Vie privée

« La révolution numérique était en train de bâtir brique par brique le rêve millénaire de toutes les dictatures - des citoyens sans vie privée, qui renonçaient d'eux-mêmes à leur liberté. »

Bernard Minier, tiré de son thriller *Une putain d'histoire*

Source
The conversation
François Nicolle
18 octobre 2017

1. L'identité numérique, la face cachée de notre identité ?

« Tout le monde ment : le big data, les nouvelles données, et ce que l'Internet peut nous apprendre sur qui nous sommes vraiment » est un livre de Seth Stephens-Davidowitz analysant nos recherches Google. Cet ancien salarié du géant américain nous interpelle sur notre identité numérique.

L'existence et l'analyse de ces données cachées sous-entendent que notre identité numérique ne résulterait pas simplement de ce que nous diffuserions mais révélerait aussi notre présence masquée sur Internet. Par exemple, chaque recherche que nous effectuons dans un moteur de recherche peut donner des informations sur nos envies ou nos craintes sans que nous ne les exprimions.

Or cette gestion de l'identité numérique est centrale dans notre société. Plus de la moitié des employeurs font des recherches Internet sur les candidats ; les tweets des personnalités politiques ressortent avant chaque élection, la moindre trace laissée sur Internet peut parfois prendre des proportions incontrôlées.

L'identité numérique devient également importante dans nos établissements d'enseignement supérieur. En effet, les néo-bacheliers sont des *digital natives*, pour la plupart nés après Google (1998), qui ont découvert Facebook dès l'école primaire (2004) puis Instagram (2010) au collège.

Qu'est ce que l'identité ?

Dans le dictionnaire Larousse, l'identité est définie comme le « caractère permanent et fondamental de quelqu'un, d'un groupe, qui fait son individualité, sa singularité. »

Le terme d'identité trouve son origine du latin *idem*, un dérivé du verbe être, qui signifie *le même*.

Si la définition de l'identité fait débat en sciences sociales, un certain consensus se retrouve sur l'essence de ce concept.

C'est notamment le cas de la définition d'Alex Mucchielli dans son ouvrage _L'identité : « ensemble de significations apposées par des acteurs sur une réalité physique et subjective, plus ou moins floue, de leurs mondes vécus, ensemble construit par un autre acteur. C'est donc un sens perçu donné par chaque acteur au sujet de lui-même ou d'autres acteurs ».

Ainsi l'identité serait unique, permettant de se distinguer des autres, de se reconnaître, de s'identifier à autrui.

Et l'identité numérique alors ?

La définition de l'identité numérique est, par nature, beaucoup plus récente et discutée.

Pour Julien Pierre, « l'identité numérique est une représentation, c'est-à-dire la redite d'un état, structurée par des capitaux qui la composent et les supports qui la contiennent, structurant les

conditions d'existence sociale des individus ». Ainsi selon ce chercheur, l'identité numérique n'est que le prolongement de l'identité réelle de l'individu. Cette identité est basée sur l'existence sociale, donc le rapport aux autres.

S'agissant d'Internet le rapport aux autres ne comprend que ce qui est visible par autrui, cette définition ne prend donc pas en compte les requêtes des individus.

Pascal Lardellier définit aussi l'identité numérique autour du rapport aux autres, il met en avant le développement de l'ego avec le 2.0, avec notamment l'avènement d'un « Je expressif numérique ». Cet ego se développe avec le web social et la possibilité de s'exprimer, se mettre en avant, et donc prend plus en considération ce que nous publions que ce que nous faisons sur le web.

Dominique Cardon, de son côté, nous explique que l'identité numérique est « moins un dévoilement qu'une projection de soi. » Cette définition tend à contredire la définition classique de l'identité car nous sortons de l'équation A=A pour devenir A=A'.

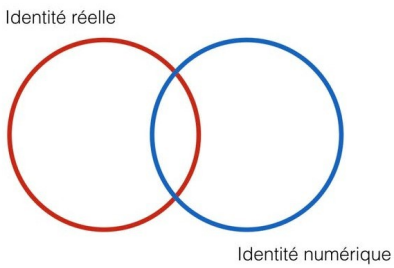
Pour Fanny Georges « l'identité devient mixte elle se compose d'informations acquises en face-à-face et dans les sites sociaux ». Cette identité numérique correspond à la somme des traces conservées par le support multimédia, l'interprétation des traces de l'Autre envisagées par le sujet comme support de présentation de soi dans une « présence à distance »

Toujours selon cette chercheuse l'identité numérique est composée de 3 identités : l'identité déclarative (description, mise en page, l'identité agissante (modification de statut et de profil) et l'identité calculée (nombre de posts, de tweets ou d'amis)

Cette définition est très détaillée mais reste circonscrite à la partie visible par les autres sur les réseaux sociaux, elle est néanmoins très intéressante dans sa structure en prenant en compte plusieurs niveaux d'identité.

Une nouvelle définition de l'identité numérique

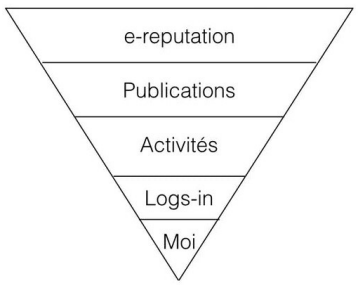
Comme certains auteurs le montrent, nous pouvons considérer que l'identité numérique est complémentaire de l'identité réelle mais elles ne sont pas assimilables, car, sous couvert d'alias, d'avatar, de pseudo, certains individus ont une vie totalement différente *online* que dans la vie réelle. Les pratiques, elles-mêmes, sont différentes, même si une base commune existe entre ces deux identités.



Identité numérique/identité réelle @FrançoisNicolle.

La définition que nous proposons s'appuie sur les définitions précédemment citées en prenant en compte la dualité du visible et du masqué.

L'identité numérique se compose de 5 strates : *e-réputation*, *publications*, *activités*, *logs-in*, et *Moi*.



Typologie identité numérique @FrançoisNicolle.

E-réputation : ce que les autres disent de nous, cela comprend tous les articles, publications qui mentionnent notre nom. Il s'agit par exemple des résultats d'une recherche Google sur notre nom.

Publications : ce que nous publions sur les différents sites sociaux. Par exemple nos publications sur Facebook, Instagram ou Twitter. C'est ce que nous rendons délibérément public.

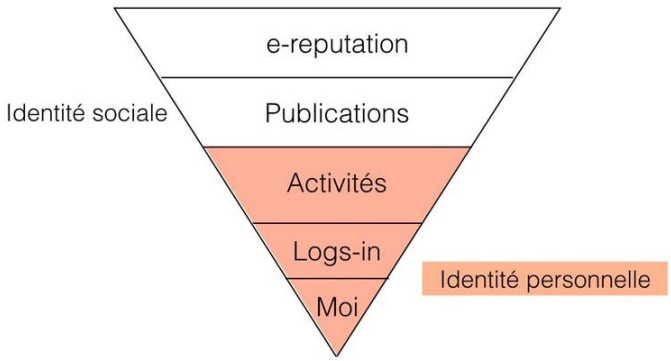
Activités : ce que nous faisons sans que les autres internautes soient au courant. Cela comprend notre historique de navigations, nos cookies, nos recherches sur les moteurs, les messages écrits non envoyés.

Logs-in : assimilables à l'identité juridique, ce sont nos identifiants, nos mots de passes, il s'agit du processus d'identification

Moi : le Moi est l'identité intrinsèque à l'être humain.

Dans cette définition, l'identité numérique n'est plus une projection mais se rapproche d'un dévoilement. En effet nous pouvons distinguer deux types d'identité numérique. Tout comme pour l'identité réelle, il y a l'identité personnelle et l'identité sociale.

Or, pour reprendre l'expression de Dominique Cardon, « l'identité sociale est une projection de soi. » Elle correspond à ce que nous faisons dans le jeu social, pour se donner un rôle en société et comprend notre e-réputation et nos publications, ce que nous souhaitons rendre public. Mais notre identité numérique comprend aussi nos activités, logs-in et Moi, qui nous sont propres et ne contribue pas à ce jeu d'image.



Identité sociale/identité personnelle @FrançoisNicolle.

Il peut d'ailleurs exister de fortes tensions entre ces identités sociales et personnelles. Pour caricaturer nous pourrions prendre l'exemple d'un hacker qui peut dans le même temps tenir un blog sur la citoyenneté en ligne.

Un espace de liberté à domestiquer

Cette identité numérique nous ouvre un nouvel espace de liberté au travers des alias, des avatars et autres pseudos qui nous permettent d'être perçu pour ce que nous voulons. Si cet espace de liberté est à conquérir, il est surtout à préserver. En effet en communiquant toutes nos données aux géants du web nous dévoilons une part importante de nous : nos achats, nos trajets, nos désirs… Cette concentration de données au profit de quelques acteurs et le risque de dérives potentielles qui en résulte doit nous alerter sur la nécessaire éducation à l'identité numérique.

D'autant plus si nous imaginons que certains fondateurs de réseaux sociaux pourront faire le choix de la politique dans un futur proche.

Protéger son identité c'est aussi protéger sa liberté.

Source
Slate.fr
Aurélie Rodrigues
28 mars 2018

2. Données personnelles : ce que Facebook et Google savent vraiment sur vous

Depuis les révélations de l'affaire *Cambridge Analytica*, nos données personnelles sont devenues une réelle préoccupation. *Facebook* vient tout juste de sortir un nouvel outil qui permet à ses utilisateurs de supprimer plus facilement le contenu qu'ils ont partagé via le réseau social. Mais le mal est fait : votre localisation, l'historique de vos recherches, vos mails, vos téléchargements en torrent… ces informations peuvent se révéler préjudiciables si elles sont exploitées contre vous. Eh oui, c'est bien pire que ce que vous pensiez.

Dylan Curran, expert data, s'est plongé au plus profond des données qu'il a partagées avec *Facebook* et *Google*. Voici quelques-unes de ses conclusions :

Vos données Google peuvent remplir plusieurs millions de documents Word

- Google vous suit partout. Si la géolocalisation est activée sur votre smartphone, *Google* sait où vous allez. Il est possible de visualiser une carte de vos déplacements en suivant ce lien : google.com/maps/timeline?pb. La date et l'heure sont bien sûr indiquées sur chaque entrée GPS…
- Google adapte ses publicités à votre profil. Les renseignements que vous avez partagés sur Google comme votre localisation, votre sexe, votre âge, vos hobbies, votre situation amoureuse ou même votre poids servent à créer votre profil publicitaire. La publicité « *Des rencontres près de chez toi* », ça vous dit quelque chose ? Pour voir votre profil publicitaire : google.com/settings/ads/
- Google Takout: toutes vos données dans un même fichier. Il est possible de demander à Google de vous envoyer les données qu'il a conservées à propos de vous. Dylan Curran a reçu un fichier de 5,5 Go soit l'équivalent de trois millions de documents Word. Ce dossier contenait ses favoris, tous ses mails, ses contacts, ses documents *Google Drive*, son historique de recherche Google et Youtube, ses déplacements, les téléphones qu'il a possédés, les sites qu'il a créés... la liste n'en finit pas.

En feuilletant son historique de recherches, Dylan Curran a notamment découvert que ses téléchargements en torrent étaient visibles... Des téléchargements illégaux...

Pour télécharger votre contenu Google : google.com/takeout

Facebook conserve une quantité gigantesque d'informations sur vous

Le réseau social, quant à lui, conserve vos historiques de conversations *Messenger*, les documents et les messages audios que vous avez reçus ou envoyés et les contacts sur votre téléphone. Mais ce n'est pas tout, il y a aussi les photos et vidéos que vous avez envoyées et reçues.

Mais Facebook va encore plus loin, il fait du profilage : selon vos mentions « J'aime » et vos sujets de conversations sur Messenger, il détermine ce que vous aimez. Par exemple, Dylan Curran affectionne le sujet « fille ». Encore plus inquiétant : il a découvert que Facebook conservait ses historiques de connexion : l'heure, l'endroit et les appareils utilisés pour se connecter.

Ce qu'il faut retenir

Comme le souligne Dylan Curran, si ces informations venaient à tomber entre de mauvaises mains, elle pourraient être utilisées à mauvais escient. Il suffit d'avoir les identifiants du compte Google ou Facebook de la personne en question et vous avez accès à son journal intime détaillé, très détaillé.

Malgré tout, tous les jours, nous acceptons de rendre ces informations disponibles aux géants du web. La phrase « *Big Brother is watching you* » résonne bien plus fort que jamais.

Source
Watson
Fabien Feissli
7 septembre 2021

3. Comment lutter contre les photos non-consenties sur les réseaux sociaux ?

Aujourd'hui, il suffit de deux clics pour prendre en photo quelqu'un et diffuser l'image sur Internet. Une situation qui impacte notre vie privée et peut conduire à des cas de cyberharcèlement. Une recherche menée par la HEC Lausanne pointe différentes solutions pour lutter contre le

problème.

Une photo d'une soirée trop arrosée, une image volée dans les vestiaires de gym ou encore un cliché en train de se gratter le nez. À l'ère des smartphones et des réseaux sociaux, en deux secondes, vous pouvez vous retrouver sur Internet dans une position peu valorisante. « Les cas les plus extrêmes, c'est la pornodivulgation. Mais même les photos les plus banales peuvent nous porter préjudice », observe Kevin Huguenin, professeur à la Faculté des HEC de l'Université de Lausanne.

« On a beau faire attention à protéger notre vie privée, elle peut être mise à mal par les autres »
Kevin Huguenin, professeur à la HEC Lausanne

Celui qui dirige le laboratoire de sécurité de l'information et protection de la vie privée souligne à quel point nous sommes désormais dépendants des autres pour préserver notre sphère privée en ligne : « L'un des exemples les plus saillants, ce sont les photos publiées sans notre consentement. »

Ces dernières peuvent, par exemple, poser problème vis-à-vis d'un futur employeur qui cherche à en savoir davantage sur vous sur Internet. « Le cyberharcèlement est aussi de plus en plus répandu, notamment chez les très jeunes », pointe Kevin Huguenin.

Flouter les visages sur toutes les photos, est-ce la solution?

Selon les recherches qu'il a menées avec son collègue Mauro Cherubini, 16 % des utilisateurs des réseaux sociaux interrogés ont déclenché un conflit en partageant une photo sans consentement, au cours des douze derniers mois précédant l'étude, et environ 7 % ont subi des conséquences graves, comme l'humiliation publique, la discrimination ou la pornodivulgation.

« Ce qui pourrait pousser les réseaux sociaux à s'intéresser au problème, c'est le risque que les utilisateurs partent sur un autre site s'ils ne se sentent pas en sécurité »
Kevin Huguenin

Pour tenter de remédier au problème, les deux professeurs à HEC Lausanne ont publié une étude dans laquelle ils proposent plusieurs solutions concrètes. Des solutions dont ils espèrent que les géants comme Facebook ou Instagram s'inspireront :

- Un dispositif qui floute automatiquement le visage de toutes les personnes présentes sur une photo lorsque celle-ci est publiée (à l'exception de celui de l'auteur). Les concernés doivent ensuite valider l'image pour que leur visage soit déflouté.
- Un message d'avertissement visant à sensibiliser l'utilisateur avant qu'il ne publie une photo et l'inciter à demander l'autorisation des autres personnes présentes sur l'image.

« Ce qu'on a observé, c'est que les gens avaient besoin de certitudes. Ils préfèrent donc une approche où on bloque techniquement la publication plutôt que de la sensibilisation », analyse Kevin Huguenin.

Des robots comme médiateurs

Une autre proposition a émergé suite aux discussions des chercheurs avec les utilisateurs. « Certains ont proposé un système de médiation avec l'idée que ce conflit entre la personne qui publie et celle qui figure sur l'image peut se résoudre par le dialogue », détaille le professeur à HEC.

Problème, des centaines de millions de photos sont publiées chaque jour sur Internet. « Il est impossible que des humains animent ces discussions. On a donc pensé à des chatbots (réd: une intelligence artificielle qui gère une conversation) », poursuit Kevin Huguenin, qui souligne que l'option sera étudiée dans les mois à venir par son équipe.

Prendre le temps de réfléchir et de dialoguer

Sociologue du numérique à l'Université de Lausanne, Olivier Glassey confirme l'importance de s'intéresser au problème : « On ne sait pas comment ces images de nous postées par d'autres vont circuler, ni à quel moment elles vont réapparaître. Cela constitue une sorte de menace invisible. »

« Au moment de prendre la photo, est-ce qu'on pense aux conséquences pour les personnes sur l'image ? »
Olivier Glassey, sociologue du numérique

À ses yeux, les smartphones n'ont cessé de simplifier et d'accélérer la prise et la publication de photos ces dernières années. « C'est dans cette spontanéité encouragée que vont se nicher les problèmes de divulgation d'images. Il reste peu d'espace pour réfléchir aux conséquences. »

Si le sociologue est convaincu que l'on pourrait faire mieux techniquement pour protéger la vie privée des utilisateurs, il souligne que les algorithmes ne sont pas le seul remède : « Ce n'est pas la technologie qui va apporter l'entièreté de la solution à un problème qu'elle a créé. »

« Les gens ont envie de communiquer, mais ils aimeraient avoir la garantie que cela ne restera pas »
Olivier Glassey, sociologue du numérique

De ce point de vue là, Olivier Glassey apprécie d'ailleurs le dispositif de floutage imaginé par la HEC Lausanne. Selon lui, le système va amener des négociations entre les différentes personnes en les forçant à dialoguer, pour savoir pourquoi ils ont validé, ou pas, une photo. « Nous n'avons pas tous la même perception de ce qui est gênant. Ce sont des enjeux dont on ne parle pas souvent et dont il faudrait discuter davantage. »

Garder le contrôle sur son image

Juriste spécialisé dans le droit des nouvelles technologies, François Charlet va dans le même sens. Il préfère pourtant la seconde solution proposée par Kevin Huguenin et son équipe, c'est-à-dire les messages de sensibilisation. « Il y a un côté éducatif, cela permet de rappeler qu'il y a des choses qui se font et d'autres pas. Au-delà de questions juridiques, il y a aussi le savoir-vivre. »

« Sans tomber dans la paranoïa, on ne sait jamais la manière dont les images, même banales, peuvent se retourner contre nous »
François Charlet, juriste

Le juriste rappelle toutefois que prendre et publier un cliché n'est jamais anodin. Même pour une photo quelconque, chacun a le droit de décider de la manière dont son image est utilisée. « Et même si vous êtes d'accord sur le moment de faire une photo, vous ne dites pas oui à plus que ça. Publier l'image sur les réseaux sociaux va plus loin que l'autorisation implicite que vous avez donnée. »

Source
rts.ch
Pauline Turuban
4 octobre 2017

4. Les bons réflexes pour protéger ses données personnelles sur internet

Moteurs de recherche, navigateurs, réseaux sociaux, applications... Ces outils du quotidien sont de véritables aspirateurs à données personnelles mais quelques précautions simples peuvent limiter les fuites.

Faire le vide dans son navigateur

Les navigateurs (Explorer, Safari, Chrome, ...) stockent tout : login, mots de passe, achats, clics sur des sites de rencontre, tout y passe. C'est pourquoi il est important d'effacer régulièrement les cookies.

« Ce sont eux qui permettent de tracer les requêtes d'un même utilisateur, parfois même à travers plusieurs sites », explique Philippe Oechslin, chercheur en sécurité informatique à l'EPFL. Certains navigateurs disposent d'une option permettant de refuser les cookies de sites tiers. Autre astuce : activer le mode « navigation privée ».

Limiter ses connexions à Google

Plus Google sait de choses sur vous, mieux il se porte. Le géant informatique « incite à être connecté en permanence sous prétexte d'offrir des services personnalisés, mais cette simplification est payée par les données de l'utilisateur », alerte Solange Ghernaouti, spécialiste de la cybersécurité à l'Université de Lausanne.

La chercheuse invite à varier de temps en temps les moteurs de recherche et les fournisseurs de services afin de ne pas laisser toutes ses informations au même endroit. Évitez d'être connecté à Google lorsque vous faites une recherche, de sorte qu'elle ne soit pas ajoutée à votre profil personnel. Il faut y être attentif si vous utilisez en même temps d'autres services en ligne de Google tels que

Gmail, Google Drive ou autre.

Réclamer son historique

Google garde un historique -parfois étonnamment précis- de votre activité en ligne, qu'il est possible de consulter et d'effacer sur la page myactivity.google.com.

La page https://www.google.com/maps/timeline permet quant à elle de consulter et d'effacer l'historique de localisation.

Une nouvelle fonctionnalité sur Facebook permet aussi de demander au réseau social les informations qu'il a accumulées sur vous. « Cette démarche est intéressante car elle peut permettre de prendre conscience de tout ce que l'on a donné. Plus les gens le feront, plus les géants d'internet seront forcés de rendre des comptes », relève Solange Ghernaouti.

Le pire espion, votre smartphone

Quasiment toutes les applications demandent d'accéder à votre localisation. Si vous acceptez, le moindre de vos déplacements sera enregistré. La bonne nouvelle, c'est que si elle ne vous est pas utile, cette fonction peut être désactivée dans les paramètres de votre appareil.

Pour ce qui est des applications, « la grande majorité ne sont pas altruistes », avertit Philippe Oechslin. « Leurs créateurs gagnent de l'argent soit en affichant de la publicité soit en vendant les informations qu'elles arrivent à glaner sur leurs utilisateurs » poursuit l'expert.

Les applications doivent déclarer explicitement les droits d'accès dont elles veulent faire usage (par exemple l'accès à l'appareil photo, la localisation ou votre agenda). « Si une application de lampe de poche demande l'accès à votre localisation, il faut refuser et désinstaller l'application », poursuit Philippe Oechslin.

Détail ironique : ces applications trop intrusives sont facilement détectables par d'autres applications censées scanner votre téléphone, comme F-Secure, Eset ou Sophos.

Méfiez-vous des questionnaires

Les pétitions, sondages ou autres formulaires de contact en ligne peuvent servir à vous soutirer des données qui seront plus tard revendues à des fins de publicité ciblée. « Soyez attentifs aux champs obligatoires et donnez le plus de fausses informations possibles », conseille Solange Ghernaouti.

Ce qui est posté sur Facebook ne vous appartient plus

Les spécialistes ne le diront jamais assez, la confidentialité n'existe pas sur Facebook et tout ce qu'on y poste est utilisé, à des fins pas toujours très transparentes. « L'usage idéal de Facebook serait de s'en passer », plaisante Solange Ghernaouti. « Le plus simple est de considérer que toute information que l'on poste sur Facebook est publique », résume Philippe Oechslin.

La chercheuse appelle à s'interroger sur l'utilité de chacun de ses actes sur le réseau social. « Aimer une publication, réagir, partager ce qui relève de l'intime et du sentiment... C'est permettre à Facebook de dresser un profil personnalisé. » Et d'énoncer une dernière recommandation : « Ce n'est pas parce que l'on a rien à cacher qu'il faut tout montrer ».

Source
Korii
Barthélemy Dont
2 juillet 2019

5. Comment effacer sa mauvaise réputation sur Google

Des entreprises spécialisées peuvent créer un écran de fumée pour camoufler les résultats négatifs associés aux noms.

Si vous cherchez sur internet le nom d'Adrian Rubin, vous trouverez que de nombreuses personnes talentueuses partagent ce patronyme. Adrian Rubin est un directeur créatif, auteur d'un livre sur le design. Adrian Rubin est aussi une chercheuse spécialisée sur le climat et militante écologiste. Un troisième homonyme est le PDG d'une entreprise d'immobilier, un quatrième offre une bourse scolaire.

Caché au milieux de ces résultats élogieux se trouve en revanche une page web moins glorieuse : le site du ministère de la Justice des États-Unis indique qu'un certain Adrian Rubin a été condamné à trente-sept mois de prison et au remboursement de près de dix millions de dollars (8,8 millions d'euros) à la suite d'une escroquerie.

Le seul Adrian Rubin à réellement exister est l'escroc : les autres sont en réalité des alter ego,

créés de toute pièce par une entreprise chargée d'améliorer sa réputation en ligne. Adrian Rubin n'est pas le seul à s'être fait un lifting numérique – à ses côtés se trouvent, selon Buzzfeed News, des médecins, des businessmen ou encore des criminels.

Le **SEO** (pour *search engine optimization* : optimisation pour les moteurs de recherche) est un ensemble de techniques visant à optimiser la visibilité d'une page web dans les résultats de recherche

Les entreprises qui offrent ce genre de services sont spécialisées dans le SEO, l'optimisation pour les moteurs de recherche. En clair, elles s'arrangent, moyennant finance, pour que les algorithmes de Google ne fassent plus ressortir d'informations négatives sur leurs client·es.

Écran de fumée numérique

La difficulté tient dans les performances desdits algorithmes. Il ne suffit pas de mettre en ligne quelques sites web positifs et remplis d'homonymes pour éclipser les autres résultats –en particulier s'ils proviennent de sites solidement référencés, comme des médias ou des sites officiels.

Créer de faux comptes Twitter et Facebook est un bon début : ces sites apparaissent systématiquement en haut des recherches. Mais cela ne suffit pas. C'est pour cela que Rubin dispose d'une bourse scolaire, une tactique courante de SEO. Il suffit de promettre une somme, ici mille dollars, afin d'aider un·e lycéen·ne à s'inscrire à l'université. Ainsi, Rubin se retrouve cité dans la rubrique "aide financière" de l'université du Maine. Un site important qui, Graal pour le référencement, dispose de l'extension « .edu », réservé aux universités –donc jugé extrêmement fiable.

Autre tactique : les livres autoédités sur Amazon. Via une société nommée Home Funding Corporation, Ian Leaf a escroqué des millions au trésor britannique. Lui aussi désire donc nettoyer internet de ce passé sombre. Jouer sur son simple nom ou prénom ne suffirait pas –quiconque taperait « Ian Leaf HFC » dans Google risquerait de découvrir le pot aux roses.

Pour parer à ce problème, Ian Leaf a autoédité sur Amazon un livre intitulé *Ian Leaf's Starting a HFC Business at Home*. Couverture rose et stock photo d'une jeune femme, HFC signifie ici « *High Fashion Clothing »*, vêtement de haute couture, et noie du même coup la référence à la société incriminée.

Les faux sites peuvent aussi être dopés artificiellement grâce à des « réseaux de liens », des sites internet bien référencés qui, contre une somme d'argent, proposent de poster des liens vers le site de leurs client·es. Qui, par capillarité, sont à leur tour propulsés en haut des résultats Google.

Source
Usbek & Rica
Lucile Meunier
27 juillet 2019

6. Données personnelles : une étude enterre (définitivement) l'anonymat

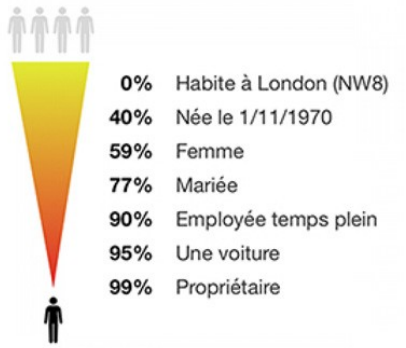
Même si leurs données ont été anonymisées, 83 % des Américains peuvent être ré-identifiés à partir de leur genre, de leur date de naissance et de leur code postal, selon une nouvelle étude.

Les données sont devenues la clef de voûte de l'économie moderne. Essentielles pour les progrès médicaux comme la lutte contre le cancer, elles sont aussi utilisées dans le domaine du ciblage publicitaire. Mais assez souvent, surtout dans le secteur de la santé, les données sensibles sont anonymisées avant de pouvoir être partagées ou vendues. C'est ce qu'on appelle la dé-identification : on retire de la base de données les informations permettant d'identifier facilement une personne. Par exemple, les hôpitaux effacent les noms des patients, leurs adresses, leurs dates de naissance, et peuvent intégrer de fausses valeurs.

Mais toutes ces précautions pour protéger l'anonymat sont vaines, affirment des chercheurs de l'Université catholique de Louvain et de l'Imperial College de Londres, dans une étude publiée dans *Nature* le 23 juillet 2019. Ils ne sont pas les premiers à exposer les failles de l'anonymisation des données, déjà mises en avant dans des études de l'Université de Princeton (2014), de Cornell (2017) ou encore dans une enquête du *Guardian* (2017). Mais cette fois-ci, les chercheurs ont évalué la probabilité exacte d'identifier une personne à partir d'un ensemble de données dites « anonymisées ». Ils ont pour cela développé un algorithme de *machine learning*, capable d'identifier quels critères peuvent rendre une personne unique dans un groupe donné.

Selon eux, 83 % des Américains peuvent être ré-identifiés à partir des trois critères que sont le genre, la date de naissance et le code postal. Et ce chiffre monte à 99,98 % à partir de 15 critères démographiques (âge, genre, lieu, métier, etc.). « *Beaucoup de personnes vivant à New York sont des hommes et ont la trentaine. Parmi eux, beaucoup moins sont également nés le 5 janvier, conduisent une voiture de sport rouge, ont deux enfants et un chien* », explique un des chercheurs dans un communiqué de presse. Or, de telles informations sont souvent demandées par les entreprises pour

cibler leurs publicités.



Un processus de ré-identification expliqué par les chercheurs / Université catholique de Louvain et l'Imperial College de Londres

Les chercheurs ont mis en ligne le code source de leur algorithme afin de pouvoir reproduire l'expérience. Leur site permet également de calculer, grâce à ce modèle, la probabilité pour un individu d'être identifié en fonction de sa date de naissance, de son genre et de son code postal.

L'impuissance du RGPD

Afin de mieux encadrer l'utilisation des données, l'Union européenne a adopté le Règlement général européen pour la protection des données (RGPD), entré en vigueur en France le 25 mai 2018. Une solution pourtant insuffisante, selon les chercheurs : « *Une donnée anonymisée n'est plus considérée comme donnée personnelle et échappe aux régimes de protection des données comme le RGPD* ». Avant d'ajouter : « *Nos résultats remettent en question la comptabilité des standards d'anonymisation avec les lois de protection des données telles que le RGPD* ».

L'étude pointe également du doigt certaines pratiques du courtier en données Experian, qui achète et revend des données dans un but commercial. Même si l'entreprise met en vente des bases de données dites « anonymisées », celles-ci contiennent jusqu'à 248 caractéristiques par foyer, permettant donc d'identifier très facilement chaque individu. Selon les chercheurs, 120 millions d'Américains seraient concernés.

Vers plus de contrôle

Les chercheurs encouragent donc les législateurs à agir pour ne pas avoir à revivre des scandales comme celui ayant touché Facebook en 2018. À l'époque, l'entreprise *Cambridge Analytica* avait aspiré les données personnelles de 50 millions d'Américains sur le réseau social, et ainsi permis à Donald Trump de cibler ces profils dans le cadre de la dernière campagne présidentielle américaine.

Mais là où les données sont particulièrement sensibles, c'est dans le domaine de la santé, alors que plus de 26 millions de personnes ont déjà fait un test ADN en vente libre. Le secteur bancaire est également à risque, surtout depuis le lancement du Libra, la cryptomonnaie de Facebook, pour laquelle se pose la question de la délimitation entre données personnelles et données financières.

Des solutions alternatives existent, mais elles sont pour l'instant insuffisantes, rappelle le *New York Times*. Il est par exemple possible de contrôler l'accès aux données médicales sensibles, en interdisant la copie de celles-ci, ce qui constitue toutefois une barrière à la recherche scientifique. Un autre moyen pourrait être de crypter ces données, mais si le résultat final d'une étude scientifique cryptée s'avère faux, les chercheurs auront du mal à revenir à la source du problème.

Pour changer la législation, encore faut-il qu'il y ait une prise de conscience. Ce qui n'est pas exactement le cas, selon une étude de la société Norton Lifelock. Si deux tiers des Français se disent préoccupés par la protection de leurs données personnelles, 59 % seraient toutefois prêts à vendre ou à donner leurs informations de géolocalisation ou leurs historiques de recherche à des entreprises. Au nom de la gratuité et de l'amélioration du service.

Source
Futura
Fabrice Auclert
17 octobre 2019

7. Réalité augmentée : les jeux sur mobile savent tout de vous !

Devenus célèbres avec Pokemon Go, les jeux en réalité augmentée ont besoin d'une puce GPS pour permettre aux joueurs de se déplacer dans la réalité. Un média américain a voulu en savoir plus sur les données collectées... Et c'est plutôt effrayant.

Avec la sortie cet été de Wizards Unite, un jeu basé sur l'univers Harry Potter, Niantic a gagné de nouveaux joueurs utilisant ses applications de réalité augmentée qui comprennent des titres comme Pokémon Go ou Ingress. À première vue, une excellente nouvelle d'un développeur qui veut faire bouger les joueurs et qui résume sa mission en trois mots : exploration, exercice et social. Cependant, ces jeux qui rapprochent le monde réel et le monde virtuel ne cartographient pas uniquement la Terre, elle suit également à la trace ses utilisateurs.

Le site Kotaku a mené une enquête pour mieux comprendre le fonctionnement de la collecte de données. Ils ont demandé à dix joueurs européens de réclamer leurs données auprès de Niantic grâce au règlement général sur la protection des données (RGPD). Ils ont découvert des informations comme le nombre de calories brûlées pendant une session, la distance parcourue, les promotions avec lesquelles ils ont interagi, et surtout des données de localisation.

Des données permettant de connaître toutes les habitudes des joueurs

En moyenne, le jeu Wizards Unite a enregistré la localisation treize fois par minute pendant le jeu, soit le double de Pokémon Go. Pour l'un des joueurs, ils ont découvert au moins une information par heure, à toute heure du jour et de la nuit, indiquant que le jeu collecte des données même sans être ouvert !

En analysant les données d'un des joueurs, ils ont pu correctement identifier le domicile et le lieu de travail, le chemin emprunté entre les deux, leurs habitudes quotidiennes, et même qu'ils mangent régulièrement du fast food. Dans un autre cas, ils ont pu déduire des informations lorsqu'un autre utilisateur a dévié de ses activités habituelles. Il est passé à la pharmacie le matin et n'a pas utilisé l'application le soir. Ils en ont correctement déduit que lui ou un membre de sa famille était malade, ce que le joueur a confirmé, indiquant qu'il s'agissait d'un de ses enfants.

La vie privée menacée par les jeux

En révélant à ces volontaires les informations qu'ils ont pu obtenir en analysant leurs données, les employés de Kotaku ont eu des réactions quasi unanimes de surprise, les joueurs n'imaginant pas que les applications collectaient autant d'informations, et surtout qu'il était possible d'en apprendre autant sur leur vie. Certains ont indiqué avoir limité leur usage des jeux. Les joueurs en question ont pu avoir accès à des données détaillées grâce au règlement européen, mais Niantic a indiqué qu'ils ne partagent pas ces données avec des tiers. Toutes les données revendues à d'autres entreprises le sont sous forme anonymisée, des statistiques comme combien de personnes se sont rendues à tel endroit ou combien ont interagi avec un objet en jeu.

La collecte de données est une réelle invasion dans la sphère de la vie privée et il ne suffit pas d'anonymiser les données pour protéger les utilisateurs. Des chercheurs ont montré qu'il suffit de quatre localisations associées à l'heure exacte de leur relevé pour identifier un utilisateur parmi une collection de données. La collecte et la revente des données sous forme de jeux pourrait conduire à une dystopie où la vie privée a disparu.

Source
lebigdata.fr
Bastien L
11 octobre 2019

8. Les Smart TVs collectent et vendent vos données personnelles

Les Smart TVs ou télévisions connectées collectent de nombreuses données à l'insu de leurs utilisateurs. C'est ce que révèle une étude menée par les chercheurs de l'Université de Princeton…

De plus en plus d'objets connectés collectent les données personnelles de leurs utilisateurs. C'est le cas des télévisions connectées ou Smart Tvs selon une nouvelle étude publiée par la Princeton University.

Pour mener cette étude, les chercheurs Arvind Narayanan et Hooman Mohajeri Moghaddam ont laissé un robot installer automatiquement des milliers de chaînes sur leurs boîtiers TV connectées Roku et Amazon Fire TV.

Le robot a ensuite imité le comportement d'un utilisateur humain lambda, en naviguant et en visionnant différentes vidéos. Dès qu'une publicité apparaissait à l'écran, le robot a vérifié quelles données étaient collectées en arrière-plan par des trackers.

Certaines des informations aspirées ne permettaient pas d'identifier l'utilisateur. C'est le cas du type d'appareil, de la ville ou du pays où est basé l'utilisateur. En revanche, d'autres données comme le numéro de série ou le réseau WiFi peuvent être utilisées pour cerner un individu et ainsi dresser son profil complet à des fins de ciblage publicitaire. Pire encore : certaines chaînes transmettent aux trackers les adresses mail des utilisateurs et les titres des vidéos qu'ils visionnent sans chiffrement…

Les Smart TVs Roku et Amazon regorgent de trackers publicitaires

Au total, l'étude révèle que 69 % des chaînes Roku et 89 % des chaînes Amazon Fire contiennent des trackers. Certains sont bien connus, comme Google dont le service DoubleClick est présent sur 97 % des chaînes Roku, tandis que d'autres sont des entreprises inconnues au bataillon.

Il est possible de désactiver le ciblage publicitaire sur les boîtiers des deux marques, mais seul « l'identifiant publicitaire » de l'utilisateur cesse alors d'être collecté. Les autres données permettant de l'identifier sont toujours aspirées.

Comme pour beaucoup d'appareils électroniques, la collecte de données personnelles a permis de faire baisser les prix. Tout comme Facebook propose ses services gratuitement en échange de données, Roku propose ses télévisions connectées pour moins de 200 dollars en compensant par le ciblage publicitaire data-driven.

Malheureusement, de nombreux utilisateurs ignorent que leurs données sont moissonnées et vendues. C'est ce que reprochent les chercheurs de Princeton aux constructeurs. Selon eux, « le ciblage publicitaire est tout bonnement incompatible avec la confidentialité puisque les plateformes devront nécessairement se tourner vers le data mining et la personnalisation d'algorithmes pour maximiser leurs revenus »…

Source
francetvinfo.fr
Laure Narlian
30 janvier 2020

9. « La montre Apple apporte beaucoup plus d'informations sur son possesseur que le bracelet de cheville des condamnés ! », alerte le chercheur Bernard E. Harcourt

Le « business model » de l'économie numérique est basé sur le fait que nous livrons nos données personnelles volontairement et gratuitement. Comment ? Pourquoi ? Et comment reprendre la main sur notre vie privée ? Auteur d'un essai passionnant sur le sujet, Bernard E. Harcourt a accepté de répondre à nos questions.

Bernard E. Harcourt a publié « La société d'exposition » au Seuil en janvier 2020.

Dans *La société d'exposition*, un essai passionnant qu'il vient de publier, le chercheur franco-américain Bernard E. Harcourt pointe avec quelle désinvolture nous abandonnons chaque jour un peu plus notre vie privée au profit de la société numérique. Cette société de la transparence, qui repose entièrement sur les données personnelles que nous livrons avec enthousiasme à chacun de nos clics, ce professeur de droit et de philosophie politique à Columbia University lui a donné un nom : la société d'exposition, qui est aussi le titre de son ouvrage publié au Seuil.

Nous avons rencontré Bernard E. Harcourt à la mi-janvier, lors de l'un de ses passages à Paris où il est aussi directeur d'études à l'École des hautes études en sciences sociales. Dans cet entretien, il nous éclaire à la fois sur les ressorts et sur les risques de cette dangereuse divulgation de nous-mêmes.

Franceinfo Culture : Vous qualifiez la société numérique dans laquelle nous vivons de « *société d'exposition* », expression qui donne son nom à votre livre. Quelles sont ses caractéristiques ?
Bernard E. Harcourt : La caractéristique la plus importante, c'est que nous sommes amenés à divulguer volontairement toutes nos informations privées. C'est la différence avec les sociétés de contrôle antérieures. Tout se passe aujourd'hui comme si quelqu'un avait compris que pour avoir accès à nos informations privées, il fallait nous amener à les livrer volontairement, par désir et par plaisir. C'est avec notre pleine et entière participation que la circulation du pouvoir dans la société a

complètement changé. Je ne pense pas que l'on ait encore pris toute la mesure des enjeux, de ce que cela signifie pour nos vies privées, pour notre propre subjectivité et pour nos politiques. C'est ce que j'essaye d'exposer dans cet essai.

Selon vous, nous et nos pulsions narcissiques sommes le moteur de la nouvelle société numérique. Nous nous retrouvons piégés par nos propres désirs.
J'essaye de ne pas utiliser le mot narcissique d'une manière trop négative, car il s'agit plus simplement du désir d'être aimé, apprécié, populaire, des désirs que nous avons tous. La technologie fait tout pour stimuler nos désirs, avec notamment le puissant levier de la récompense. Nous pouvons mettre des selfies en ligne sur Instagram, et ensuite voir que des gens nous « aiment », nous « suivent » et aiment nos images. C'est ce sentiment de narcissisme qui fait fonctionner tout le système. Parce que pour satisfaire ce désir d'être aimé et regardé nous sommes amenés à divulguer de plus en plus de nous-mêmes, de notre personnalité, de nos images, de nos opinions et de nos goûts. Au risque d'y laisser notre liberté.

Vous dites que les traces numériques que nous laissons en permanence constituent notre double numérique, notre « *doppëlganger* ». Or, ce double est désormais selon vous plus tangible, plus fiable et plus stable que notre moi mortel, de chair et d'os.
En d'autres termes, dans notre corps de chair nous pouvons nous imaginer autres que ce que nous sommes et que ce que nous faisons. Mais avec toutes les traces numériques que nous laissons il est très difficile de ne pas connaître cette personne dans le moindre de ses actes. On peut se raconter des histoires, se dire par exemple que l'on n'aime pas lire un certain genre de littérature. Mais si on les lit, il y a une trace numérique qui montre qu'on les a lus, qu'on y est retourné et que c'est ça qu'on aime plus que toute autre littérature. Ces traces indélébiles sont interprétées comme étant plus fiables.

La surveillance de tous, partout, tout le temps, ne sert pas qu'aux services de renseignement des Etats, soulignez-vous. Nos données alimentent aussi un immense marché.
L'économie numérique est entièrement vouée à la publicité. On parle de centaines de milliards d'euros. Toutes ces données que nous divulguons ont une immense valeur parce qu'elles permettent à Google et Facebook de dire aux publicitaires vers qui diriger les informations publicitaires et de vendre chèrement ces données. Elles permettent aussi à Netflix ou Amazon de prédire nos comportements et d'influencer nos désirs avec les recommandations. Mais nos données font également fonctionner d'autres sociétés.

Donnez-nous un exemple.
Prenons l'exemple du domaine de la santé aux États-Unis. Une compagnie d'assurance, mettons United Health, reçoit toutes les informations des médecins en vue de rembourser (ou pas) les frais de santé des patients. Donc on va chez le docteur, on se croit dans le monde analogique parce que le médecin nous tâtonne et écrit quelque chose à la main, sauf que tout cela est scanné, rendu numérique et envoyé à cette société. Aux États-Unis, une loi très stricte interdit la divulgation d'informations nominatives par ce genre de société. Sauf que cette société a une succursale, Optum, qui s'occupe des big datas avec toutes ces infos des médecins. Cette succursale achète parallèlement auprès d'autres courtiers tout ce qu'elle peut comme autres datas et autres bases de données – venues de réseaux sociaux, de cartes de fidélité, de cartes de crédit, de cartes de transports etc. Ensuite, en agrégeant tout ça, cela leur permet d'en savoir plus sur moi, ma façon de vivre et mon niveau de vie. Cette grosse base de données personnelles, la société peut à la fois l'utiliser pour sa propre information – cette personne fume-t-elle, a-t-elle un mode de vie sain etc - , mais aussi la revendre très cher, par exemple à un fabricant de médicaments, à une seule condition : anonymiser les données.

« *Notre vie numérique commence étrangement à ressembler à celle d'un sujet carcéral sous surveillance électronique* », écrivez-vous. « *Pendant que certains sont forcés de porter des bracelets électroniques à la cheville, d'autres attachent lascivement leur montre Apple à leur poignet.* »
Le pire c'est que la montre Apple apporte beaucoup plus d'informations sur son possesseur que le bracelet de cheville des condamnés ! Sur les smartphones et sur les montres Apple, toutes les applications travaillent ensemble. Dès lors que vous avez Facebook, Facebook a accès à toutes les autres applications que vous utilisez. À partir de ça on peut tout savoir de vous, suivre vos moindres

faits et gestes minute par minute, en particulier avec la géolocalisation et le GPS. Or pour la plupart des applications, la géolocalisation est nécessaire. C'est effarant ce que la géolocalisation peut révéler de nous-mêmes.

Comment expliquez-vous que les révélations et les alertes répétées des lanceurs d'alerte comme Snowden et des scandales comme celui de Cambridge Analytica, ne réveillent pas les consciences ?
Parce que nous donnons clairement moins d'importance à la vie privée. Non seulement l'économie numérique a fait de nos vies privées une marchandise mais elle les a aussi privatisées. Pour avoir une vie privée, pour être plus protégés en ce qui concerne les e-mails ou les autres plateformes, il faut payer. C'est en ce sens-là que ça a été privatisé. Avant, nous considérions la vie privée comme quelque chose de nécessaire comme l'eau ou l'air. Cette mentalité a complètement basculé avec l'introduction d'un coût à la vie privée. En réalité tout le monde reste sur G-mail tout en sachant que c'est assez surveillé parce que c'est gratuit.

La plupart des gens vont vous rétorquer : « *mais moi je n'ai rien à cacher* ».
Eh bien, la plupart des gens se trompent. D'abord, ils ne comprennent pas que nous sommes devenus des marchandises. Ensuite, de n'avoir vraiment rien à cacher est un signe de privilège absolu, c'est vraiment qu'on est au plus haut de la hiérarchie. Car dès qu'on est minoritaire, qu'on n'est pas dans la norme, on est vulnérable. Je pense que cette idée qu'on n'a rien à cacher est une des choses qui nous trompent le plus. Quiconque va se retrouver dans une situation difficile sera vulnérable à travers sa présentation de lui-même sur internet. Certains pensent qu'il y a un tel volume d'informations sur internet que personne ne va retrouver quoi que ce soit les concernant. Mais avec l'accroissement des technologies, avec la reconnaissance faciale, et la puissance des ordinateurs, on peut fouiller très loin et tout retrouver.

Votre livre a été publié aux États-Unis en 2015 (sous le titre *Exposed*). Beaucoup de choses ont changé depuis, et notamment en Chine avec le programme de fichage numérique de la population qui s'est concrétisé et l'avènement d'une « *note sociale* » (véritable notation du comportement des gens) attribuée aux individus. Pensez-vous que c'est ce qui risque de nous arriver ?
Je ne connais pas assez bien la Chine, mais d'après mes recherches, je pense que c'est ce qui risque de nous arriver. La grande différence c'est qu'en Chine l'hyper centralisation fait que les différentes notes des citoyens sont agrégées dans une seule. Aujourd'hui, aux États-Unis, tout le monde a ce qu'on appelle des « credit scores », des « cotes de solvabilité » nécessaires pour acheter une maison, une voiture ou tout autre gros achat. Trois agences s'occupent de ça au États-Unis et elles ont élaboré une cote de solvabilité pour chaque Américain. Mais il existe de plus en plus d'autres cotes. On les connaît moins et on en entend moins parler mais il existe aussi des « health risk scores », des cotes de risques à la santé, d'autres sur la consommation, sur le risque de fraude, sur notre employabilité, etc. Comme nous le montrent des chercheurs aux États-Unis, nous sommes notés sur de multiples dimensions. Les Américains sont aussi notés que les Chinois sauf qu'il n'y a pas d'hyper centralisation pour l'instant.

Alors, comment lutter ? Comment reprendre le pouvoir sur nos données personnelles ?
Dans mon livre je propose plusieurs pistes. 1) Limiter notre usage, mais ça va contre tous nos désirs, c'est pour ça qu'il faut comprendre ce système. 2) Utiliser des logiciels de cryptage mais ça coûte cher et c'est compliqué. Et puis est-ce que ça va vraiment marcher contre une telle puissance technologique, quand on sait que le FBI est dans TOR (réseau informatique permettant d'anonymiser l'origine des connexions, NDLR) maintenant… 3) Aller vers un système où chacun contrôle ses données et leur éventuelle exploitation commerciale. Mais ce serait difficile parce qu'il y a de telles inégalités avec les très grandes entreprises existantes du secteur. 4) Repenser le modèle de toutes ces plateformes. En inventer de nouvelles qui soient à la fois attrayantes tout en protégeant notre vie privée. 5) Transformer les médias sociaux en associations non marchandes. Mais pour tout ça il faudrait une révolution à la fois des mentalités et de l'économie politique. Or les médias sociaux et les gouvernements ne le veulent pas parce que leur « business model » est basé sur le fait que toutes nos données sont livrées gratis.

Vous ne suggérez pas de démanteler les GAFA comme le préconise Elisabeth Warren,

candidate à l'investiture démocrate pour la présidentielle américaine. Pourquoi ?
Parce que si on les démantelait on aurait à la place et pour chacun cinq compagnies différentes. Or si la logique économique et politique qui sous-tend le fonctionnement de tout ça demeure intacte, je ne suis pas sûr que cela changerait grand-chose. Il y a certainement des problèmes de monopoles mais le démantèlement et la concurrence qui en découlerait ne changeraient rien a leur modèle de business. Je crois qu'il faut plutôt attaquer la rationalité économique qui veut que l'on cède toutes nos datas gracieusement à des sociétés privées qui les exploitent pour leur propre profit.

Mais n'est-il pas déjà trop tard ?
Parfois on a l'impression qu'il est déjà trop tard, c'est vrai. Que ce monde est trop plein de satisfactions et de plaisirs, d'émoticônes mignons et de notifications vibrionnantes, qu'on est trop distraits et trop pris dans ce jeu pour penser à des solutions. Chaque fois qu'on pense à se mobiliser, il y a déjà un autre bing, un autre ding, et on est déjà repris dans le jeu. Il me semble qu'il sera trop tard quand on ne pourra plus avoir des conversations comme la nôtre actuellement. Quand on ne sentira même plus cette gêne d'être surveillés, façonnés, quand on ne se posera plus de questions. Il me semble que tant qu'on a ce sentiment d'être sur une dérive, il y a de l'espoir, ce n'est pas trop tard.