

# *Un enjeu pour l'enseignement* **Comprendre l'identité numérique**

François Filliettaz

Direction des systèmes d'information et service écoles-médias (DSI-SEM)

Version 1.0, janvier 2011



© Chappatte - [www.globecartoon.com/dessin](http://www.globecartoon.com/dessin) – dessin publié avec l'autorisation de l'auteur.



Ce document est publié par le DIP Genève sous licence Creative Commons utilisation sans modification autorisée sous conditions: <http://www.ge.ch/sem/cc/by-nc-nd/>

Nota Bene: dans le but de simplifier la lecture de ce document, les termes qui se rapportent à des personnes exerçant des charges, mandats ou fonctions (enseignants, collaborateurs...) s'appliquent indifféremment aux hommes et aux femmes.

## Table des matières

<b>1.Objectif.....</b>	<b>3</b>
<b>2.Introduction.....</b>	<b>3</b>
<b>3. Identité et sphère privée.....</b>	<b>4</b>
3.1.Définition de l'identité.....	4
3.2.Les données personnelles.....	5
3.3.La vie privée.....	6
3.4.Faut-il changer de paradigme?.....	7
3.5.Les motivations à agir.....	7
<b>4. Identité numérique, une réalité mouvante.....</b>	<b>8</b>
4.1.Définition de l'identité numérique.....	8
4.2. Identité numérique et construction sociale.....	10
4.3.Médias sociaux et constitution de l'identité numérique.....	12
4.4. Identité numérique et personnalité.....	13
<b>5.Construire une identité numérique.....</b>	<b>14</b>
5.1.Utiliser les bons outils.....	14
5.2.Comment j'aimerais qu'on me voie ?.....	14
5.3.Trouver la bonne exposition de soi.....	15
5.4.Quelle stratégie ?.....	15
5.5.Quel media choisir ?.....	15
5.6.Améliorer sa e-réputation.....	16
5.7.Avatars et anonymat .....	17
<b>6.Réseaux sociaux et politiques de confidentialité.....</b>	<b>17</b>
<b>7.Quid du droit à l'oubli ?.....</b>	<b>18</b>
<b>8.Conclusion.....</b>	<b>19</b>
<b>9.Dix points à retenir.....</b>	<b>20</b>

# 1. Objectif

Le but de ce guide est de donner les informations et les indications pratiques qui permettront une utilisation responsable d'Internet à l'école et en dehors.

Il cherche à situer le problème de l'identité numérique sur Internet dans une perspective nouvelle, éloignée des considérations restrictives et peu pédagogiques qui ont encore souvent cours aujourd'hui. Il n'a cependant pas pour but de donner une position unique sur les enjeux liés à l'identité numérique, mais doit permettre à chacun de les appréhender.

Ce guide s'adresse principalement au corps enseignant et aux directions d'école et, d'une manière générale, à tous les protagonistes du système scolaire.

Il reste « en construction », c'est-à-dire qu'il sera régulièrement adapté à l'évolution du sujet.

# 2. Introduction

D'un côté, le monde réel, dans lequel nous avons un nom, une adresse, où des éléments indiscutables permettent de confirmer que nous, c'est nous. De l'autre, un nouvel espace informatisé qui ne prend forme qu'habillé des pixels de nos écrans, où les éléments les plus fiables nous identifient à notre insu (qui connaît le numéro IP de son ordinateur, et combien connaissent même son existence ?), où des millions d'ombres aux noms bizarres semblent autant de menaces à nos individualités estampillées. Mais une fois la crainte dissipée par l'attrait de ce jeu, quand nous avançons masqués, à l'image de **Descartes, premier avatar**, et jouissons de cette liberté nouvelle, nous apprenons, parfois à nos dépens, que l'écran derrière lequel nous croyions être à l'abri n'est même pas un rideau de fumée, et que nous semons les pièces d'un puzzle le long des chemins, qu'il suffira de rassembler pour reconstituer notre identité véritable, bien réelle. Pire, on nous met en garde : ce puzzle dit nos convictions, nos vertus et bien sûr nos vices, et tout cela pourrait le moment venu être retenu contre nous.

Qu'en est-il vraiment ? Faut-il protéger et interdire, bloquer les accès aux sites les plus « risqués », ou au contraire informer et former les nouvelles générations

**Plutôt qu'interdire l'accès aux sites risqués, il vaut mieux former et informer.**

à la gestion de ces risques, sachant que ce nouveau monde est pour elles le nouvel espace public ? C'est bien sûr cette seconde alternative qui sera développée ici, la compréhension des concepts et des bonnes pratiques étant la meilleure manière de contenir les risques dans une mesure raisonnable. Il n'est pas plus question de les éliminer sur Internet que dans la « vraie vie », et

comme dans celle-ci, le rôle des écoles est d'aider les jeunes à les affronter et surtout à les maîtriser.

L'époque des craintes irraisonnées est révolue, de nombreuses recherches ont montré que les jeunes sont beaucoup plus habiles et rationnels qu'on ne le pense généralement dans la gestion de leur identité en ligne. Mais pour qui n'est pas déjà immergé dans ce « nouveau monde », il est essentiel de comprendre qu'il s'agit bien d'un nouvel espace public qui ne peut être occupé que par des identités privées, numériques et variables au gré des nécessités. Et comme l'identité piagétienne dans la « vraie vie », cette identité numérique se construit ou se péjore au gré des navigations et des rencontres dans cet espace d'un nouveau genre.

Quelques affirmations pour commencer, qui situent le contexte de l'identité numérique:

« Il y a eu 5 exabytes (10<sup>18</sup> octets) d'informations créées depuis la naissance de la civilisation jusqu'en 2003. Mais cette même quantité d'information est maintenant créée tous les deux jours et cette rapidité augmente... Les gens ne sont pas prêts pour la révolution technologique qu'ils vont subir... Si j'ai suffisamment de vos messages à disposition et que je connais les endroits où vous vous trouvez, je peux, en utilisant de l'intelligence artificielle, prédire où vous allez aller. Montrez nous 14 photos de vous et nous pouvons vous identifier. Vous pensez qu'il n'y a pas 14 images de vous sur l'Internet? » Eric Schmidt, PDG de Google

Le métier de Google est de monétiser ces mêmes données.



René Descartes, Larvatus prodeo : « Je m'avance masqué. » (*Cogitationes privatae*)

L'avatar est un personnage représentant un utilisateur sur internet et dans les jeux vidéo. Peut être créé pour des raisons ludiques, pour simplement représenter un internaute, de manière anonyme ou non, ou être un avatar utilitaire, utilisable par exemple dans des simulateurs ou processus d'apprentissage à distance ou jeux pédagogiques évolués.

En 1999 déjà, le président de *Sun*, Scott McNealy lançait : « Vous n'avez déjà plus de vie privée, il faut vous y faire!<sup>1</sup> »

L'identité numérique doit pourtant s'envisager de manière positive. Pour l'essentiel, elle n'est que le prolongement de notre vie quotidienne, le miroir de nos activités. Nous en avons encore la maîtrise.

## 3. Identité et sphère privée

### 3.1. Définition de l'identité

La société doit définir des critères précis pour identifier et individualiser ses membres. Des critères prédéfinis par la loi s'appliquent à tous les citoyens pour garantir leur unicité juridique, alors que d'autres considérations bien différentes vont être retenues pour circonscrire leur personnalité. Celle-ci aura éventuellement une valeur dans la sphère juridique dans le cas où elle pourrait permettre d'éclairer certains comportements, et augmenter ou diminuer la responsabilité des auteurs d'actes délictueux ou criminels.

L'*identité* se définit de plusieurs manières :

- Elle est l'ensemble identique d'éléments descriptifs (nom, prénom, date de naissance, sexe, etc.) d'individus différents (mais qui peuvent partager des goûts, des comportements...).
- Elle est la somme des différences (forcément relatives) qui composent un individu unique.

Il existe donc une identité par regroupement de critères – sociale – et une identité par distinction ou discrimination – individuelle.

**Sur Internet,  
la personnalité  
est l'ensemble  
des comportements  
et préférences  
qui caractérisent  
une personne.**

Autre composante essentielle de l'identité sur Internet, la *personnalité* est l'ensemble des comportements et préférences qui caractérisent une personne, et qui permet à une autre personne ou organisation de la qualifier, d'expliquer ses actes, ses motivations, etc. Sa détermination est extérieure au sujet, par exemple un profil de personnalité fabriqué automatiquement par un site de vente en ligne, qui comprendra votre identité (nom, adresse, numéro de carte de crédit, etc.) et vos préférences : achats antérieurs, recherches et autres informations permettant de prédire que tel ou tel produit aura une forte chance de vous intéresser et d'être acheté par vous.

L'identité qui nous intéresse ici est donc l'ensemble des caractéristiques énoncées par un individu, autrui ou une entité organisationnelle (administration, entreprise..) à son propos. Sa détermination est externe, officielle ou non, elle a une grande importance sociale.

Cette *nouvelle identité* est l'intersection de trois éléments : le corps (sexe, taille, corpulence, couleur de la peau, etc.), le groupe (famille, école, clubs, etc.), et le Moi, creuset où se fond l'identité, où elle s'écrit, se construit, se « fictionnalise »<sup>2</sup>. Elle est dynamique et s'actualise sans cesse dans les intentions et relations que nous entretenons avec nous-mêmes, les autres et nos objets d'intérêt. Elle est le flux des fictions entretenues sur et par un individu. Avec cette définition, il est possible de comprendre l'évolution de l'*identité en ligne*.

Pour comprendre les difficultés et les éventuels risques causés aux individus par la navigation sur Internet, il faut mesurer l'effet de la publication (divulguer, rendre publique, partager) de ce qu'on appelle les « données personnelles », notion juridique protégée dans la loi.

<sup>1</sup> Cité par Daniel Kaplan, Informatique, libertés, identités, Fing #08, éditions FYP 2010, p. 63

<sup>2</sup> Lionel Naccache, *Le Nouvel Inconscient Freud, le Christophe Colomb des neurosciences*, Odile Jacob Poches, 2006, 2009. « Fictionnaliser »: Transformer quelque chose de réel en fiction, en inventant des mobiles imaginaires, en oubliant et/ou en ajoutant des faits, etc. Selon les neurosciences, il s'agirait du fonctionnement normal de la conscience, Freud n'ayant pas découvert les mécanismes d'un inconscient introuvable dans la description qu'il en a fait, mais bien ceux de la conscience.

## 3.2. Les données personnelles

En Suisse, les données personnelles désignent toutes les informations qui se rapportent à une personne identifiée ou identifiable<sup>3</sup>.

Données qui permettent l'identification directe ou indirecte d'une personne physique ou morale : nom, prénom, adresse e-mail, numéro de téléphone, date de naissance, etc. Ces données ne peuvent être collectées, traitées et conservées que si une déclaration à l'autorité a été faite au préalable.

**Les données personnelles sont désormais des données qui ne le sont plus.**

On appelle *données sensibles* les données personnelles qui permettent de déterminer les origines raciales, les opinions politiques, philosophiques ou religieuses, les appartenances syndicales ou les mœurs d'une personne. Les données de santé sont également assimilées à des données sensibles, ainsi que les données sur les poursuites, les sanctions pénales ou administratives. Il est absolument interdit de les collecter, de les traiter ou de les conserver sans autorisation.

« Les données personnelles sont aujourd'hui l'une des matières premières de l'économie numérique, elles permettent de construire des relations, elles sont la substance des services et des produits. Nos lois en matière de vie privée sont anciennes. Elles étaient certes prophétiques, mais elles ont toutes entre 30 et 35 ans. Elles se sont adaptées, mais les données personnelles à l'époque, on savait où elles étaient, on savait qui les collectait, on les produisait de manière consciente permettant de déclarer des fichiers, et on savait où elles étaient physiquement stockées. Or, tout cela a changé. Les données personnelles sont désormais des données qui ne le sont plus. Il suffit d'en recouper quelques-unes pour pouvoir nous réidentifier. Elles sont produites par des objets qu'on achète ou utilise ou porte, elles sont produites par les autres (qui parlent de nous, nous étiquettent) et par nous. Elles sont des sous-produits de toutes les activités humaines qui ont un substrat numérique. Elles ont tendance à se dupliquer tant et si bien qu'on ne sait plus où elles sont.<sup>4</sup>» Daniel Kaplan, délégué général de la FING<sup>5</sup>

«Il est illusoire de croire que les services sur Internet sont gratuits; on les paie en fournissant des données personnelles. Toutes les offres Internet ont pour objectif premier de rassembler un maximum de données personnelles, afin de générer des recettes publicitaires.» Hanspeter Thür, préposé fédéral à la protection des données

Sur la page d'information au public du préposé fédéral à la protection des données, on peut lire également cet avertissement: « Les services de réseautage social (SRS) sont le plus souvent gratuits, mais ce ne sont pas des institutions d'intérêt public. Il y a « marchandage »: ils offrent des prestations aux utilisateurs en échange des données personnelles de ces derniers. Derrière ces portails se cache un pouvoir commercial redoutable incarné par de puissantes multinationales qui doivent générer des profits croissants sous la pression des investisseurs et des actionnaires. Les SRS n'ont que des données personnelles à offrir ; la valeur boursière de certains de ces sites en dit long sur l'intérêt que présentent ces données»<sup>6</sup>.

Les réseaux sociaux mettent à la disposition des spammeurs une quantité d'informations: les outils de recherche permettent de sélectionner des segments démographiques donnés, et les pages de fans et les groupes permettent d'envoyer des messages à tous les inscrits qui partagent les mêmes intérêts.

Beaucoup d'informations ne sont pas a priori personnelles, mais elles peuvent le devenir a posteriori grâce au **data mining**, par recoupements, analyse, traitement sémantique, etc.

Les données personnelles, une fois saisies sur les réseaux sociaux, appartiennent à l'entreprise qui gère le site, conformément au contrat de licence d'utilisation accepté au moment de l'inscription. Elles peuvent donc être retravaillées et diffusées, y compris des années plus tard.



Le *Data mining* a pour objet l'extraction d'un savoir ou d'une connaissance à partir de grandes quantités de données, par des méthodes automatiques ou semi-automatiques.

<sup>3</sup> Loi fédérale sur la protection des données, Art. 3 [http://admin.ch/ch/fr/rs/235\\_1/a3.html](http://admin.ch/ch/fr/rs/235_1/a3.html)

<sup>4</sup> Daniel Kaplan, Lift 2010 [http://www.internetactu.net/2010/07/19/maitriser-sa-vie-privee/?utm\\_source=feedburner&utm\\_medium=feed&utm\\_campaign=Feed%3A+internetactu%2FbcmJ+%28InternetActu.net%29](http://www.internetactu.net/2010/07/19/maitriser-sa-vie-privee/?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+internetactu%2FbcmJ+%28InternetActu.net%29)

<sup>5</sup> Site de la FING : <http://fing.org/>

<sup>6</sup> Pages d'informations au public du Préposé fédéral à la protection des données et à la transparence (PFPDT) : <http://www.edoeb.admin.ch/themen/00794/01124/01254/index.html?lang=fr&lang=fr>

### 3.3. La vie privée

La vie privée repose sur le comportement (ce que nous voulons partager), la propriété (le contrôle des données) et ce que les autres peuvent faire avec nos données.

Pour les générations nées avant les années 80, la vie privée est encore un bien quasi sacré qu'il faut protéger à tout prix. Pour les générations ultérieures, depuis les **digital natives**, accoutumés aux caméras de surveillance et à la traçabilité des communications, elle n'est plus un objet particulier idéalisé, séparé de son support. Elle est par exemple sur *Facebook*, nouvel espace public et privé, lieu de rencontre et d'exposition de soi.

« L'avenir de la vie privée est de la maîtriser. Ce qui mérite d'être défendu, c'est la vie privée comme base de l'autonomie personnelle. C'est la vie privée qui me permet de revenir sur mon expérience pour décider ce que je veux faire. La vie privée est une tête de pont pour se projeter. La valeur de la vie privée est de nous permettre d'avoir une vie publique. La protection et la projection de soi sont si liées dans les aspirations, qu'elles nécessitent de repenser les outils qui doivent nous permettre de réaliser nos aspirations. La société doit offrir à ses membres des lois et des règles pour protéger la vie privée, mais nous devons également équiper et outiller les individus pour atteindre la capacité à se projeter. » D.Kaplan



Le *Digital native* est une personne ayant grandi dans un environnement numérique comme celui des ordinateurs, Internet, les téléphones mobiles et les baladeurs MP3. Génération née après 1980.

La question n'est plus tant celle de la vie privée que celle de la vie publique, puisqu'il est tout à fait possible d'avoir une vie privée dans un espace public. C'est le cas sur *Facebook* quand les utilisateurs vivent consciemment une vie publique en se mettant en scène, en divulguant des données de leur vie privée. Il ne s'agit plus seulement de protéger la circulation et l'usage des données personnelles. Les individus défendent encore (pas toujours) leur vie privée, mais ils cherchent surtout à affirmer leur identité et leur personnalité publique dans un monde en réseaux.

#### Le vrai problème de la protection de la vie privée réside dans la récolte et l'exploitation des traces.

Sont-ils pour autant irresponsables ? Pas du tout, relève Danah Boyd<sup>7</sup>, spécialiste des réseaux sociaux : « Quand, par défaut, notre vie est privée, on doit faire attention à ce que l'on rend public. Mais quand, par défaut, ce que l'on fait est public, on devient très conscient des enjeux liés à sa vie privée. Et je pense que les gens n'ont jamais été aussi soucieux de leur vie privée. Parce que l'on ne veut pas partager tout ce que l'on fait, tout le temps, avec tout le monde et n'importe qui. »

Le vrai problème de la protection de la vie privée est ailleurs, dans la récolte et l'exploitation des traces : recherches sur *Google* mémorisées, visites aux sites enregistrées et conservées par les fournisseurs d'accès, destinataires de nos courriers électroniques ; toutes ces informations peuvent aussi, en plus de servir à la surveillance, être agrégées et vendues pour définir des profils individuels indispensables aux spammeurs et autres marchands sur le net. Et, plus simplement, un employé indélicat de *Google* peut aller fouiller dans les emails d'un utilisateur<sup>8</sup>...

Pourtant, des chercheurs ont identifié un comportement particulier des utilisateurs du net, qu'ils ont appelé le « paradoxe de la vie privée »<sup>9</sup> : bien qu'il se sentent de plus en plus sous surveillance, ces utilisateurs seraient de plus en plus enclins à tout laisser savoir d'eux-même. Mais des chercheurs<sup>10</sup> contestent que les jeunes disent tout et n'importe quoi sur les sites sociaux ; ils voient au contraire une forme de rationalité dans leurs comportements – très ciblés en fonction des sites et des publics visés selon un vrai calcul coûts/bénéfices – et une gestion souvent clairvoyante des risques. Et cela irait de pair avec un glissement de certaines données personnelles sensibles d'un statut protégé vers un statut plus indifférent. Ce serait le cas des préférences sexuelles et des opinions politiques.

<sup>7</sup> Sur le site de Dana Boyd, *Public by Default, Private when Necessary*, [http://www.zephorias.org/thoughts/archives/2010/01/25/public\\_by\\_defau.html](http://www.zephorias.org/thoughts/archives/2010/01/25/public_by_defau.html)

<sup>8</sup> Article de ZDnet, *Un ingénieur de Google pris en flagrant délit d'espionnage de données privées*, <http://www.zdnet.fr/actualites/un-ingenieur-de-google-pris-en-flagrant-delict-d-espionnage-de-donnees-privées-39754595.htm#xtor=RSS-8>

<sup>9</sup> Commission européenne, *Young People and Emerging Digital Services: An Exploratory Survey on Motivations, Perceptions and Acceptance of Risks* : <http://ipts.jrc.ec.europa.eu/publications/pub.cfm?id=2119>

<sup>10</sup> Daniel Kaplan, op. cit

### 3.4. Faut-il changer de paradigme?

Les réponses contemporaines à ces nouveaux environnements numériques visent le plus souvent « à empêcher la collecte de certains types de données, à en restreindre l'exploitation ou à interdire certaines pratiques issues de leur exploitation<sup>11</sup> ». Mais face aux exabytes de données créées journalièrement, la tâche est clairement impossible. De nouvelles propositions ont été avancées, qui visent à résoudre le problème d'une manière globale : la transparence absolue, l'anonymat et la propriété des données personnelles. Mais il est douteux qu'on puisse résoudre les problèmes liés aux données personnelles grâce à la pression sociale (transparence), au droit (anonymat) ou à l'économie (propriété). Aucune de ces solutions n'apportent de réponse valable aux aspirations des utilisateurs du web.

### 3.5. Les motivations à agir

Pour mieux cerner les motivations des utilisateurs du web vis-à-vis de leurs données personnelles, **Daniel Kaplan**<sup>12</sup> propose quatre moteurs, auxquels il faudra donner un poids différent selon les types de relation envisagés : la construction de soi, la maîtrise de l'information, la commodité et la valorisation de soi.



Daniel Kaplan est le délégué général de la Fondation pour l'Internet Nouvelle Génération (FING), un projet collectif et ouvert qui se consacre à repérer, stimuler et valoriser l'innovation dans les services et les usages du numérique et des réseaux. Il préside également l'Institut européen du e-learning (EifEL). Il a été désigné en 2002 par le magazine Newbiz comme l'une des 100 personnalités qui « font vraiment bouger la France ».

#### La construction de soi

« Le monde numérique offre à cette construction identitaire un formidable terrain de jeu. Il permet tout à la fois de tester plusieurs manières d'être (plusieurs identités plus ou moins cloisonnées et pérennes), d'analyser ce que les autres nous renvoient, de construire une mémoire personnelle, de se comparer et s'évaluer, de rejoindre et abandonner différentes communautés, etc. »

#### La maîtrise de l'information

« La propension des individus à dévoiler des informations sur eux et à négliger l'usage de la plupart des dispositifs destinés à minimiser le risque de collecte ou d'usage abusif de leurs données ne signifie nullement qu'ils ne prêtent aucune attention à ces questions. Ils se protègent, mais si le jeu en vaut la chandelle. Souvent, de fait, ils négocient. [...] En matière de maîtrise, on confond trop souvent sécurité et contrôle. La sécurité consiste à s'assurer que ses données personnelles ne sont pas compromises, transmises par effraction à qui n'en a pas l'autorisation. Le contrôle consiste à vérifier que ceux qui ont l'autorisation de détenir certaines de ses données personnelles n'en abusent pas. Mais l'attente de maîtrise ne se limite pas à cela. A nouveau, l'identité de chacun est une construction jamais achevée, un périmètre jamais clos. Il ne suffit pas de la protéger comme un bien précieux; gérer son image et sa réputation, se présenter sous son meilleur jour, d'une manière adaptée à différents interlocuteurs, relève également de la maîtrise. »

#### La commodité

« Tout ce qui fera gagner du temps, tout ce qui réduira le besoin de mémoriser soi-même une multitude d'informations, tout ce qui assurera un accès de qualité et sans peine aux ressources ou aux interlocuteurs qui comptent, a une valeur. Et cette valeur, nous sommes souvent trop heureux de la payer en information plutôt qu'en argent : par exemple en laissant des sites inscrire des cookies, des petits fichiers relatifs à nos visites, qui permettent de nous reconnaître la fois suivante. Nous la payons également en acceptant certains risques. [...] La puissance de la commodité est telle, qu'elle conduit des millions d'utilisateurs à confier la quasi-totalité de leurs données à des plateformes qui gèrent désormais leurs agendas, leurs carnets d'adresses, leur correspondance et leurs documents : le **cloud computing** ou l'informatique dans le nuage, dont Google (avec Google Docs, Gmail, etc.) est le plus important représentant, correspond à un transfert massif de données ultra-personnelles depuis les disques durs des utilisateurs vers ceux de prestataires dont une partie du modèle d'affaires repose sur l'exploitation de ces données. »



Le *Cloud computing* revient à déporter sur des serveurs distants des traitements informatiques traditionnellement localisés sur le poste utilisateur.

<sup>11</sup> PDF: <http://weblaw.haifa.ac.il/he/Faculty/Zarsky/Publications/zarsky-miami.pdf>

<sup>12</sup> Daniel Kaplan, op.cit, p. 52 ss.

## La valorisation de soi

« Les gens ont de multiples raisons de divulguer, diffuser, voire de publier des informations qui les concernent : être appelés par un employeur ou un client, élargir leur cercle de relations, se faire proposer des produits qu'ils aiment... Après tout, l'identité ne s'affirme qu'en s'éprouvant au contact des autres. »

Le Web2.0, en autorisant la publication de contenus autrefois confidentiels, permet le partage et la coopération. Tout peut se partager, les idées, les photos, les vidéos, les recettes, etc. Mais pour cela il faut rendre publiques des données personnelles, et accepter les retours des autres, positifs et négatifs, qui participeront à la construction de l'identité.

L'éditeur Tim O'Reilly<sup>13</sup> pense qu'il est temps de revoir nos certitudes concernant les informations personnelles et leur utilisation : «L'ancien modèle défendant la confidentialité des données personnelles ne prend en compte aucun bénéfice éventuel lié à son renoncement ; et pourtant, ces bénéfices se font cruellement attendre aujourd'hui<sup>14</sup>».

## 4. Identité numérique, une réalité mouvante

### 4.1. Définition de l'identité numérique

L'identité sur le Net se définit comme la somme des données et des traces associées au nom (nom, prénom, pseudo). Les données sont l'ensemble des informations entrées dans les formulaires sur les sites (nom, prénom, pseudo, sexe, date de naissance, adresse, etc.).

Les traces numériques sont l'ensemble des articles, commentaires, vidéos, photos, avis (par exemple «J'aime» sur *Facebook*) dont nous avons parsemé le web, mais aussi ce qu'ont déposé les autres à notre sujet.

L'identité numérique est une forme particulière d'identité. Elle est multiforme, et sans cesse variable. Elle augmente au gré de mes navigations et peut ne pas correspondre du tout à mes données personnelles. Pour la comprendre, il faut introduire le concept de trace dans un univers informatique :

- **Identité numérique** : identité gérée via une interface informatique connectée à un réseau.
- **Identité (numérique)** : somme de mes traces techniques: adresse IP, cookies, navigateur, recherches sur moteurs de recherche web, recherches internes dans les sites visités, etc. 84% des combinaisons système d'exploitation / navigateurs / plug-ins / etc. sont absolument uniques. Et comme elles ne sont pas camouflées (ni par la désactivation des cookies, ni par la navigation privée), chaque ordinateur laisse donc une empreinte unique, permettant de dresser le profil d'un internaute et de voir quand il se reconnecte. Si le système peut permettre d'identifier des fraudes, il permet surtout d'identifier les utilisateurs. L'*Electronic Frontier Foundation* propose un site pour dévoiler aux utilisateurs ce que leur navigateur dit d'eux<sup>15</sup>.
- **Traces « profilaires »** : ce que je dis de moi = qui je suis.
- **Traces « navigationnelles »** : où je vais, qui je lis, où je commente = comment je me comporte.
- **Traces « inscriptibles »** : ce que j'exprime, publie, édite = ce que je pense<sup>16</sup> (d'après Olivier Ertzscheid).

L'identité numérique est multiple : alimentée par nos traces et celles déposées par d'autres, elle repose sur ce qu'on dit et comment cela est perçu (commentaires laissés par les lecteurs), sur les éléments associés (photos, vidéos, sons) et sur le réseau des relations et son fonctionnement.

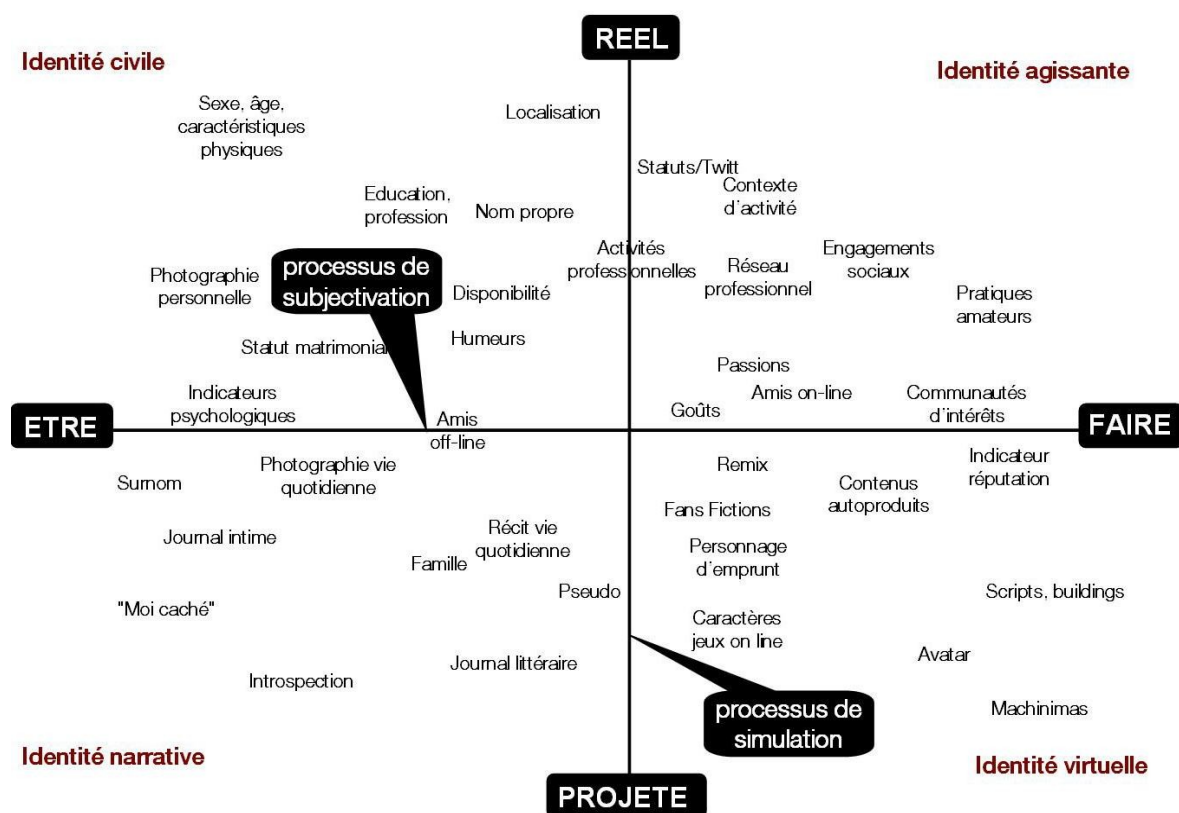
<sup>13</sup> [http://fr.wikipedia.org/wiki/Tim\\_O'Reilly](http://fr.wikipedia.org/wiki/Tim_O'Reilly)

<sup>14</sup> Article de ReadWriteWeb, *Pour Tim O'Reilly, améliorer le monde vaut bien un peu de vie privée* : [http://fr.readwriteweb.com/2010/08/02/a-la-une/tim-oreilly-amliorer-monde-vaut-bien-peu-de-vie-prive/?utm\\_source=feedburner&utm\\_medium=feed&utm\\_campaign=Feed%3A+readwriteweb-france+%28ReadWriteWeb+France%29](http://fr.readwriteweb.com/2010/08/02/a-la-une/tim-oreilly-amliorer-monde-vaut-bien-peu-de-vie-prive/?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+readwriteweb-france+%28ReadWriteWeb+France%29)

<sup>15</sup> Site mis à disposition par l'Electronic Frontier Fondation : <http://panopticlick.eff.org/>

<sup>16</sup> D'après Olivier Ertzscheid, [http://affordance.typepad.com/mon\\_weblog/2010/05/identite-numerique-ereputation.html](http://affordance.typepad.com/mon_weblog/2010/05/identite-numerique-ereputation.html)

La représentation ci-dessous permet de mieux comprendre la fictionnalisation à l'œuvre dans l'identité numérique. Si les deux identités virtuelle et narrative vont de soi dans cette optique, il faut y inclure les deux autres, agissante et civile, qui n'offrent dès lors aucune des garanties qui leurs sont attribuées dans la « vraie vie ».



Source: <http://www.internetactu.net/2008/02/01/le-design-de-la-visibilite-un-essai-de-typologie-du-web-20/>

Les traces profilaires et inscriptibles sont potentiellement les plus dangereuses, car elles ont une vie longue, très longue, souvent bien plus longue qu'on ne l'aimerait. Et elles peuvent avoir dans notre présent une importance qu'on ne soupçonnait pas 10 ans auparavant.

La très jeune génération numérique n'a que peu conscience de l'impact des traces qu'elle laisse au gré de ses navigations. Elle a une vision plutôt ludique du web, et les conséquences éventuelles de ses traces sur une encore bien lointaine recherche d'emploi, par exemple, ne la préoccupe pas encore. Mais plus elle vieillit, plus elle en est consciente et adapte ses comportements<sup>17</sup>.

Facebook semble renoncer (temporairement ?) à sa vision du « tout visible par tous » au profit d'un contrôle différencié par l'utilisateur, qui ne risque plus de partager sans le savoir des données qu'il pensait privées<sup>18</sup>.

<sup>17</sup> Fréquence écoles, *Comprendre le comportement des enfants et adolescents sur internet pour les protéger des dangers* : <http://www.frequence-ecoles.org/education:ressources/view/id/37c48d9366cfe18d321ef6e1db77cd38>

<sup>18</sup> Article de Zdnet, *Facebook élargit ses outils de contrôle des données personnelles* : <http://www.zdnet.fr/actualites/facebook-elargit-ses-outils-de-contrôle-des-données-personnelles-39755199.htm#xtor=RSS-8>

## 4.2. Identité numérique et construction sociale

L'identité a une composante sociale forte. Nom et prénom viennent des parents, ainsi que le milieu dans lequel l'individu va se développer et acquérir, ou non, des habiletés et des connaissances. Ces dernières vont déterminer ce qu'il saura faire, et serviront de base à sa réputation sur Internet, avec ses goûts, ses loisirs etc., en fonction des traces laissées dans les différents sites.

Dans la représentation ci-après, qui ajoute une couche à la précédente, on peut identifier les sites associés aux différentes identités. Apparaissent aussi cinq formats de visibilité<sup>19</sup>, définis par le sociologue **Dominique Cardon** :



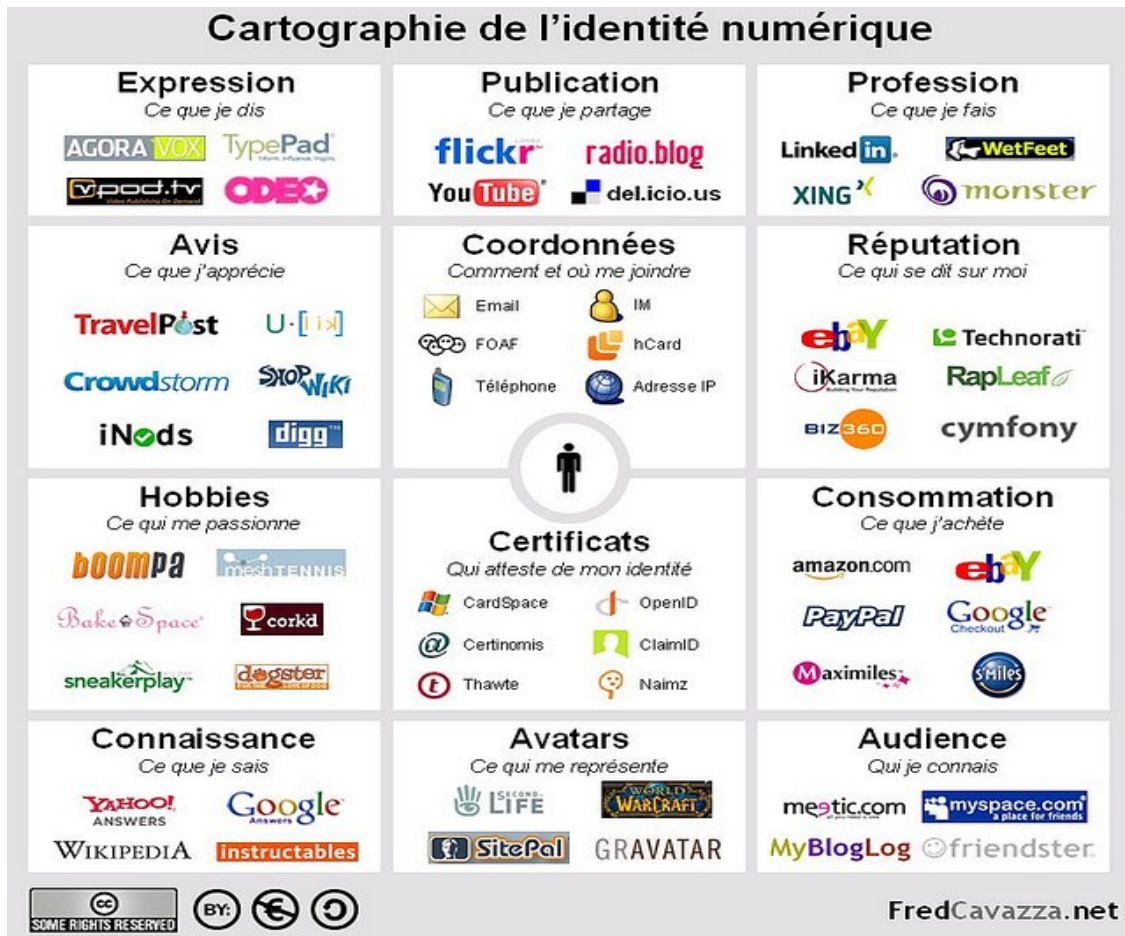
Dominique Cardon est sociologue au Laboratoire des usages de France Télécom R&D et chercheur associé au Centre d'étude des mouvements sociaux de l'École des Hautes Études en Sciences sociales (CEMS/EHESS). Ses travaux portent sur les relations entre les usages des nouvelles technologies et les pratiques culturelles et médiatiques. L'articulation entre sociabilités et espace public est à l'origine de différents travaux portant sur les pratiques culturelles, les médias alternatifs ou les programmes télévisés « interactifs ».

- **Le paravent.** Les participants ne sont visibles aux autres qu'à travers un moteur de recherche fonctionnant sur des critères objectifs. Ils restent « cachés » derrière des catégories qui les décrivent et ne se dévoilent réellement qu'au cas par cas dans l'interaction avec la personne de leur choix.
- **Le clair-obscur.** Les participants rendent visibles leur intimité, leur quotidien et leur vie sociale, mais ils s'adressent principalement à un réseau social de proches et sont difficilement accessibles pour les autres. La visibilité en clair-obscur est un principe de toutes les plateformes relationnelles qui privilégient les échanges entre petits réseaux de proches (*Cyworld*, *Skyblog*, *Friendster*). Si les personnes se dévoilent beaucoup, elles ont l'impression de ne le faire que devant un petit cercle d'amis, souvent connus dans la vie réelle.
- **Le phare.** Les participants rendent visibles de nombreux traits de leur identité, leurs goûts et leurs productions et sont facilement accessibles à tous. En partageant des contenus, les personnes créent de grands réseaux relationnels qui favorisent des contacts beaucoup plus nombreux, la rencontre avec des inconnus et la recherche d'une audience. La photo (*Flickr*), la musique (*MySpace*) ou la vidéo (*YouTube*) constituent alors autant de moyens de montrer à tous ses centres d'intérêt et ses compétences et de créer des collectifs fondés sur les contenus partagés.
- **Le post-it.** Les participants rendent visibles leur disponibilité et leur présence en multipliant les indices contextuels, mais ils réservent cet accès à un cercle relationnel restreint (*Twitter*, *Dodgeball*). Les plateformes fonctionnant sur le modèle du post-it se caractérisent par un couplage très fort du territoire (notamment à travers les services de géolocalisation) et du temps (notamment afin de planifier de façon souple des rencontres dans la vie réelle).
- **La lanterna magica.** Les participants prennent la forme d'avatars qu'ils personnalisent en découplant leur identité réelle de celle qu'ils endossent dans le monde virtuel (*Second Life*). Venant de l'univers des jeux en ligne (*World of Warcraft*), les avatars se libèrent des contraintes des scénarios de jeu pour faire des participants les concepteurs de leur identité, de l'environnement, des actions et des événements auxquels ils prennent part. Dans ces univers, l'opération de transformation, voire de métamorphose, identitaire facilite et désinhibe la circulation et les nouvelles rencontres à l'intérieur du monde de la plateforme, tout en rendant encore rare l'articulation avec l'identité et la vie réelles des personnes.

Cette représentation met en lumière les principales formes de fiction et de dissimulation offertes aux internautes. Offertes, car il faut bien réaliser que ce jeu de masques est en quelque sorte consubstantiel à l'Internet d'aujourd'hui.

<sup>19</sup> Article d'InternetActu, *Le design de la visibilité : un essai de typologie du web 2.0* : <http://www.internetactu.net/2008/02/01/le-design-de-la-visibilite-un-essai-de-typologie-du-web-20/>





### 4.3. Médias sociaux et constitution de l'identité numérique

Les médias sociaux jouent un rôle très important dans la récolte et l'analyse des données personnelles et autres informations. Des algorithmes très sophistiqués permettent d'innombrables recoupements, qui sont autant d'atteintes potentielles à la sphère privée. La typologie suivante donne une idée de l'étendue des données qui sont collectées :

- Des « **données de services** » : les données que l'on confie à un site social afin de l'utiliser. Ces données peuvent inclure votre nom légal, votre âge voir le numéro de votre carte de crédit ou celui de votre téléphone.
- Les « **données divulguées** », c'est-à-dire celles que l'utilisateur publie sur ses pages : billets de blogs, photographies, messages, commentaires.
- Les « **données confiées** », c'est-à-dire celles 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 fortuites** » sont celles que d'autres personnes publient à votre propos.
- Les « **données comportementales** » sont celles que le site recueille sur vous en enregistrant ce que vous faites et avec qui vous le faites. Il peut s'agir de jeux auxquels vous jouez, des sujets sur lesquels vous écrivez, des articles auxquels vous accédez (qui permettent de prévoir votre appartenance politique), votre préférence sexuelle, vos petites manies personnelles, vos goûts culinaires et vos loisirs favoris.

- Les « **données dérivées** » sont des données concernant l'utilisateur issu de toutes les autres données. Par exemple, si 80% de vos amis s'auto-identifient comme gays, vous êtes susceptibles d'être gay à votre tour<sup>22</sup>.
- Les « **données d'appréciation** », résultant des différents clics sur « J'aime », « Je n'aime pas », devenir membre d'un groupe, etc.

On voit ainsi que toute action sur un site social produit de l'information utilisable, qui permettra en temps voulu des recoupements ou la constitution de profils. Aujourd'hui des quantités inimaginables de données sont collectées, mais elles ne peuvent être exploitées à fond, faute de puissances informatiques suffisantes. Mais pour combien de temps encore ?

#### 4.4. Identité numérique et personnalité

L'identité en ligne est particulière. Elle n'est pas obligatoirement liée à la personne, qui peut se présenter comme bon lui semble, être unique ou multiple, authentique ou purement imaginaire, de n'importe quel sexe, de n'importe quel âge. Elle permet aussi à l'individu d'expérimenter différentes facettes de sa personnalité dans différents contextes de rencontres et d'échanges. Cette possibilité est bien sûr une nouveauté dans le processus de maturation des individus et elle correspond à une génération pour laquelle le « signe de passage » à l'âge adulte est la possession d'un téléphone portable, et non plus la cigarette.

Des psychologues, dont **John Suler**<sup>23</sup>, se sont intéressés à cette multiplicité possible, et ont identifié cinq facteurs de l'identité en ligne :

- **Niveau de dissociation et d'intégration**  
Il existe des niches pour chaque facette de la personnalité. Nul besoin de se présenter comme un tout, chaque aspect de la personnalité peut être mis en avant d'une manière totalement autonome. Le travail d'intégration, si important dans la réalité, est mis en veille.
- **Valence positive et négative**  
Les aspects positifs ou négatifs de la personnalité peuvent s'exprimer sur Internet, agressivité ou compassion, déviance ou conformisme rigide.
- **Niveau de fantasme et de réalité**  
Identité réelle (par convention : âge, sexe, lieu de résidence, profession) ou imaginaire (réelle elle aussi puisqu'endossée par un Moi bien réel, même s'il s' imagine migré dans le monde des Idées), les sites ont des exigences très variables, permettant l'expression de toutes les facettes d'une personnalité.
- **Niveau de contrôle conscient**  
Selon Suler, l'inconscient serait à l'œuvre dans le choix des avatars, des différentes identités ou des groupes choisis. La fictionnalisation explique ces comportements sans faire appel au concept d'inconscient, et donne une explication plus simple et plus claire.
- **Média choisi**  
Forums, blogs, messageries instantanées, sites sociaux, sites personnels, tous sont des moyens d'expression différenciés pour le Moi, qui les utilisera selon ses préférences et inclinations. Internet est un espace illimité pour expérimenter tout ou parties d'une personnalité à multiples facettes, souvent retenue, en réalité, dans un carcan convenable et conventionnel. On a pu parler de « tourisme identitaire<sup>24</sup> » à propos des possibilités offertes par les avatars.



John Suler est professeur de psychologie à la Rider University dans le New Jersey (USA). De nombreux travaux et recherches de John Suler portent sur la psychologie du cyber-espace et des réseaux sociaux. Il les voit comme une extension du psychisme individuel.

<sup>22</sup> Article d'InternetActu, *Taxonomie des données sociales* : [http://www.internetactu.net/2010/09/02/taxonomie-des-donnees-sociales/utm\\_source=feedburner&utm\\_medium=feed&utm\\_campaign=Feed](http://www.internetactu.net/2010/09/02/taxonomie-des-donnees-sociales/utm_source=feedburner&utm_medium=feed&utm_campaign=Feed)

<sup>23</sup> The Psychology of Cyberspace, <http://www-usr.rider.edu/~suler/psycyber/psycyber.html>

<sup>24</sup> Lisa Nakamura, *Race In/For Cyberspace: Identity Tourism and Racial Passing on the Internet*, : <http://www.humanities.uci.edu/mposter/syllabi/readings/nakamura.html>

## 5. Construire une identité numérique

L'identité numérique, on l'a vu, n'est pas donnée. Elle se construit et évolue au gré des rencontres et des visites sur le web. Mais pour ne pas se retrouver un jour à regretter amèrement son ou ses identité(s) passée(s), il faut exercer un minimum de contrôle sur les traces qu'on a et va laisser. Pour cela, il faut un peu de réflexion, quelques outils ciblés, du bon sens et de la curiosité. Il est vivement conseillé de vérifier régulièrement que notre identité n'a pas été usurpée (nom ou pseudo) ou qu'un(e) homonyme n'est pas en train de détruire notre réputation.<sup>25</sup>

### 5.1. Utiliser les bons outils

D'abord se demander : que peut-on voir de nous ? Et faire le tour des principaux moteurs de recherche spécialisés dans la quête des traces. Un site simplifiera grandement la tâche : <http://www.tahitidocs.com/outils/traces/signature.html>. Entrez vos nom et prénom(s), et passez successivement en revue tous les sites en liens.

Pour des requêtes encore plus pointues, visiter les sites suivants, tous spécialisés dans la recherche de traces sur Internet :

#### Contenus indexés

<http://www.yasni.ch/>  
<http://snitch.name/>  
<http://www.spokey.com>  
<http://Pipl.com>  
<http://yonline.com>  
<http://checkusernames.com>  
<http://fauxlowers.com/>  
<http://http://youopenbook.org/>  
<http://webmii.com/Default.aspx>

Vérifier sur <http://knowem.com/> que le pseudo utilisé ou envisagé et le nom ne sont pas déjà utilisés par d'autres. A noter que ce site peut, pour une certaine de francs, faire changer le nom sous lequel on s'est inscrit sur les différents réseaux sociaux.

#### Contenus non-indexés

Accessibles par les moteurs de recherche internes des réseaux, inaccessibles depuis l'extérieur. Ces contenus sont une partie essentielle de l'identité numérique et de la réputation sur le web.

Pour rechercher des informations sur les réseaux où on a déjà créé un profil, utiliser namechk : <http://namechk.com/> qui permet aussi de découvrir d'éventuelles usurpations d'identité, ou plus simplement des homonymes.

### 5.2. Comment j'aimerais qu'on me voie ?

Le site <http://sociogeek.admin-mag.com/> permet de prendre conscience de l'effet produit sur la réputation par certaines photographies ou certaines informations. Il vaut la peine d'y passer un moment.

Quelles informations peuvent être rendues publiques ? Quelles informations pouvant avoir un impact négatif sur l'e-reputation doivent être gardées pour soi ?

Ne pas oublier que ce qui peut nous valoriser aujourd'hui dans un petit groupe d'amis peut avoir plus tard des conséquences graves dans des cercles plus larges tels que celui des employeurs potentiels ou ceux de la vie publique et politique.

<sup>25</sup> Présentation *Comment construire son identité numérique* : <http://www.slideshare.net/batier/comment-construire-son-identite-numerique> , et *Guide pratique de l'E-Réputation à l'usage des Individus* : [http://digitalreputationblog.com/wp-content/uploads/2010/09/Guide\\_Pratique\\_E\\_Reputation\\_Usage\\_Individus.pdf](http://digitalreputationblog.com/wp-content/uploads/2010/09/Guide_Pratique_E_Reputation_Usage_Individus.pdf)

### 5.3. Trouver la bonne exposition de soi

Se poser les « bonnes » questions pour atteindre l'adéquation entre les actions en ligne et les objectifs :

- Pourquoi être présent sur le web ?
- Quelle image de moi mes profils et traces doivent-ils refléter ?
- Quelles informations peuvent être visibles, publiques ou privées ?
- Dois-je montrer des images de moi, ou des avatars, ou rien du tout ?
- Puis-je multiplier mes identités: nom réel, pseudonymes ?
- Mon objectif est-il de me faire connaître, de gagner en légitimité dans une communauté, de démontrer mon expertise ?

### 5.4. Quelle stratégie ?

Une fois les raisons d'une présence sur Internet définies (simple présence, audience, recherche d'amis, recherche d'emploi, etc), pour donner un sens à la démarche, il faudra mettre en place une stratégie, avec des objectifs le plus souvent qualitatifs. Et à chaque fois, on ne divulguera que les informations et les données essentielles pour atteindre le but, mais rien de plus. On se souviendra que toute information laissée sur le web peut permettre des analyses et éventuellement des recoupements, et faciliter ainsi notre identification quand nous utilisons un pseudo ou un avatar.

Un site permet de réfléchir à une stratégie, et aide à la mettre en place :

<http://ahtgroup.com/services/social-media-strategies>

### 5.5. Quel media choisir ?

Parmi les centaines de réseaux sociaux actifs dans le monde, il est possible de faire une première distinction entre réseaux généralistes comme *Facebook* et *MySpace*, réseaux mi-généralistes mi-professionnels comme *Twitter* et réseaux professionnels comme *LinkedIn* et *Viadeo*.



## 5.6. Améliorer sa e-réputation

La réputation sur internet se définit ainsi : perception, évaluation, opinion que l'on se fait d'un individu, d'une marque ou d'une entreprise à partir de son identité numérique. Ce qu'on dit de moi, ma marque (*personal branding*<sup>26</sup>), mes traces; elle est subjective et fluctuante. Elle se constitue autour de concepts comme confiance et crédibilité. Elle se construit et se déconstruit, mais est plus que la somme de confiance + crédibilité : elle est devenue la notion centrale dans l'économie de l'accès.

### 77% des recruteurs effectuent des recherches en ligne

Sur Internet, aujourd'hui l'absence devient suspecte. Individus et entreprises ont intérêt à y être, mais cette présence demande beaucoup d'attention : mise à jour régulière, interactions avec les pairs et les membres du réseau, partager toutes sortes d'informations. On ne valorise pas son identité numérique en créant simplement des profils sur les réseaux sociaux ; un compte très détaillé, mais laissé à l'abandon aura un impact négatif sur la notoriété.

Quelques chiffres cités par *techcrunch*<sup>27</sup> :

- 77% des recruteurs effectuent des recherches en ligne. Une étude américaine<sup>28</sup> constate que 45% des employeurs américains déclarent utiliser les réseaux sociaux pour recueillir des informations sur les candidats à une embauche. D'après une très récente étude de la HEG de Genève, ils seraient près de 15% en Suisse. Mais certains pays veulent empêcher cette pratique<sup>29</sup>.
- 35% des recruteurs ont déjà éliminé un candidat en se basant sur les résultats de leurs recherches.
- 7% de toutes les requêtes effectuées sur les moteurs se font sur le nom d'une personne. On a vu plus haut quelques outils qui peuvent servir aussi à surveiller une réputation. Autre outil très efficace: le système d'alerte proposé par *Google*, qui avertit quand un nouvel article sur le thème recherché est découvert par le moteur de recherche: <http://www.google.ch/alerts?hl=fr>.

En cas d'atteinte à l'image personnelle, il ne faut pas hésiter à demander un droit de rectification aux sites qui diffusent cette mauvaise image et à *Google* de désindexer les pages concernées. Il existe aussi des sites spécialisés, comme *ReputationDefender*: <http://www.reputationdefender.com/>, qui publie toutes sortes d'informations utiles, et peut aussi agir pour corriger une image défectueuse.

Dans les cas extrêmes, mais sans aucune garantie de réussite à 100%, on peut faire appel à des sites spécialisés dans la destruction de la présence sur Internet, qui proposent des marches à suivre<sup>30</sup>.

De très nombreux sites offrent des services de restauration d'image<sup>31</sup>, c'est aujourd'hui un marché appelé à un très fort développement.

<sup>26</sup> Blog du Modérateur, *Le personal branding au service de l'entreprise* : <http://moderateur.blog.regionsjob.com/index.php/post/Le-personal-branding-au-service-de-l-entreprise>

<sup>27</sup> Article de TechCrunch, *Réputation en ligne : c'est parti* : <http://fr.techcrunch.com/2007/11/27/fr-reputation-en-ligne-cest-parti/>

<sup>28</sup> *More Employers Screening Candidates via Social Networking Sites* : [http://www.careerbuilder.com/Article/CB-1337-Getting-Hired-More-Employers-Screening-Candidates-via-Social-Networking-Sites/?ArticleID=1337&cbRecursionCnt=1&cbid=372d16b8bb104c1e8040782018f41adc-335342726-VN-4&ns\\_siteid=ns\\_fr\\_g\\_careerbuilder\\_social](http://www.careerbuilder.com/Article/CB-1337-Getting-Hired-More-Employers-Screening-Candidates-via-Social-Networking-Sites/?ArticleID=1337&cbRecursionCnt=1&cbid=372d16b8bb104c1e8040782018f41adc-335342726-VN-4&ns_siteid=ns_fr_g_careerbuilder_social)

<sup>29</sup> *Germany Plans Limits on Facebook Use in Hiring* : [http://www.nytimes.com/2010/08/26/business/global/26fbbook.html?\\_r=2](http://www.nytimes.com/2010/08/26/business/global/26fbbook.html?_r=2)

<sup>30</sup> *How to Delete Yourself from the Internet* : <http://www.wikihow.com/Delete-Yourself-from-the-Internet>

<sup>31</sup> <http://caddereputation.over-blog.com/> , <http://www.spintank.fr/e-reputation-comment/>

## 5.7. Avatars et anonymat

Les avatars rassurent ; qui pourrait nous reconnaître derrière un faux nom et une image de Mickey ?

Malheureusement, la réalité est bien différente, et parfois très désagréable. Des utilisateurs anonymes, et bien sûr masqués, d'un site dédié à l'exposition des attributs virils ont ainsi eu la désagréable surprise de constater que n'importe qui pouvait les identifier sur une *GoogleMap* créée frauduleusement à partir de leurs adresses IP, enregistrées à leur insu par un hacker farceur.

**Les avatars ne garantissent pas l'anonymat.**

L'exploitation de plus en plus sophistiquée des traces laissées par la navigation sur Internet diminue chaque jour l'espace de liberté offert par l'anonymat, à moins d'utiliser des outils spécialisés comme *Tor*<sup>32</sup>, qui complique encore la recherche, mais ne garantit pas non plus l'impunité.

## 6. Réseaux sociaux et politiques de confidentialité

La politique de confidentialité d'un site peut changer d'un jour à l'autre, sans préavis et sans consultation préalable de ses membres. Des données qu'ils pensaient privées et réservées à un public restreint qu'ils avaient soigneusement délimité, se retrouvent ainsi accessibles par un plus grand nombre, sans qu'ils aient pu prendre des dispositions pour empêcher cette ouverture. On imagine sans peine les conséquences que peuvent avoir de telles décisions sur la réputation.

Pis encore, des failles de sécurité sont découvertes régulièrement dans *Facebook*. Par exemple:

« Les failles à base de CSRF et XSS décrites dans le détail par Wargan semblent aujourd'hui corrigées mais leur potentiel de nuisance – et même de destruction – peut vous coller une bonne trouille rétrospective, notamment dans la capacité qu'elles offraient à un utilisateur malveillant de s'emparer de l'intégralité de vos données privées ou – pire pour certains – de diffuser publiquement sur votre propre mur et celui des autres vos messages privés. Un peu comme si, sans le savoir, vous donniez les clés de votre boîte aux lettres à un inconnu et qu'il étalait toute votre correspondance sur le mur de votre immeuble, et celui de la mairie.<sup>33</sup> »  
Site du réseau Tor



Tim O'Reilly est le fondateur d'O'Reilly Media, une maison d'édition spécialisée dans l'informatique. Ses ouvrages et articles sont considérés comme des références par la communauté du World Wide Web. Il a été l'un des initiateurs du premier sommet de l'Open Source. Il a inventé l'expression Web 2.0.

Pour comprendre le problème en quelques clics, l'évolution de la protection des données sur *Facebook* est résumée ici: <http://mattmckeon.com/facebook-privacy/>

La question de la protection des données personnelles ou au contraire de l'ouverture vers plus de transparence occupe de nombreux chercheurs et juristes. Pour certains, le bénéfice individuel de l'ouverture serait bien plus important que celui de la fermeture. « Vous ne changez pas le monde en donnant aux gens ce qu'ils demandent, mais en leur donnant quelque chose dont ils ignorent avoir besoin »<sup>34</sup> affirme un spécialiste à propos du changement de politique de *Facebook*, qu'il défend<sup>35</sup>.

Pour Tim O'Reilly, déjà cité plus haut : « l'ancien modèle défendant la confidentialité des données personnelles ne prend en compte aucun bénéfice éventuel lié à son renoncement ; et pourtant, ces bénéfices se font cruellement attendre aujourd'hui.<sup>36</sup> »

<sup>32</sup>Site de Tor : <http://www.torproject.org/>

<sup>33</sup>Article de Presse-citron, *Facebook : méfiez-vous aussi des failles* : <http://www.presse-citron.net/facebook-mefiez-vous-aussi-des-failles>

<sup>34</sup>«You don't change the world by giving people what they say they want, but by giving them something they didn't know they needed»

<sup>35</sup> Article de WIRED, *What if the Facebook (Un)Privacy Revolution Is a Good Thing?*: [http://www.wired.com/epicenter/2010/05/facebook-firestorm-good-thing/?utm\\_source=feedburner&utm\\_medium=feed&utm\\_campaign=Feed%3A+wired%2Findex+%28Wired%3A+index+3+%28Top+Stories+2%29%29](http://www.wired.com/epicenter/2010/05/facebook-firestorm-good-thing/?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+wired%2Findex+%28Wired%3A+index+3+%28Top+Stories+2%29%29)

<sup>36</sup>Pour Tim O'Reilly, améliorer le monde vaut bien un peu de vie privée : [http://fr.readwriteweb.com/2010/08/02/a-la-une/tim-oreilly-amliorer-monde-vaut-bien-peu-de-vie-prive/?utm\\_source=feedburner&utm\\_medium=feed&utm\\_campaign=Feed%3A+readwriteweb-france+%28ReadWriteWeb+France%29](http://fr.readwriteweb.com/2010/08/02/a-la-une/tim-oreilly-amliorer-monde-vaut-bien-peu-de-vie-prive/?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+readwriteweb-france+%28ReadWriteWeb+France%29)

Ce débat, passionnant, sort du cadre de cette étude, mais il vaut la peine de le connaître pour s'attendre, dans un avenir proche, à des changements encore plus considérables que ceux qui ont agité les esprits à propos de *Facebook*.

Dans ce sens, un article récent de *Read Write Web*, « *Why Facebook Should Pass Out More, Not Less, User Info*<sup>37</sup> », reprenant un article du *Wall Street Journal* à propos des failles découvertes sur *Facebook*, ouvre un débat inimaginable il y a quelques années<sup>38</sup>. Le recoupement d'informations personnelles publiques y est banalisé et même encouragé.

**Les Etats se soucient à leur manière, forcément restrictive, de protection de la vie privée.**

Par exemple: « Les machines tracent ce que vous dites – mais est-ce une menace? Pour moi, c'est un bien social. »<sup>39</sup>

Et aussi: « J'aime l'expression de *gaz d'échappement de données*. Les gens dispersent tant d'informations sans intérêt et ennuyeuses prises

séparément, mais quand vous en possédez suffisamment, des structures émergent.<sup>40</sup>»

Il est impossible aujourd'hui de transférer l'ensemble des données déposées dans un site social sur un autre, prétendument plus digne de confiance. Fermer un compte revient à perdre tout son contenu, à moins d'en récupérer au préalable un à un tous les éléments par copier-coller; inimaginable dans la majorité des cas.

Les Etats se soucient à leur manière, forcément restrictive, de protection de la vie privée. La Résolution de Madrid<sup>41</sup> (2009) vise à l'élaboration d'une convention internationale spécifique. L'Assemblée nationale française lui apportera peut-être son soutien<sup>42</sup>.

## 7. Quid du droit à l'oubli ?

Autre question très débattue aujourd'hui, inverse de la précédente, le droit à l'oubli, contrairement à ce qu'il laisse entendre, n'est pas un droit reconnu dans la plupart des systèmes juridiques en matière de données numériques.

Il existe un droit à l'oubli pour certaines condamnations pénales, pour des procédures administratives (poursuites etc) et autres actes juridiques. La société en général et donc le droit, considèrent qu'il est nécessaire pour le bien de tous que de telles normes existent pour permettre à chacun de s'affranchir d'un passé peut-être lourd, mais qui ne menace pas la collectivité dans son ensemble, et garantir la possibilité d'un nouveau départ. Tout le monde doit pouvoir bénéficier d'une nouvelle chance, et cela passe par l'oubli. Mais aujourd'hui cet idéal est attaqué dans sa substance par la mémoire des réseaux, quand une information erronée peut ressurgir à tout moment en tête de liste dans une recherche sur *Google*, et un acquittement n'être référencé que dans les profondeurs jamais atteintes de la liste.

**Les vieux réflexes sécuritaires ont la vie dure, et la résistance au droit à l'oubli est loin de reculer.**

Un des aspects existants de ce droit à l'oubli est la prescription, qui s'applique, elle, même aux cas les plus graves. Mais si d'un côté on assiste à la montée d'une demande précise d'un droit à l'oubli sur Internet, on voit en même temps surgir des demandes inverses, qui aimeraient abolir l'oubli, et donc une forme de pardon temporel, et rendre imprescriptibles certains crimes. Les vieux réflexes sécuritaires ont la vie dure, et la résistance au droit à l'oubli sous toutes ses formes est loin de reculer.

<sup>37</sup> « Pourquoi Facebook devrait divulguer plus, pas moins, de données de ses utilisateurs ».

<sup>38</sup> Why Facebook Should Pass Out More, Not Less, User Info : [http://www.readwriteweb.com/archives/why\\_facebook\\_should\\_pass\\_out\\_more\\_not\\_less\\_user\\_in.php?utm\\_source=feedburner&utm\\_medium=feed&utm\\_campaign=Feed%3A+readwriteweb+%28ReadWriteWeb%29](http://www.readwriteweb.com/archives/why_facebook_should_pass_out_more_not_less_user_in.php?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+readwriteweb+%28ReadWriteWeb%29)

<sup>39</sup> "Machines are tracking what you say - but is that a threat? This looks like a social good to me"

<sup>40</sup> "I love the term 'data exhaust'. People are spewing out so much information that is completely non-sensitive and individually boring, but when you get enough of it patterns emerge"

<sup>41</sup> Wikipedia, article *Résolution de Madrid* : [http://fr.wikipedia.org/wiki/R%C3%A9solution\\_de\\_Madrid](http://fr.wikipedia.org/wiki/R%C3%A9solution_de_Madrid)

<sup>42</sup> Des députés UMP demandent une protection internationale de la vie privée : <http://www.numerama.com/magazine/17025-des-deputes-ump-demandent-une-protection-internationale-de-la-vie-privee.html>

**Eric Schmidt**, encore lui, déclarait en 2009 : « si vous faites des choses en souhaitant que personne ne le sache, alors vous devriez peut-être vous en dispenser ». Ce refus des grands collecteurs de données d'assumer une responsabilité sociale qui irait à l'encontre de leur modèle d'affaire est probablement le frein le plus important à un droit à l'oubli, inapplicable sans leur concours<sup>43</sup>.

Mais la société a besoin de mémoire autant que d'oubli, et le « devoir de mémoire » s'oppose au « droit à l'oubli ». Dans ce contexte, l'exercice d'un droit à l'oubli pourrait s'apparenter à de la censure.

On le voit, le problème n'est pas simple, et il y a fort à parier qu'il ne trouvera pas de solution d'ici longtemps. Inutile et dangereux donc d'y compter pour se refaire plus tard une virginité.

Reste la dernière proposition loufoque du même Eric Schmidt, qui dans une interview au *Wall Street Journal*<sup>44</sup>, explique que la société évolue et s'adapte aux nouvelles technologies. Il ne s'agit donc plus, selon lui, de contrôler les éventuels dérapages du Web, mais de s'en accommoder, au point de permettre à une majorité d'individus de changer de nom pour ne pas avoir à affronter leur passé numérique. Quand on connaît la puissance des outils informatiques dont dispose *Google*, lui permettant de faire tous les recoupements possibles et imaginables, cette nouvelle identité serait en un rien de temps reliée à l'ancienne.



Eric Schmidt a rejoint Google en 2001. Sous sa direction, Google a considérablement développé son infrastructure et élargi ses offres. Avec les fondateurs Sergey Brin et Larry Page, Eric Schmidt est responsable de la stratégie technique et commerciale de Google. Il est également président de la New America Foundation.

## 8. Conclusion

L'identité sur Internet est composée d'éléments disparates et souvent insoupçonnés, dont la méconnaissance peut avoir des conséquences inattendues. L'ignorance ou l'imprudence peuvent se payer cher, mais tout compte fait, la connaissance nécessaire pour garantir un niveau de sécurité acceptable n'est ni compliquée, ni étendue. Il s'agit avant tout d'attitudes à développer, dont les plus importantes sont sans doute le regard sur soi : qu'est-ce que je montre, en quoi je me découvre, est-ce acceptable dans ce contexte ? Et l'esprit critique : puis-je me fier à ce site, à cette personne, à ces informations, à ces règles d'usage ?

Le droit à l'oubli n'existant pas, il serait vain d'espérer pouvoir un jour effacer toute trace devenue difficile à assumer, sans parler des innombrables traces abandonnées au fil des navigations sur le web dont nous n'avons même pas conscience. Il vaut mieux s'astreindre aux bonnes pratiques, et minimiser au maximum l'impact que nos fantaisies d'aujourd'hui pourraient avoir demain. Si vous pensiez que « naviguer masqué » vous mettait à l'abri de toute surprise, vous savez maintenant que le masque est presque transparent.

**Si vous pensiez que «naviguer masqué» vous mettait à l'abri de toute surprise, vous savez maintenant que le masque est presque transparent.**

Mais la réputation sur Internet est faite aussi de ce que d'autres disent sur nous, des photos qu'ils publient à notre insu et qui nous montrent dans des postures ou situations que nous pensions strictement privées. Il faut donc adopter une attitude proactive et vérifier régulièrement tous les éléments susceptibles de ternir notre image.

Ajoutées aux autres précautions indispensables sur le Net (par exemple ne jamais payer avec une carte de crédit sur un site dont l'adresse **ne commence pas** par **https://...** ou dont l'adresse, quand vous survolez le lien censé vous y conduire, est différente dans la barre d'état du navigateur que celle inscrite dans le lien) ces quelques mesures ne vous garantiront pas une sécurité absolue, mais permettront une navigation raisonnablement sûre et une bonne protection de votre identité sur Internet.

<sup>43</sup> Facebook's critics 'unrealistic', says US privacy law expert : [http://www.theregister.co.uk/2010/06/18/facebook\\_hoofnagle\\_podcast/](http://www.theregister.co.uk/2010/06/18/facebook_hoofnagle_podcast/)

<sup>44</sup> Google and the Search for the Future : <http://online.wsj.com/article/SB10001424052748704901104575423294099527212.html#articleTabs%3Darticle>

L'identité n'est pas seulement à protéger ; elle se construit pour une part de plus en plus importante sur Internet. Ne pas exister sur le web équivaut à une forme d'inexistence dans la « vraie vie ». Et cette tendance semble appelée à s'intensifier. L'enjeu principal de l'identité numérique est certainement celui-ci. Et pour le maîtriser, il faut être à l'aise sur les réseaux, s'y promener avec sécurité, faire preuve de créativité dans la manière de se présenter et d'entrer en relation avec les autres occupant de cet espace.

L'école est appelée à jouer un rôle essentiel dans la formation des utilisateurs de plus en plus jeunes et autonomes (devant l'ordinateur) de cet univers lui aussi en expansion. Plus ils sont jeunes, plus ils se montrent naïfs et ont du web une vision avant tout ludique. Les conséquences éventuelles de comportements inappropriés sont pour eux trop lointaines pour qu'ils les envisagent dans leur pratique des réseaux. Si avec l'âge ils deviennent plus prudents, ils seront d'autant mieux protégés que l'école les aura préparés tôt – et mieux – à affronter ce monde pas si différent de la réalité et très propice aux apprentissages et expériences.

## 9. Dix points à retenir

- **Dans quel but vais-je sur Internet : professionnel, socialisation, jeu, communauté d'intérêts, achats ? A chaque objectif, sa stratégie.**
- **S'interroger sur ce que je peux montrer et/ou dire ?**
- **Mon identité numérique est non seulement composée de mon nom et prénom, ou pseudo, mais elle se construit également avec ce que je montre, dis ou fais (notamment les sites que je visite).**
- **Il est préférable de scinder l'identité numérique en quatre entités distinctes : professionnelle, amicale, familiale, personnelle.**
- **Prendre conscience que tout ce qui sera publié pourra être utilisé à mon insu, voire contre moi.**
- **Toutes les demandes de services et notamment les paiements par internet peuvent constituer une base de donnée commerciale sur mes goûts et mes achats.**
- **Il est très difficile d'effacer des traces «encombrantes» de mon passage sur Internet.**
- **La politique de confidentialité d'un site de réseaux sociaux peut rapidement varier.**
- **Il importe de connaître la spécificité de chaque site sur lequel je suis actif : blog, forum, réseau social de type *Facebook*.**
- **Les employeurs consultent de plus en plus souvent Internet pour chercher des traces laissées par les candidats à des postes de travail.**