

Identité numérique : être ou ne pas être sur le Web ?

Par Andrée Beaudin-Lecours, chargée de projet
La Vitrine Technologie-Éducation



Depuis l'avènement de ce qu'il est convenu d'appeler l'« École 2.0 » (*School 2.0*), dans la foulée du Web 2.0, les acteurs du milieu éducatif utilisent Internet plus que jamais. Sur cette Toile qui se veut « centrée sur l'utilisateur » (*user centric*), enseignants et étudiants tendent à devenir maîtres du jeu. Ils se transforment en véritables producteurs de contenu, que ce soit par leurs interventions sur un blogue, leurs collaborations à un wiki, la diffusion de leurs vidéos, leurs photos, etc. Avec leurs contributions variées, leurs traces laissées sur le Web, se dessinent peu à peu leur identité numérique, leur marque personnelle, puis leur cyberréputation.

Cependant, ils ne sont pas véritablement maîtres de leur identité, car d'autres gèrent à leur place leurs renseignements personnels, les informations qui les concernent. S'ajoute la confusion autour de l'identité des auteurs – pensons aux vols d'identité, par exemple. Qui n'a pas entendu parler d'un étudiant qui prend la parole au nom d'un autre étudiant, d'un enseignant, voire du directeur d'un établissement d'enseignement, par exemple ? Dans cet article, nous faisons la lumière sur ce qui constitue l'identité numérique et sur les mécanismes d'identification et d'authentification. Nous présentons également quelques pistes d'action pour vous permettre de demeurer maître de votre identité tout en profitant pleinement du Web : évaluer votre image de marque, mousser votre cyberréputation, présenter votre portfolio numérique, etc.

Identité ou identités numériques ?

L'identité est ce qui caractérise un groupe ou un individu, le distingue, lui confère son individualité, ce que certains nommeraient le « soi »

ou le « moi » (*self*). L'identité est également un terme de jurisprudence. Elle permet à chacun d'entre nous d'être légalement reconnu, sans confusion aucune ; elle constitue notre personnalité civile, tout comme elle est l'ensemble des éléments qui rendent possible cette reconnaissance de notre spécificité.

Le terme « identité » est polysémique, sans compter qu'une identité se décline en plusieurs couleurs et nuances, qu'elle s'exprime sur le Web ou non, qu'elle soit numérique ou non. Employée au singulier, l'expression « identité numérique » renvoie à ce qui constitue votre « être » sur la Toile ; au pluriel, les « identités numériques » renvoient plus précisément aux données permettant de vous identifier – vos noms d'utilisateurs, par exemple.

Laisser ses traces numériques

Francis Pisani, journaliste indépendant intéressé par les nouvelles technologies de l'information et de la communication, résumait ainsi la puissance d'Internet, lors d'un entretien publié dans *Le Monde* : « Nous disposons d'un moyen de communication formidable, mais tout ce que nous faisons sur le Web laisse des traces² ». Votre identité numérique est constituée de vos contributions sur Internet, des traces numériques que vous laissez au passage, quelles qu'elles soient. Ce sont également les traces que d'autres laissent à votre sujet. Toutes ces traces concourent à bâtir votre identité numérique et peuvent servir à dresser votre portrait.

Les données qui vous identifient

Chacune des contributions qui se trouvent sur le Web est généralement accompagnée d'une signature qui permet d'en déterminer l'auteur. Ce dernier peut délibérément signer de ses

noms et prénoms légaux, ou opter pour un pseudonyme. Aussi, il peut jumeler à sa signature une représentation visuelle, un avatar³, qui sera réaliste ou non, animé ou non, en deux ou en trois dimensions. Il crée en quelque sorte sa propre carte d'identité.

Sans signature, votre passage sur le Web laisse tout de même des traces, un indice. Votre fournisseur de services Internet, qui est parfois votre employeur, peut retracer vos activités sur le Web grâce à l'adresse IP de votre ordinateur de maison ou de celui du bureau. L'adresse IP est un « numéro constitué de quatre nombres entiers séparés par des points, qui identifie de façon unique un ordinateur connecté au réseau Internet et en permet la localisation⁴ ».

Bien que vous puissiez souhaiter garder l'anonymat, il n'est peut-être pas possible de le conserver sur le Web, à moins d'utiliser l'identité d'un autre, ce que les usurpateurs ont bien compris (usurpateurs d'identités numériques, usurpateurs d'adresses IP).

Pseudonymes et désir d'anonymat

Pratique répandue dans les milieux littéraires aux siècles derniers, au nom de la libre expression, l'usage de noms de plume s'est amplifié avec l'avènement d'Internet, faisant de la Toile un réseau d'internautes anonymes, en appa-

1 Découvrez l'école de demain, sous forme de carte interactive (en anglais) : <http://etoolkit.org/etoolkit/map>

2 Article disponible à cette adresse : <http://www.lemonde.fr/web/chat/0,46-0@2-651865,55-1047893,0.html?xtor=RSS-3208>

3 À titre d'exemple, vous pouvez vous créer un avatar, dans ce cas un « voki », à partir de cette adresse : <http://www.voki.com/>

4 Adresse IP [Le grand dictionnaire terminologique, Office de la langue française, 2001] <http://www.oqlf.gouv.qc.ca/ressources/gdt.html>

rence. Malheureusement, ce masque sert parfois les cyberintimidateurs, comme si, sur Internet, tout pouvait se dire sans censure sous le couvert d'un pseudonyme. Bien que l'usage de noms d'emprunt soit souvent associé à des activités illicites dans le quotidien – pensons aux « pseudos » des prostitués et des caïds –, il apparaît légitime dans ce vaste espace public qu'est Internet, ne serait-ce que par précaution.

François Guité propose plusieurs réflexions sur ce sujet dans son blogue *Relief* consacré à l'éducation. Le billet intitulé « Identité et vie privée⁵ » soulève une question pertinente : « Les étudiants doivent-ils utiliser un pseudonyme ou leurs véritables noms et prénoms sur le Web, que ce soit sur des blogues ou autres espaces d'expression ? » Dans un autre article, il s'inquiète de « l'innocence des jeunes sur le Web » qui affichent sans pudeur leur vie privée :

« Maintenant que les jeunes se sont emparés des blogues avec une candeur déconcertante, les risques qu'ils encourent sont beaucoup plus grands qu'ils ne le réalisent. [...] Le danger est d'autant plus grand pour les plus jeunes, eux qui affichent innocemment noms, adresse, photos et autres informations personnelles. En plus de l'évidente question de sécurité, les jeunes doivent prendre conscience des risques que toute cette information peut représenter pour leur avenir. Plusieurs informations, une fois lâchées dans le cyberspace, sont irrécupérables et viennent nous hanter plus tard⁶. »

Se dévoiler, désir d'authenticité ?

Les réseaux sociaux sur Internet amènent les participants à se dévoiler, et même, dans les réseaux de rencontre où les pseudonymes sont présentés comme un gage d'anonymat, vient un moment crucial où les correspondants doivent un tant soit peu dévoiler leur véritable identité, ne serait-ce que pour se fixer un rendez-vous. Dans le cas de Facebook, service se décrivant comme « un réseau social qui vous relie à ceux qui comptent pour vous⁷ », les participants s'y présentent en toute transparence et n'hésitent pas à dévoiler à leurs « amis » des renseignements personnels⁸, dont quelques-uns sont accessibles à tous les internautes par une

fonction de recherche que seule la configuration de ses paramètres de confidentialité permet de contrer⁹.

Bien que l'on puisse se demander si les réseaux sociaux menacent la vie privée, connaître la personne à qui l'on s'adresse est un besoin légitime sur le Web comme ailleurs. Ce besoin exprime aussi un désir d'authenticité dans les relations entretenues sur le réseau Internet. Sur le blogue « Les identités numériques, enjeux et pratiques d'une construction identitaire sur

nisme ne permet pas de déterminer la véritable identité de la personne qui utilise ces clés. À noter que les failles de sécurité viennent souvent du comportement des utilisateurs, en dehors des considérations informatiques.

Open ID et authentification unique

Comme chaque site offre ses clés d'accès, il est facile d'en échapper quelques-unes hors de votre trousseau, sans même que vous vous en rendez compte. Comme solution de rechange à une gestion complexe de vos noms d'utilisa-

« Bien que l'on puisse se demander si les réseaux sociaux menacent la vie privée, connaître la personne à qui l'on s'adresse est un besoin légitime sur le Web comme ailleurs. »

Internet¹⁰ », de Julien Pierre, enseignant en communication à Grenoble, une caricature de Peter Steiner¹¹ illustre bien les limites d'un réseau d'internautes anonymes : « Sur Internet, personne ne sait que t'es un chien ». En plus de vouloir connaître ses interlocuteurs, fraudes et vols d'identité incitent à transformer Internet en un réseau d'internautes identifiables.

Vers un réseau d'internautes identifiables

Actuellement, la cryptographie asymétrique est la méthode privilégiée permettant l'identification, donc l'accès à un site Internet sécurisé. Elle fonctionne à partir de deux clés : une clé publique (l'identifiant) et une clé privée (l'authentifiant). L'identifiant est un nom, un code d'utilisateur que vous créez ou qui vous est octroyé par le fournisseur du service que vous souhaitez utiliser. L'identifiant seul ne permet pas l'authentification. L'accès à un site Internet sécurisé est possible lorsque l'identifiant est jumelé à un authentifiant, c'est-à-dire à un « code secret », un mot de passe qui doit demeurer personnel, confidentiel. Il suffit de posséder les deux clés pour ouvrir le compte, comme pour un coffre-fort. Toutefois, le méca-

teurs et mots de passe, se présente l'OpenID¹², système qui permet l'« authentification unique » ou la fédération des identités. Il se base sur une technologie non propriétaire et vise précisément à réduire le nombre de « d'identités » : un seul couple identifiant-authentifiant géré par son propriétaire, ou une seule paire de clés pour accéder à différents sites Internet sécurisés. Bien que l'OpenID utilise la cryptographie asymétrique avec les limites exposées précédemment, l'authentification unique facilite la gestion de

5 Article disponible à cette adresse : <http://www.oopossum.ca/guitef/archives/002027.html> (François Guité, Blogue Relief, 7 mai 2005)

6 Article disponible à cette adresse : <http://www.oopossum.ca/guitef/archives/002658.html> (François Guité, Blogue Relief, 21 janvier 2006)

7 Voir <http://fr-fr.facebook.com/> (consulté en août 2008).

8 Découvrez la définition de « renseignement personnel » sur ce site du Commissariat à la protection de la vie privée du Canada : <http://youthprivacy.ca/fr/liife.html>

9 À ce sujet, lire l'article « Facebook prend le risque d'exposer la vie privée de ses utilisateurs » (Philippe Astor, 7 septembre 2007), disponible à cette adresse : <http://www.zdnet.fr/actualites/internet/0,39020774,39372774,00.htm>

10 Voir la caricature sur la page d'accueil, à droite : <http://www.identites-numeriques.net/>

11 D'autres caricatures de Peter Steiner se trouvent à cette adresse (en cliquant sur son nom) : http://www.thenewyorkerstore.com/product_details.asp?sid=22230

12 Qu'est-ce que l'OpenID ? : <http://openid.net/what/>

vos mots de passe, dont la modification fréquente est l'un des gages de sécurité sur Internet.

Pour créer son compte OpenID, il suffit de s'inscrire sans frais auprès d'un fournisseur « de confiance » et de lire, comme toujours, les contrats. L'utilisateur se voit attribuer une adresse URL (un URI) et peut, de là, créer sa propre carte d'identité, avec photo ou non. Il peut y afficher les renseignements personnels qui lui conviennent. Certains fournisseurs, comme ClaimID, offrent des fonctionnalités qui transforment la carte en un véritable portfolio numérique par l'intermédiaire duquel s'exprime l'identité de l'auteur. De plus, un fournisseur comme myOpenID indique au propriétaire de la carte chacune des « transactions » faites, ce qui permet de retracer les intrus, comme sur votre compte de téléphone ou de carte de crédit.

En somme, l'OpenID permet la portabilité des données, soit « la possibilité de gérer soi-même ses données personnelles¹³ ». De plus en plus d'acteurs sur Internet s'allient à l'OpenID et tendent vers la fédération des identités. Cela signifie que vous pourrez ultimement utiliser votre carte unique, personnalisée, pour accéder à leurs différentes sphères d'activités. Il existe d'ailleurs des répertoires¹⁴ de sites qui supportent l'OpenID, comme Oxfam International¹⁵. Des projets de fédération des identités prennent également naissance en milieu scolaire, comme celui du Comité Réseau des Universités (France), pour lequel « l'objectif de la fédération d'identités est de faciliter le partage de ressources numériques en ligne entre établissements d'enseignement supérieur en interconnectant leurs services d'authentification¹⁶ ».

Biométrie et carte d'identité numérique

Parallèlement à l'OpenID se développent les projets de cartes d'identité numérique reconnues légalement. Jusqu'ici, ce type de cartes n'a pas été adopté, mais il semble en voie de l'être. Par exemple, le ministère de l'Intérieur, de la Sécurité intérieure et des Libertés sociales de la République française propose le programme INES (pour Identité Nationale Électronique Sécurisée), visant, entre autres, à « offrir

aux citoyens les moyens de prouver leur identité sur Internet et de signer électroniquement, afin de favoriser le développement de l'administration électronique¹⁷ ». Cette carte est basée sur la biométrie, une technologie d'authentification dite « forte ». Aux données qui permettent habituellement de vous identifier – noms de famille, prénoms et autres renseignements personnels figurant ou non dans un registre de l'état civil (date et lieu de sa naissance, adresse, état matrimonial, etc.) – s'ajoutent les caractéristiques biologiques et comportementales.

Il peut s'agir de votre empreinte digitale, de la configuration de votre iris, de votre dynamique de frappe au clavier ou de votre dynamique de signature.

Les technologies d'authentification forte visent à connaître la véritable identité des interlocuteurs. Ainsi, sous prétexte de contrer la cybercriminalité, la biométrie, fille de l'anthropométrie, connaît actuellement un immense engouement et déchaîne tout autant la critique. Elle soulève plusieurs questions éthiques qui méritent d'être débattues sur la place publique, et aussi en classe de philosophie et d'anthropologie. Pour chacune des données retenues et analysées, il convient de se demander : sont-elles si précises ? Sont-elles infalsifiables ? Permettent-elles une identification irréfutable ? Qui les possède ? Quel usage en fait-on ou compte-t-on en faire¹⁸ ? Devra-t-on obligatoirement présenter une carte d'identité numérique nationale pour utiliser les différents services disponibles sur Internet ? Daniel Kaplan, d'InternetActu.net, s'interroge : « Carte d'identité numérique : quels usages au-delà des transactions officielles ?¹⁹ ». Quels usages pourra-t-on en faire en éducation ? La biométrie

n'est pas invulnérable²⁰. De plus, ces questions laissent place à l'imagination et évoquent les meilleures séquences de science-fiction : puis-je emprunter votre œil ?

Contrôler votre identité numérique

Autour de vos noms et prénoms véritables, noms d'utilisateurs, pseudonymes et autres « identités » se dessine le schéma²¹ de vos activités sur Internet. Aux réseaux sociaux s'ajoute la cartographie de vos relations

« Ainsi, sous prétexte de contrer la cybercriminalité, la biométrie, fille de l'anthropométrie, connaît actuellement un immense engouement et déchaîne tout autant la critique. »

sociales. Ces amalgames divers forment votre image, votre « identité numérique », votre « être numérique ». Sur Internet, votre réputation se bâtit en fonction du regard porté sur vous, sur l'un ou l'autre de vos profils, voire sur l'ensemble, sans compter ce qui est dit sur vous ou en votre nom. Homonymes et usurpateurs d'identités peuvent vous côtoyer. Le billet « Maîtrisons-nous notre identité numérique ? », signé d'un pseudonyme et publié sur le blogue OpenID, résume bien la question :

13 Définition accessible à cette adresse :

<http://fr.wikipedia.org/wiki/DataPortability>

Pour en savoir plus sur la portabilité des données

(*dataportability*) : <http://www.openid-leblog.fr/> ;

<http://microformats.org/wiki/data-portability-fr>

14 Où utiliser votre OpenID ? <http://openid.net/where/> ;

<http://openiddirectory.com/>

15 Compte d'utilisateur, Oxfam International :

<http://www.oxfam.org/fr/user>

16 Comité Réseau des Universités, Fédération d'identités :

<https://federation.cru.fr/>

17 Description du programme disponible à cette adresse :

<http://www.foruminternet.org/telechargement/forum/pres-prog-ines-20050301.pdf>

18 L'histoire récente nous montre les limites des systèmes

d'identification basés sur des caractéristiques physiques.

19 Article disponible à cette adresse :

<http://www.internetactu.net/2005/03/09/carte-didentit-numrique-quels-usages-au-del-des-transactions-officelles/>

20 Pour en savoir plus sur la biométrie :

<http://www.securiteinfo.com/conseils/biometrie.shtml>

21 Voir Touchgraph à cette adresse :

<http://www.touchgraph.com/TGGoogleBrowser.html>

« Aujourd'hui, sur le Web, il est très difficile de savoir qui fait quoi, c'est entre autres pour cela que de nombreux sites nous demandent de saisir nos identifiants et mots de passe. Au-delà de cet aspect technique, l'identité numérique fait référence à des personnes. La question de l'image se pose alors. Désormais, nous avons tous une présence sur la Toile, et celle-ci va conditionner notre image, mais aussi notre réputation²². »

Évaluer votre image de marque

Quelles que soient vos activités sur le Web, vous pouvez évaluer votre image, votre marque personnelle en effectuant d'abord une simple recherche sur vous. Vous serez peut-être surpris des résultats. Vous découvrirez peut-être vos homonymes, voire un usurpateur d'identité.

Voici une procédure simple :

1. Établir la liste des éléments qui permettent de vous identifier sur le Web, entre autres :
 - Noms et prénoms légaux et leurs variantes, avec ou sans abréviations ;
 - Noms d'utilisateurs, pseudonymes et leurs variantes, avec ou sans abréviations ;
 - Vos adresses électroniques et adresses URL.
2. Pour chacun de ces éléments, à l'aide de différents outils de recherche, trouvez sur le Web ce qui vous concerne. Il est à noter que chaque moteur de recherche ne couvre qu'une partie du spectre de tout ce qui se fait sur le Web. En d'autres mots, ne vous limitez pas à Google ! Aussi, les astuces de recherche habituelle peuvent vous aider, comme :
 - Utiliser les guillemets dans votre requête pour l'expression exacte.
3. Pour chacun de ces éléments, évaluer les résultats et l'image globale qui est véhiculée.
4. Pour être au fait de ce qui est publié sur le Web en votre nom, qu'il soit d'emprunt ou non, vous pouvez automatiser votre veille personnelle en créant des alertes Google,

par exemple. Il existe également d'autres outils, comme Bloglines, ou la Watchlist offerte par Technocrati²³.

5. Gardez en note les informations que vous fournissez aux distributeurs de services sur Internet, ainsi que les contrats que vous signez avec eux.
6. Surveiller les actualités qui concernent Google et pourquoi pas, tous vos fournisseurs de services Internet ! Le bulletin électronique

simplement vous démarquer dans l'espoir de mieux naviguer au sein de l'actuel marché du travail ?

Les sites sur la *personal branding* abondent, provenant du milieu du marketing plutôt que de celui de l'éducation. À titre d'exemple, nous avons retenu le site « Envie d'entreprendre », conçu pour « le partage d'expériences et de connaissances concernant le monde de l'entreprise²⁷ ». L'article intitulé « Comment créer et

« Sans espérer devenir une star du Web, peut-être voulez-vous simplement vous démarquer dans l'espoir de mieux naviguer au sein de l'actuel marché du travail ? »

*Branchez-vous*²⁴ et le bulletin de La Vitrine Technologie-Éducation²⁵ peuvent vous soutenir dans cette tâche.

Il est suggéré d'effectuer des veilles distinctes pour votre sphère personnelle et votre sphère professionnelle, si vous souhaitez éviter les recoupements. Peut-être voudrez-vous supprimer certains passages qui vous concernent ? Rien ne garantit que cette démarche sera simple, raison pour laquelle des firmes se spécialisent dans cette voie, un marché émergent dans cet écosystème de l'identité numérique. Peut-être souhaitez-vous disparaître complètement du Web ? Il est à noter que, pour le moment, le suicide numérique n'existe pas, comme le soulignait Serge Ravet, président d'EIFEL (European Institute for E-Learning), lors de la conférence *ePortfolio et identité numérique*²⁶, à Montréal, en mai 2008.

Mousser votre cyberréputation

À l'instar d'artistes reconnus qui contribuent à faire de leur nom une véritable marque de commerce, une œuvre d'art, chaque internaute soucieux de sa réputation souhaite la préserver et peut-être la mousser un peu. Sans espérer devenir une star du Web, peut-être voulez-vous

gérer votre "marque personnelle" sur Internet ? (*personal branding* numérique) » présente des trucs et astuces pour entretenir votre image de marque, dont la nécessité de demeurer authentique. L'auteur Olivier Zara invite d'ailleurs les internautes à demeurer maîtres de leur identité numérique, rappelant ceci :

« Avec Internet, il n'y a plus d'inconnus. Inutile de débrancher votre ordinateur, inutile de résilier votre abonnement à Internet, il suffit que votre voisin, votre collègue ou un ami publie des informations ou son opinion sur vous et vous ne serez plus un inconnu. Internet est une place publique mondiale sur laquelle va se construire votre image de marque. [...] On ne choisit pas d'avoir une marque personnelle. Tout le monde en a une : positive, neutre ou négative. Grâce ou à

22 Disponible à cette adresse : <http://www.openid-leblog.fr/dotclear/index.php?2008/03/22/29-maitrisons-nous-notre-identite-numerique>

23 Ces deux derniers outils n'ont pas été testés par l'auteur.

24 Pour vous abonner : <http://www.branchez-vous.com/>

25 Pour vous abonner : <http://ntic.org/>

26 Site Web de l'événement : http://events.eifel.org/eportfolio_montreal

27 Accessible à partir de cette adresse : <http://www.enviedentreprendre.com/>

cause d'Internet selon le point de vue, elle deviendra tôt ou tard publique et accessible mondialement. Si vous ne définissez pas votre marque personnelle, ce sont les autres qui la définiront pour vous et il y a des risques qu'elle ne vous corresponde pas²⁸. »

Hington Klarsey est un autre de ces spécialistes offrant « conseil en protection de la réputation et de la e-réputation des marques et des notoriétés ». Il propose un site consacré à la « Web-réputation²⁹ » et surtout, des services : noyer une rumeur, contrer une campagne de dénigrement, modifier ses données personnelles, supprimer un message, gérer sa réputation, etc.

Présenter votre portfolio numérique

Sans avoir recours à ces spécialistes de l'image, vous pouvez créer votre portfolio numérique, défini comme un « dossier évolutif qui rassemble des documents numériques décrivant et illustrant le parcours, l'expérience et les compétences de la personne qui l'a constitué, et qui peut être utilisé à des fins d'apprentissage, d'évaluation ou de présentation³⁰ ». La possibilité de trouver et de gérer à partir d'un même endroit l'ensemble de ses traces laissées sur le Web correspond au nouveau modèle de portfolio numérique. À la limite, nous pourrions dire que la nouvelle génération de portfolios numériques est en fait une nouvelle génération d'applications permettant de retracer les contributions faites sous une signature donnée et d'en faire état dans un lieu commun qu'est une page Web. ClaimID³¹, l'exemple mentionné précédemment, permet de générer un portfolio numérique qui présente vos publications sur le Web.

Pour être véritablement maître de votre identité numérique, il est aussi possible de réserver votre nom de domaine (.com, .org, .net, etc.) à votre nom usuel ou d'emprunt et d'en faire votre carte d'identité, voire votre portfolio. Vous pouvez alors vous servir de votre adresse URL comme nom d'utilisateur lors de l'inscription à différents services. Contrairement à l'OpenID, cette façon de procéder n'est pas gratuite, puisque vous devez payer une contribution

annuelle pour vos noms de domaine, mais l'URL vous appartient. À cette adresse URL, sur une page Web, vous pouvez également répertorier vos différentes contributions. Ce processus n'est pas automatisé, mais permet d'authentifier vos productions. En fait, vous reconnaissez comme vôtre ce qui est à cette adresse (et ce qui est signé avec cette adresse).

être fait des informations que vous donnez ? Que spécifiait le contrat de confidentialité concernant vos renseignements personnels ? L'avez-vous lu ?

À y regarder de plus près, contrôler son identité n'est pas une tâche simple. Plus vous utilisez Internet, plus la tâche se complexifie. Limiter le nombre de ses signatures, mots de passe,

« Pour être véritablement maître de votre identité numérique, il est aussi possible de réserver votre nom de domaine (.com, .org, .net, etc.) à votre nom usuel ou d'emprunt et d'en faire votre carte d'identité, voire votre portfolio. »

Il est possible aussi de créer des portfolios hybrides, c'est-à-dire dont une partie est gérée manuellement par son propriétaire, et l'autre par des mécanismes automatiques. L'étudiant qui opte pour ce portfolio numérique peut démontrer par ricochet sa connaissance des outils du Web 2.0. Rappelons toutefois que les informations publiées sur Internet peuvent avoir une vie bien au-delà de votre page Web, même si vous en supprimez les contenus.

En conclusion : être ou ne pas être sur le Web ?

Contrôler votre identité numérique implique de choisir sous quelles signatures vous présenter, sans oublier la gestion des mots de passe. Cela signifie aussi contrôler votre image en sélectionnant les contributions associées à vos signatures tout en soignant vos relations, votre réseau social, votre cyberréputation. Contrôler votre identité, c'est également vous assurer que vous êtes la seule personne à parler en votre nom, en sachant en contrepartie qu'il n'est pas aisé de contrôler ce que l'on dit sur vous. Aussi, contrôler votre identité, c'est être au fait des informations détenues sur vous ! Quelles informations avez-vous données aux fournisseurs de services sur Internet ? Qu'est-ce qui peut

adresses de courriel et URL peut faciliter la tâche – ce qu'offre l'OpenID – tout comme la présentation d'une carte d'identité extensive : le portfolio numérique. L'identité numérique commande de nouvelles compétences, notamment la gestion de ses renseignements personnels. Elle commande peut-être aussi un « virage dans l'éducation aux TIC », pour reprendre le titre d'un billet de François Guité, auteur du blogue *Relief*, qui souligne : « Il ne s'agit plus seulement d'enseigner aux jeunes l'utilisation technique de l'ordinateur et de ses applications, mais également les coulisses du monde virtuel³². »

Alors, être ou ne pas être sur le Web ? ■

28 Article disponible à cette adresse : <http://reputation.axiopole.info/2008/01/10/creer-votre-marque-personnelle-personal-branding/>

29 Voir les sites : <http://www.hingtonklarsey.com/> et <http://www.web-reputation.com/>

30 Portfolio numérique [Le grand dictionnaire terminologique, Office de la langue française, 2008] <http://www.oqlf.gouv.qc.ca/ressources/gdt.html>

Voici deux exemples de portfolios numériques de personnes spécialisées dans le domaine : http://samanthaslade.ca/wiki/index.php?title=Main_Page et <http://electronicportfolios.org/> (Helen Barrett)

31 Voir le portfolio numérique de Marga Perez, à ces adresses : <http://www.margaperez.com/>; <http://claimid.com/margaperez>.

Notez que Marga Perez spécifie ce qui n'est pas d'elle, mais de ses homonymes.

32 <http://www.oppsum.ca/guitef/archives/002849.html>