu. La crédibilité est évidemment moins « objective » mais joue sur la qualité de la facture du site, sa fonctionnalité, sa structuration... Il s'agit là de deux approches opposées, et le marketing personnel sera fertile en positionnements différentiels. Pour se démarquer de l'usage précédent il s'agit ici de nourrir un projet qui dépasse le seul motif de s'afficher, d'exploiter le maximum des possibilités offertes par les réseaux sociaux pour parvenir à un but prédéterminé.

### **Pour ne pas conclure**

Nous éviterons de conclure sur un sujet éminemment évolutif. Comme toujours dans ces technologies et technosciences médiatiques, l'observateur s'avère toujours écartelé entre la fascination et la terreur. Terreur d'une intrusion implacable dans son intimité privative. Fascination d'une socialisation « augmentée ». Aujourd'hui la nébuleuse des réseaux sociaux accumule les données des utilisateurs actifs ou passifs afin de créer de la visibilité sociale débouchant sur de la (pseudo) valeur ajoutée potentielle pour des usages divers, en complément de l'utilisation normale des applications. Nous finirons avec une citation de B. Le Gendre qui illustre bien cette problématique de l'identité numérique telle que nous avons voulu la présenter : « Tel le Petit Poucet, l'homo numericus laisse des cailloux blancs partout : courriels, blogs, chats, texto, recherches Google, achats en ligne... Chaque jour c'est une part de notre moi que nous abandonnons ainsi à l'Ogre. Jusqu'où ira sa voracité ? »<sup>15</sup>.

### **Bibliographie**

Abu S., *De l'identité et du sens, la mondialisation de l'angoisse identitaire et sa signification plurielle*, Paris, Perrin, 2009.

Berger P., Luckmann T., *La construction sociale de la réalité*, Paris, Méridiens Klincksieck, 1986.

Blin T., *Phénoménologie de l'action sociale. A partir d'Alfred Schütz*, Paris, L'Harmattan, 1999.

Desgens Pasanau G., Freyssinet E., *L'identité à l'ère du numérique*, Paris, Dalloz, 2009.

Gauthier A., *Le virtuel au quotidien*, Belfort, les éditions Circé, 2002.

Javeau C., *Le bricolage du social*, Paris, PUF, coll. Sociologie d'aujourd'hui, 2001.

Kaplan D., *Informatique, libertés, identités*, Limoges, Fyp, 2010.

Meirieu P., *Repères pour un monde sans repères*, Paris, Desclée de Brouwer, 2002.

Morin E., *Introduction à la pensée complexe*, Paris, ESF éditeur, coll. Communication et complexité, 2<sup>e</sup> tirage, mars 1991.

Morin E., *La méthode*, Paris, Seuil, 1977.

Nel N., (Sous la dir. de) *Les enjeux du virtuel*, Paris, L'Harmattan, 2001.

---

<sup>14</sup>. D. Cardon *op. cit.*

<sup>15</sup>. B. Le Gendre. *Notre moi et son double numérique*. <http://www.lemonde.fr>. 14 juin 2009.

Pastinelli M., *Des souris, des hommes et des femmes au village global. Parole, pratiques identitaires et lien social dans un espace de bavardage électronique*, Presses de l'Université de Laval, Laboratoire de communautique appliquée, Canada, mars 2007.

Pignier N., *De l'expérience multimédia. Usages et Pratiques culturelles*. Paris, Hermès-Lavoisier, 2009.

Queau P., *Le virtuel, vertus ou vertiges*, Seyssel, Champ Vallon, 1993.

Serres M., *Le temps des crises*, Paris, Ed. le pommier, 2009.

Schieir B., Ferguson N., Kohno T., *Cryptography Engineering: Design Principles et Practical Application*, Ed. John Wiley et Sons Ltd, 2010.

Tricot A., Rouet J.-F. (sous la dir. de), *Les hypermédias, approches cognitives et ergonomiques*, Paris, **Hermès Science Publications**, 1998.