Rakmana
Revue d'études en sciences de l'information et de la communication

Volume 02 | Numéro 03
Mois et Année
Pages 192 - 205

ISSN-2773-4285
EISSN | 2830-8417
Dépôt légal | 07/2021
Adresse | 11, Route Dodo Mokhtar, Ben Aknoun, Alger
Fax | (023) 23 88 50
Téléphone | (0561) 62 29 75

Reçu le 07/11/2022
Accepté le 17/12/2022
Publié le 31/12/2022

SAOUDI Asmaa
l'Académie Militaire de Cherchell du défunt Président Houari Boumediene (Algérie),
asma-saoudi@hotmail.fr

La gestion de l'identité numérique: Dimension et enjeux

إدارة الهوية الرقمية: البعد والتحديات

SAOUDI Asmaa
l'Académie Militaire de Cherchell du défunt Président Houari Boumediene (Algérie)
asma-saoudi@hotmail.f

Résumé

L'objet de cet article est d'analyser la question relative à la gestion d'une identité numérique qui demeure difficile à cerner. en effet, gérer son image virtuelle est devenue une nécessité aussi bien pour les particuliers que pour les entreprises.

Afin de porter des éléments de réponses aux questions suivantes: Comment construire une identité numérique? Et pourquoi est-ce devenu un enjeu premier aujourd'hui, notamment en ce qui concerne la protection des données personnelles ? Cet article propose un éclairage sur le concept même de la gestion d'une identité numérique et comment se créer une identité numérique? Et les différents types de cette dernière, pour pouvoir ensuite souligner les risques & les enjeux d'une identité virtuelle, qui demeure une question centrale dans l'écosystème internet.

Mots-clés: identité numérique , gestion, protection, renseignements personnels, E-réputation.

الملخص:

الغرض من هذه الورقة البحثية هو تحليل مسألة إدارة الهوية الرقمية التي لا يزال من الصعب تحديدها. خاصةً و أن إدارة الصورة الافتراضية أمر لا مفر منه لكل من الأفراد أو المؤسسات. بغية الوقوف على ماهية الهوية الرقمية يسعى هذا البحث للإجابة على الأسئلة التالية: كيف يمكن بناء هوية رقمية ؟ ولماذا أصبحت قضية رئيسية اليوم، خاصة فيما يتعلق بحماية البيانات الشخصية؟

تقدم هذه المقالة نظرة ثاقبة على مفهوم إدارة الهوية الرقمية وكيفية إنشاء هوية رقمية ؟ والأنواع المختلفة من الهوية الرقمية، كما تسلط هذه الورقة البحثية الضوء على مخاطر وتحديات الهوية الافتراضية، والتي تظل مشكلة مركزية في عالم للإنترنت.

الكلمات المفتاحية: الهوية الرقمية، إدارة الهوية الرقمية، الخصوصية، السمعة الرقمية.

1. Introduction

Avec la prolifération des outils numériques, les utilisateurs fournissent de grandes quantités de données personnelles, intentionnellement ou non, comme par exemple acheter des produits sur sites marchands, utiliser des outils de géo localisation, échanger des emails , remplir des formulaires sur des sites internet, remplir des comptes sur les réseaux sociaux ou autre entraînent nécessairement la collecte de données. Toutes les actions effectuées sur internet sont matérialisées par des traces sur lesquelles l'utilisateur a plus ou moins de contrôle. L'ensemble de ces informations permet de définir un profil personnel et constitue une « identité numérique ».

Les avis des clients sur les produits d'une entreprise par exemple peuvent entraîner une perte de ventes. Internet est alors conçu pour stocker une empreinte numérique de chaque utilisateur. Ces journaux reflètent les activités en ligne d'individus ou d'entités. Par conséquent, nos identités numériques sont complexes et difficiles à utiliser.

Dans le cadre de cet article, nous voulons mettre en relief le recours à l'identité numérique qui est actuellement inévitable. Soucieux de l'image et de la réputation, les internautes font fréquemment recours à la diffusion de publications sur la toile. Cela permet de transférer rapidement les informations et d'avoir une meilleure visibilité en ligne.

L'objet de cet article est d'analyser la question relative à la gestion d'une identité numérique qui demeure difficile à cerner. En effet, gérer son image virtuelle est devenue une nécessité pour une organisation quelque soit une entreprise une association ou une administration. les enjeux d'ordres économique et stratégique sont très importants et dépassent largement la problématique de la stratégie de communication.

Afin de porter des éléments de réponses aux questions suivantes: Comment construire une identité numérique? Et pourquoi est-ce devenu un enjeu premier aujourd'hui, notamment en ce qui concerne la protection des données personnelles ? cet article propose un éclairage sur le concept même de la gestion d'une identité numérique et comment se créer une identité numérique? Et les différents types d'identité numérique, pour pouvoir ensuite souligner les risques & les enjeux d'une identité virtuelle, qui demeure une question centrale dans l'écosystème internet, aussi bien pour les particuliers que pour les entreprises.

2. La gestion de l'identité numérique: c'est quoi ?

a. Définition de l'identité numérique:

Pour étudié le concept d'identité numérique les définitions sont nombreuses, complémentaires ou partiellement contradictoires (Merzeau 2013, Georges 2014 , Ertzscheid 2009…). C'est pourquoi on souhaite mieux comprendre cette notion en évoquant plusieurs définitions qui ont donné lieu à une vaste revue de littérature interdisciplinaire étudiant à la fois les modèles de l'identité numérique et les contextes d'usage.

D'abord, le terme d'identité vient de l'étymologie latine idem qui signifie, le même. Dans un premier sens, il s'agit du caractère identique de deux ou de plusieurs

éléments, notamment dans le champ des mathématiques. En tant que concept, l'identité correspond à ce qui rassemble plusieurs individus sous la même idée, soit l'identité nationale. De la même façon qu'elle permet de regrouper des éléments ou des êtres, l'identité est aussi ce qui permet de se distinguer des autres par le processus d'individualisation.

Ensuite, l'identité est aujourd'hui redéfinie au contact des technologies de l'information et de la communication (TIC). En effet, les internautes sont assimilés à une suite de traces numériques lorsqu'ils naviguent sur le web, ce qui constitue une nouvelle identité dite: identité numérique, composée à la fois de l'identité légale et de l'identité personnelle. Fred Cavazza est le premier à conceptualiser la notion d'identité numérique.

Ainsi, toutes ces informations regroupées, qu'elles soient disponibles ou non sur le web, constituent ce que l'on appelle l'« identité numérique ». Fanny Georges désigne cette identité par une « collection de traces […] enfouies, non intentionnelles et performatives » (Georges F, 2011 : p p 31-48).

L'identité numérique est constituée donc d'informations personnelles autrement dit qui vous êtes et comment vous vous présentez, ce que vous possédez, les personnes que vous connaissez, et ce que vous faites.

Selon Olivier Ertzscheid l'identité numérique est définit de la façon suivante : « la collection des traces (écrits, contenus audio ou vidéos, messages sur des forums, identifiants de connexion, etc.) que nous laissons derrière nous, consciemment ou inconsciemment, au fil de nos navigations sur le réseau et le reflet de cet ensemble de traces, tel qu'il apparaît "remixé" par les moteurs de recherche (Olivier Ertzscheid, 2013: p 15).

A noter que le concept d'identité numérique regroupe une polysémie de sens à cause de la pluralité des dénominations alternatives comme traces numériques, présence numérique, expression de soi, se dessine une multiplicité de points de vue et manières radicalement différentes de définir ce concept selon les disciplines engagées.

En ce qui concerne la notion d'identité numérique, il est davantage question du « caractère de ce qui, sous des dénominations ou des aspects divers, ne fait qu'un ou ne représente qu'une seule et même réalité » (Centre National de Ressources Textuelles et Lexicales, 2020). Ainsi, cette même réalité est régit par un même nouveau contexte, à savoir l'ère du numérique. En effet, cette identité numérique, est composée des éléments constituants nos identités « classiques », en y ajoutant d'autres facteurs, liés à l'utilisation d'internet. A travers les navigations sur le web, de nombreuses traces sont enregistrées et définissent une identité nouvelle.

L'identité numérique alors est une réalité quotidienne: c'est un identifiant plus un mot de passe et une adresse email, l'ensemble des informations que l'internaute aura communiquées le concernant. Le besoin, c'est de sécuriser cette identité numérique pour qu'elle ne soit pas, ou très difficilement fraudable, ce qui soulève la question sur comment protéger l'internaute contre le traçage de ses transactions et protéger les données et l'ensemble des informations qu'il communique.

En réalité, notre identité numérique comporte trois couches, c'est ce qu'on va expliquer dans les différents types d'identité numérique. Selon Katarzyna Szymielewicz cofondatrice de la Fondation polonaise Panoptykon (qui milite pour la protection de la liberté et des droits de l'homme à l'ère numérique) nous ne pouvons protéger qu'une seule d'entre elles. Voilà ce qu'elle explique, dans un article publié le 25 janvier 2019 dans Quartz:

> *" Ce serait bien de penser que nous avons le contrôle sur notre profil numérique. Nous décidons quelles photos nous voulons partager et lesquelles doivent rester privées. Nous acceptons ou rejetons les invitations, contrôlons les balises, et réfléchissons à deux fois avant de publier un message ou un commentaire. Nous sommes critiques et sélectifs quant au contenu que nous aimons ou partageons. Alors pourquoi n'aurions-nous pas le contrôle ?*
> *La mauvaise nouvelle, c'est que lorsqu'il s'agit de notre profil numérique, les données que nous choisissons de partager ne sont que la pointe de l'iceberg. Nous ne voyons pas le reste qui est caché sous l'eau des interfaces conviviales des applications mobiles et des services en ligne. Les données les plus précieuses nous concernant sont déduites hors de notre contrôle et sans notre consentement. Ce sont ces couches plus profondes que nous ne pouvons pas contrôler qui prennent vraiment les décisions, pas nous"*

L'identité numérique est donc l'ensemble des traces numériques qu'une personne ou une collectivité laisse sur internet. Toutes ces informations, laissées au fil des navigations, sont collectées par les moteurs de recherche, comme Google, et sont rendues public. Une identité numérique, ou IDN, peut être constituée par : un pseudo, un nom, des images, des vidéos, des adresses IP, des favoris, des commentaires etc. Cette identité sur internet a donc une influence sur la e-réputation, sur la façon dont les internautes perçoivent une personne.

Cette identité virtuelle se crée par le biais des réseaux sociaux, comme Facebook ou Twitter, ou des publications sur un blog. Les sites web de tous les genres construisent également notre identité, grâce à laquelle vous pouvez donc être connu et avoir une présence en ligne. Cependant, ces données, qui se retrouvent à la portée de tous, constituent un risque permanent pour les utilisateurs et pour la protection de leur vie privée. Aujourd'hui, les informations inscrites sur Internet sont très difficiles à effacer. C'est pour cette raison qu'il est préférable de bien réfléchir avant de laisser une trace numérique afin d'éviter toutes les conséquences négatives d'une mauvaise e-reputation. Il faut faire attention à ce que nous publions sur Internet et que nos données sont récupérées par les moteurs de recherche mais nous n'en connaissons pas forcément les mécanismes et les stratégies pour nous en prémunir (Olivier Ertzscheid, 2013: p 53).

b. Définition de la gestion de l'identité numérique:

A l'ère d'internet, l'expression de nos identités numériques est prise en porte-à-faux, ce qui exige de repenser notre façon de gérer notre identités numériques. D'un côté, l'invention par les citoyens-internautes de nouvelles modalités d'expression et de revendications identitaires, individuelles et collectives sont susceptibles de renforcer le lien social et l'existence démocratique. D'un autre côté, la propension de contrôle de ces identités à des fins économiques et politiques s'accroît via la captation, la fidélisation et la traçabilité des profils. Répression et surveillance de nos comportements numériques semblent plus que jamais d'actualité (Jean-Paul Fourmentraux , 2015: p 222).

La gestion de l'identité numérique, appelée également e-réputation, constitue aujourd'hui un enjeu essentiel pour une entreprise, quel que soit son secteur d'activité. En effet, une atteinte à la réputation est susceptible d'avoir un impact très négatif sur le résultat d'une entreprise et peut même dans certains cas entraîner sa facilite. Les exemples sont vraiment nombreux d'entreprises mal préparées à la gestion de telles crises qui ont un impact négatif sur la performance de l'entreprise, cette dernière qui n'a pas anticiper leur apparition, ni en maîtriser les effets, du moins autant que faire se peut.

Par ailleurs, la présence des entreprises sur le net sollicite une gestion de son l'identité numérique qui se présente à plusieurs niveaux : par des informations identitaires qu'elles émettent volontairement ou non et par des informations réputationelles émises par des acteurs externes et qui sont elles aussi volontaires ou non.

La diffusion de traces sur internet et l'évolution majeure est l' émission (et non l'existence) publique de tracés volontaires informels, c'est-à-dire de témoignages de salariés de l'entreprise. En cohérence avec la définition de l'identité numérique de l'entreprise ou de l'organisation, ces sources sont identitaires et portent des enjeux importants et nouveaux pour la réputation de l'entreprise.

Cependant, la présence numérique d'une entreprise ne se résume pas aux données identitaires volontaires ou non. En effet, des réactions à ces données identitaires ou des commentaires extérieurs sont la preuve des traces et tracés réputationnels d'une organisation et qui pourraient être classés de la façon suivante:

- le public externe peut émettre des jugements sur l'entreprise même sans être salarié ;
- les candidats à un recrutement sont considérés comme externes à l'organisation contrairement aux salariés ;
- les clients sont intégrés car l'activité commerciale d'une organisation détermine aussi sa qualité d'employeur.

La question de la gestion des identités numériques, dans le contexte de la multiplication des traces laissées consciemment ou non par les utilisateurs renvoie effectivement à de nombreux enjeux : droit à l'anonymat ou à l'oubli mais aussi usurpation d'identité, établissement de la confiance nécessaire aux interactions interpersonnelles ou marchandes, exploitation marketing ou managériale des traces individuelles, garantie d'espaces où initier des interactions en maîtrisant la visibilité de celles-ci.

Une meilleure gestion d'une identité numérique passe par la meilleure connaissance des outils et technologies en présence. Les priorités sont de surveiller ses propres traces et ce qui se dit de soi.

À partir des publications de l'entreprise sur internet et réseaux sociaux par exemple on peut définir votre identité numérique. En plus, elle peut être connue à partir des contenus publiés par d'autres personnes. C'est alors un moyen qui permet d'évaluer le comportement, l'émotion et la capacité intellectuelle d'une personne. Afin de donner une bonne image de sa vie, de nombreux internautes utilisent des outils d'alertes. Ces instruments permettent aussi de mieux gérer leur activité sur internet et leur e-notoriété.

En revanche, la gestion d'une identité numérique repose sur plusieurs piliers permettant d'éviter les risques liés à notre exposition en ligne parmi ses piliers protéger et préserver le nom d'utilisateur, définir son périmètre de sécurité, s'impliquer, veiller au grain se sont des principes indispensables sur la façon de gérer notre identité numérique.

La gestion d'une identité numérique dépend de la représentation orale ou graphique d'une personne étant le produit d'une réduction, consiste en la mise en évidence de signes qui distinguent empiriquement un individu d'un second.

Dans la communication médiée par ordinateur CMO, la représentation de l'utilisateur, telle qu'elle apparaît par défaut, ne permet pas de différencier un individu d'un autre. L'information minimale est le pseudonyme, qui ne constitue pas un critère assez distinctif pour identifier une personne, de nombreux utilisateurs possédant le même. La représentation acquiert un caractère distinctif par son alimentation : plus le profil utilisateur comporte de signes, plus la représentation est distinctive. Remarquons qu'à l'inverse, si les signes qui représentent les individus sont trop distinctifs, il n'existe plus de critères de mise en relation dans les moteurs de recherche pour « apparier les individus » (Cardon, 2008 : p. 107).

3. Comment se créer une identité numérique?

Par ailleurs, une identité numérique prouve que l'utilisateur du service est bien la personne concernée. Les bureaux de poste demandent souvent la création de ce dispositif. L'identifiant créé doit en principe correspondre à un seul individu.

De ce fait, il dispose de son propre code secret qu'il peut utiliser pour protéger son compte. Le processus de création d'une identification numérique est simple. Le site Web vous demande de visiter une page et d'entrer votre nom d'utilisateur ou votre mot de passe. Une notification par SMS sera alors envoyée. Ce message contient un code de sécurité derrière l'écran qui confirme que c'est bien vous qui êtes connecté. La validation vérifie ensuite la demande et vous permet d'accéder au site Web.

La numérisation est au cœur de la transformation sociale depuis plusieurs années. Les grandes entreprises, les petites entreprises et les start-ups entament le processus de numérisation. Bien sûr, le changement s'est fait sentir sur le marché du travail. C'est un domaine d'activité très prometteur et de plus en plus de professionnels se lancent dans les métiers du numérique. Du développement web au marketing digital, les collaborateurs

osent plonger dans le monde digital. Les outils d'identité numérique n'ont pas d'autre but que de permettre les processus :

- d'identification : présenter une identité;
- d'authentification : vérifier l'identité revendiquée par une personne, au moyen d'un objet qu'il possède, d'une information qu'il connaît, ou encore par une des caractéristiques physiques personnelles (biométrie). On parle d'authentification forte lorsque deux moyens sont mis en œuvre, par exemple un objet possédé plus la connaissance d'un secret. Par opposition, l'identification en tapant au clavier un identifiant et l'authentification en tapant un mot de passe n'apportent pas une sécurité suffisante dès lors que des enjeux commerciaux ou de protection de données sont en cause;
- de signature électronique : comme pour la signature manuelle, il s'agit d'engager sa responsabilité (commande, signature d'un contrat,…), et encore mieux, la signature électronique permet en plus de protéger le contenu du document (son intégrité).

4. Les différents types d'identité numérique:

Il faut savoir que si le fondement de l'identité numérique de l'entreprise ne diffère pas de l'identité individuelle, le nombre et la nature des acteurs concernés portent une distance certaine.

Selon certains auteurs, notamment Georges et Merzeau, dans le cas de l'identité individuelle, deux acteurs principaux déterminent le contenu des traces : l'individu lui-même mais aussi les dispositifs utilisés (Georges F, 2009: p 165).

En revanche, dans le cas des entreprises et selon les travaux de Quinio (Quinio 2013), de nombreux acteurs interviennent pour façonner une identité non pas éclatée mais fragmentaire (Quinio P, 2013: p p 167-178).

En effet, alors qu'un individu constitue le centre des traces dont l'espoir de rassemblement s'éloigne au fur et à mesure des progrès des algorithmes de traitement, dans le cas de l'entreprise, la variété des acteurs fragmente en morceaux dispersés et distants de l'identité de l'entreprise dont la maitrise devient alors un enjeu majeur ou plutôt un idéal.

Dans un graphique assez impressionnant Panoptykon détaille les trois couches d'information qui composent l'identités numérique en ligne. Il existe plusieurs types d'identités numériques qui répondent à différentes catégories d'informations, en fonction de la source, de son contenu et de son auteur.

Ces informations circulent aussi parfois à l'insu de leur utilisateur, et peuvent avoir une influence néfaste sur l'intégrité de la personne ou de l'entité correspondante. On peut facilement créer trois catégories distinctes d'identité numérique correspondant à l'origines des sources différentes et aux informations divulguées:

a. Premier type : déclaratif – ce que nous exprimons

La première couche dite déclarative, la plus restreinte, se compose des données que nous partageons, sur le web et les médias sociaux, à travers toutes sortes de services en ligne ou applications mobiles. Elle comprend les informations de nos profils, nos messages publics et privés, nos goûts, nos requêtes de recherche, les photos téléchargées, les tests et enquêtes que nous effectuons, les événements auxquels nous assistons, les sites Web que nous visitons et tout autre type d'interactions conscientes.

Ce type d'identité numérique correspond aux diverses informations qui ont été déclinées par la personne ou l'entité concernée, avec des renseignements variés, portant sur la nature du sujet, sur son état civil et sur d'autres éléments très objectifs.

C'est ce que Dominique Cardon (Cardon Dominique, 2008: p 22) appelait en 2008 l'identité déclarative (âge, sexe, ville, bio, intérêts, etc.), par laquelle la personne décide elle-même comment elle se représente.

b. Deuxième type : comportemental – les traces que nous laissons

La deuxième couche appelée également identité agissante, plus étendue, est composée de l'ensemble des métadonnées qui fournissent un contexte à nos choix par exemple: emplacement en temps réel, échanges personnels et professionnels, habitudes en ligne et hors ligne.

L'identité agissante est déterminée par les différentes actions menées sur le web par l'utilisateur. Ainsi, on pourra effectuer une trace de ce dernier en observant ses attitudes et ses habitudes à partir de son compte personnel. De même que son ami sur Facebook notamment. Ses données seront ainsi récoltées. Le code bancaire et le mot de passe n'ont plus aucun secret pour ces sites web en guise d'illustration. Par ailleurs, ces informations sont une vraie mine d'or pour certaines entreprises, qui utilisent des données de masse en tant que statistiques très instructives au niveau commercial. Une question se pose alors : où se limite le droit à la vie privée et aux données privées ?

Notre activité en ligne constitue notre identité agissante, qui complète, parfois à notre insu, notre identité narrative ou projetée. En effet, du fait de sa capacité à tracer toutes nos opérations en ligne, le web consigne des tas de données sur nous : visite de telle page, achat de tel article, performances à tel jeu. Ce qui rend notre empreinte numérique bien plus riche que nous ne l'imaginons.

c. Troisième type : calculatoire – ce que les algorithmes interprètent

La troisième couche identité calculatoire, infiniment plus vaste et parfois inquiétante, découle des interprétations de différents opérateurs et algorithmes qui sont en mesure de recomposer les différentes facettes de notre identité déclarative et comportementale pour extrapoler de nouveaux éléments sur nos goûts et convictions, notre appartenance culturelle ou sociale, nos forces et nos faiblesses.

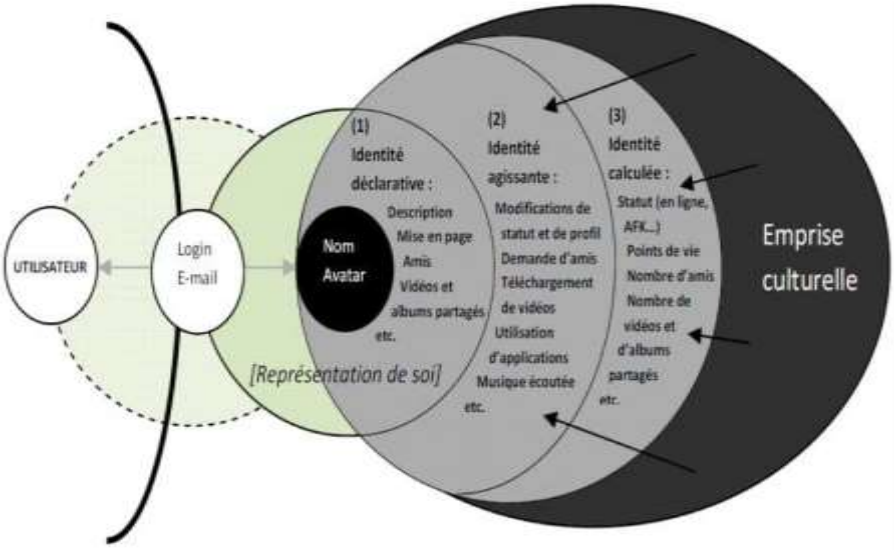
De l'analyse de nos traces numériques découlent des conclusions non seulement sur ce que nous faisons, mais aussi sur qui nous sommes en fonction de notre comportement et de nos métadonnées (Georges, F, 2009: p 193). L' « identité calculée » se

manifeste par des variables quantifiées produites d'un calcul du Système (exemple : nombre d'amis, nombre de groupes).

L'identité calculée résulte des différentes analyses menées à propos de l'identité agissante. Les conclusions permettent ainsi d'établir un profil de l'individu ou d'un service auquel il est affilié.

Or, pour regrouper ses différents types d'identité numérique le schémas suivant propose une illustration dont les utilisateurs prennent des décisions pour se présenter sur la toile il s'agit de la création de leurs identités. Elle peut comprendre une part de leur identité réelle, lorsque ils indiquent leur noms, prénoms, âge, etc. mais également une identité fictive afin de protéger leur anonymat, notamment lorsque ils font usage d'un pseudonyme et d'un avatar qui ne vous représentent pas. La figure suivante illustre les différents types d'identité numérique**:**

Figure 1. Les différents types d'identité numérique



Source: https://c-marketing.eu/identite-numerique-risques-enjeux-pour-les-entrepreneurs/#, consulté le 18 octobre 2022.

Kaufmann , dans son analyse de l'émergence de l'« invention de soi », parle de concept « barbe à papa » pour qualifier l'identité, tant les contextes d'utilisation et les éléments qui lui ont été associés sont pléthore. Il reprend ainsi la métaphore employée par Goffman pour illustrer le fait que le processus identitaire s'apparente à « un enregistrement unique et ininterrompu de faits sociaux qui vient s'attacher, s'entortiller, comme de la « barbe à papa », comme une substance poisseuse à laquelle se collent sans cesse de nouveaux détails biographiques » (J.-C. Kaufmann, 2004: p 21).

Cependant, le concept « barbe à papa » de Kaufmann tout n'est pas identité et que certaines informations sont liées directement au dispositif et interagissent avec les différentes formes de traces. Par ailleurs, un même outil peut être à la fois identitaire et réputationnel. Et enfin, la réputation des uns correspond à l'identité des autres (un

commentaire d'un statut est réputationnel pour le profil concerné (voir page écran) mais identitaire pour celui qui l'a rédigé) ce qui explique partiellement l'apparence inextricable de l'identité et de la réputation avec une vue globale.

5. Comment gérer son identité numérique sur le web ?

Les utilisateurs sont obligés de remplir leur profil avec le maximum d'informations pour pouvoir bénéficier d'une visibilité optimale sur la toile. A savoir que la diversité dans les modes d'expression par le biais d'une identité numérique (IN) est entretenue régulièrement par les réseaux socio numériques (RSN) sur lesquels la question de l'identification de l'individu se pose en termes de constitution de profil d'une part et en termes d'évolution et de renouvellement de ce profil d'autre part.

Néanmoins, la divulgation de tous ces renseignements ne peut pas se faire sans précautions. Voici quelques reflexes à avoir pour éviter de prendre des risques liés à votre image et à votre e-notoriété :

- **Gérer ses paramètres de confidentialité sur les réseaux sociaux**: Trop de personnes oublient cette étape indispensable. Les réseaux sociaux sont une source d'informations conséquentes et les paramètres de base ne vous protègent pas assez. Sans certaines modifications, vous vous exposez à une usurpation d'identité numérique. De plus, n'acceptez pas dans votre réseau des personnes que vous ne connaissez pas. Elles peuvent être malveillantes à l'égard de vos informations.
- **Se méfier de ce qui est gratuity**: « Si c'est gratuit, vous êtes le produit. » Lorsque vous naviguez, likez ou recherchez, vous dévoilez gratuitement vos choix de consommateurs. Pour les entreprises privées, ces données sont précieuses puisqu'elles permettent de mieux vous comprendre pour mieux vous vendre. De nos jours, naviguer sans donner d'informations, personnelles ou non, est quasiment impossible.
- **Changer de mot de passé:** Aujourd'hui, il existe des manières plutôt simples pour se procurer un mot de passe. Changer de mot de passe régulièrement rend cette tâche plus compliquée et sécurise un peu plus vos données personnelles et professionnelles. Idéalement, vous devez changer de mot de passe tous les trois mois.
- **Ne pas cliquer sur n'importe quel lien:** L'hameçonnage est une technique courante pour récupérer des informations. Le cybercriminel se fait passer pour une entreprise ou une personne de confiance soit par e-mail, soit par un faux site. Malgré la notoriété de cette arnaque, encore beaucoup d'internautes cliquent sur des liens dangereux.

Pour comprendre encore un peu mieux ce sujet, des schémas sur l'identité numérique ont été créés. Ils recensent les catégories d'informations divulguées selon les sites consultés. Désormais vous connaissez les dessous de l'IDN et vous avez toutes les cartes en main pour la gérer au mieux.

5. Risques & enjeux d'une identité virtuelle

Aujourd'hui, à l'heure du cloud, de l'hyper-connectivité, du travail nomade expose notre identité en danger si nous n'y mettons pas des garde-fous. En effet, l'explosion des ressources numériques avec l'avènement d'internet et maintenant du Web 2.0 a complètement transformé le monde de la communication d'entreprise. Les rumeurs concernant une entreprise ou un produit peuvent se répandre dans le monde entier en quelques heures et le cours de l'action d'une entreprise peut chuter de 20 % en une seule journée. Une campagne de diffamation peut nuire à l'image d'une entreprise pendant des années.

Cependant, les enjeux autour de l'identité numérique recouvrent des risques liés à la sécurité, à la protection de la vie privée, à des questions éthiques et à des considérations économiques.

Dans cette perspective, l'identité ne repose plus sur des affirmations définitives de projet de vie lié à un métier ou une situation personnelle mais plutôt sur des affirmations relatives à un moment de vie donné. Ce phénomène illustre la perte d'identité stable qui va de pair avec l'augmentation des événements éphémères et la diminution des expériences collectives porteuses de sens (Rosa, 2010, p 85). L'identité se trouve ainsi fortement transformée par l'accélération du temps ; à cet égard, celle-ci permet de penser et de comprendre les changements sociaux ainsi que le nouvel individu et ses nouveaux rapports à la société et à son identité (Dufour Baïdouri Armelle, 2013, p 134).

L'un des enjeux de premier plan de ce que l'on appelle « la société de l'information » est de permettre à chacun d'inverser la tendance entre l'identité numérique vécue et celle perçue, de reprendre le contrôle, de mesurer l'étendue de l'ensemble de ses traces identitaires et d'en circonscrire, si on le souhaite, c'est-à-dire le périmètre.

Comme la réputation, l'identité n'est pas figée. Elle évolue et se transforme dynamiquement au gré des interactions. II peut y avoir un décalage considérable entre l'identité online (numérique) et offline (dans le monde réel) car certaines personnes peuvent avoir une approche fractionnée et utiliser de multiples identités en fonction de leurs différentes utilisations (professionnelle, personnelle,.) et des réseaux fréquentés. II est toujours possible d'utiliser des outils technologiques pour naviguer de façon anonyme.

Dans le virtuel comme dans le réel, une marque forte et une entreprise solide se construisent en favorisant des relations de confiance avec un public cible. Ce processus exige beaucoup de temps et d'efforts. Et si quelque chose venait à briser cette confiance, les retombées et l'impact sur la perception des clients seraient potentiellement dévastateurs.

L'identité numérique d'une entreprise procède de la même logique multicouche que celle des individus. Et à chaque couche correspondent des enjeux et des risques spécifiques que l'entreprise ne saurait négliger, sous peine de voir sa croissance mise à mal.

a. La strate déclarative : image et branding

L'identité numérique d'une entreprise ne se résume pas à l'image qu'elle entend projeter d'elle-même (logo, publicité, image de marque) mais dépend surtout de l'image

perçue, amplifiée, voire déformée par les internautes, les consommateurs, les clients, les partenaires d'affaires. En cas de mauvaise interprétation, les conséquences peuvent être désastreuses pour l'entreprise.

Vu sous cet angle, on comprend que la création d'une identité forte n'est pas l'apanage du seul service marketing. C'est l'ensemble de l'entreprise qui doit contribuer à la construction de cette identité cohérente -RH, service achat, commerciaux, service client. Tous participent à l'élaboration de l'image de l'entreprise (à travers leurs communications, leurs partages et leurs commentaires en ligne, par exemple). Il y a donc un véritable travail d'information et de formation à prévoir au sein de l'entreprise.

b. La strate comportementale : notoriété et e-réputation

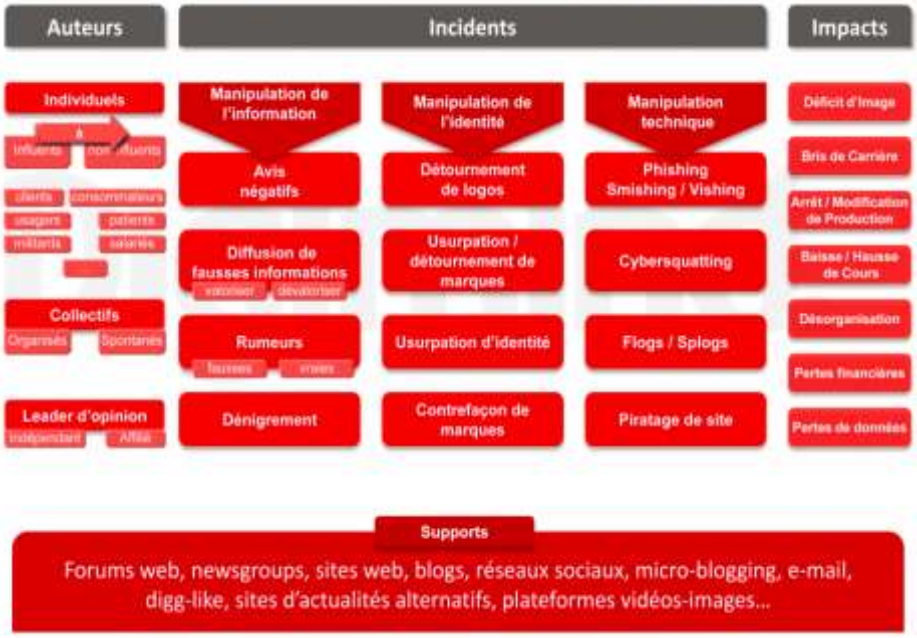
Aucune entreprise ne peut l'ignorer. La propagation d'un bad buzz via les réseaux sociaux peut faire ou défaire la réputation de l'entreprise. Or les lanceurs d'intox sont nombreux : des employés de l'entreprise aux consommateurs en passant par les concurrents, la presse, les influenceurs. Tout un petit monde qu'il faut suivre et avec lesquels il faut communiquer pour tenter de maîtriser son e-réputation et éviter des dérives indésirables.

La vitesse de propagation d'un bad buzz peut être extrêmement dommageable pour l'entreprise. L'équipe ou la personne responsable de la communication doit en être pleinement consciente et doit pouvoir intervenir rapidement et être capable de traiter efficacement tout problème touchant à la réputation de l'entreprise.

Mais sans aller jusqu'à cette extrémité, chaque entreprise doit mettre en place une veille efficace pour surveiller, gérer, réduire les risques potentiels et influencer positivement les activités en ligne qui façonnent sa réputation. En ligne comme dans la « vraie vie », mieux vaut prévenir que guérir !

Car les risques liés à l'e-réputation recouvrent de nombreux enjeux, résumés dans ce tableau de Digimind.

Table 1. les risques et les enjeux liés à l'e-réputation selon Digimind



Source: Christophe Asselin – Digimind, https://c-marketing.eu/identite-numerique-risques-enjeux-pour-les-entrepreneurs/#, consulté le 18 octobre 2022.

c. La strate sécuritaire : réglementation et cybersécurité

Depuis quelques années, et plus encore depuis l'arrivée du GDPR, les entreprises sont amenées à considérer les données personnelles comme un bien précieux à respecter et à protéger**.** Les employés, les clients, les partenaires … chacun a des droits clairement définis associés à son identité numérique.

d. L'adoption accélérée du cloud et du travail nomade pose de nouveaux problèmes

Assurer la portabilité et l'accessibilité des données mais aussi sécuriser et protéger utilisateurs et documents face aux risques accrus de fraude ou piratage. C'est que les cyber-attaques se multiplient. Or, les applications privilégient encore trop souvent la facilité d'utilisation à la sécurité. C'est donc à l'entreprise qu'il incombe la tâche ingrate de sécuriser les données, de contrôler efficacement les personnes qui y accèdent et la manière dont elles les exploitent.

6. Conclusion

Être connu c'est bien, mais être prudent c'est encore mieux. La même chose s'applique en ligne comme dans la "vraie vie". Mieux vaut prévenir que guérir. Dans ce sens peut-on contrôler sa construction identitaire ?

En effet, se construire une réputation électronique prend plus ou moins de temps. Cependant, nous sommes préoccupés par le risque de subir les ramifications d'un manque d'e-conscience. De plus, révéler votre identité sur des plateformes publiques recouvre de multiples risques.

Cependant, la protection des données personnelles est donc importante pour éviter les abus. Il s'agit de concilier les données numériques circulant sur internet avec le droit à la vie privée des individus. Pour les individus et également pour la société il est urgent de reprendre le contrôle de leurs identités numériques.

L'internet a été conçu pour conserver les traces numériques de tous ses utilisateurs. Ces historiques reflètent les activités en ligne effectuées par une personne ou une collectivité. De ce fait, notre identité numérique est complexe et difficile à maîtriser.

La question de l'identité numérique et de l'e-réputation reste toujours sensible dans l'écosystème internet, aussi bien pour les particuliers que pour les entreprises, quelque soit pour les usages individuels ou collectifs. Nous avons présenté dans cet article l'état de la recherche sur la question de l'identité numérique par un tour d'horizon sur les enjeux fondamentaux à maîtriser pour pouvoir garder le contrôle et gérer notre présence en ligne. Mais, on s'interroge toujours sur l'avenir de l'identité numérique notamment sur la dimension juridique et les enjeux de l'usage de nos données personnelles par les moteurs de recherche.

Si les fragments de notre identité permettent aux acteurs du web de mieux connaître nos préférences et ainsi d'affiner les publicités qui nous sont proposées, il existe, à l'autre bout de la chaîne, des entreprises qui proposent de gérer notre image à travers nos données personnelles par des stratégies mise en place pour surveiller notre

identité numérique. Alors pensez donc à rester vigilant quant à l'utilisation de vos données.

7. Références

- B. Quinio (2013), Les réseaux sociaux virtuels : pour une prise en compte de l'activité reliant sujet, outils et finalité. Application à l'étude des identités numériques, l'Harmattan, Paris.
- Cardon Dominique (2008), « Le design de la visibilité : un essai de cartographie du web 2.0 », *Réseaux*, Lavoisier, Paris.
- Centre National de Ressources Textuelles et Lexicales, https://www.cnrtl.fr/, (consulté le 19 octobre 2022).
- Christophe Asselin – Digimind, https://c-marketing.eu/identite-numerique-risques-enjeux-pour-les-entrepreneurs/#, (consulté le 18 octobre 2022).
- C-Marketing,https://c-marketing.eu/identite-numerique-risques-enjeux-pour-les-entrepreneurs/#, (consulté le 20 octobre 2022).
- Dufour Baïdouri Armelle (2013), L'identité numérique : un levier d'innovation pour les marques ?, Thèse de doctorat en Sciences de l'Information et de la Communication, Université Panthéon-Assas, France.
- F. Georges (2009), «Représentation de soi et identité numérique, Une approche sémiotique et quantitative de l'emprise culturelle du web 2.0», *Réseaux*, vol. 2009/2 – n° 154.
- Georges F (2011), « L'identité numérique sous emprise culturelle » De l'expression de soi à sa standardisation, Les Cahiers du numérique, 2011/1 Vol. 7.
- Georges, F (2009), « Représentation de soi et identité numérique. Une approche sémiotique et quantitative de l'emprise culturelle du web 2.0 ». Réseaux. 2/2009- n° 154.
- J.-C. Kaufmann (2004), L'invention de soi. Une théorie de l'identité, Armand Colin, Paris.
- Jean-Paul Fourmentraux (2015), Identités numériques. Expressions et traçabilité, CNRS, coll. « Les Essentiels d'Hermès », Paris.
- Katarzyna Szymielewicz, Votre identité numérique comporte trois couches et vous ne pouvez en protéger qu'une seule, Quartz, https://qz.com/1525661/your-digital-identity-has-three-layers-and-you-can-only-protect-one-of-them, (consulté le 19 octobre 2022).
- Olivier Ertzscheid (2013), Qu'est-ce que l'identité numérique ? Enjeux, outils, méthodologies, Marseille, OpenEdition Press, collection. « Encyclopédie numérique ».
- Rosa H. (2010), Accélération - Une critique sociale du temps, La découverte.