Données personnelles et internet: faut-il être paranoïaque?

Nicolas Martignoni, directeur du Centre fri-tic, centre de compétences pour les technologies de l'information et de la communication dans l'éducation du Canton de Fribourg

En 2012, un client de Minneapolis du grand distributeur américain Target (le pendant de la Migros ou de la Coop) a souhaité rencontrer le gérant du magasin local. Il lui a demandé des explications concernant sa fille, étudiante au lycée, qui recevait du magasin des publicités et des bons d'achat pour des vêtements de grossesse, des berceaux, des habits de bébé, articles donnant à penser qu'elle était enceinte. Le père de la jeune fille demanda au gérant si le magasin voulait encourager sa fille à tomber enceinte. Stupéfait, le gérant s'excusa en déclarant n'avoir aucune idée de la raison de ces promotions.

Rentré à la maison, le papa en discuta avec sa fille et découvrit qu'elle attendait effectivement un enfant. Target avait utilisé des techniques complexes d'analyse prédictive, basées sur le comportement et les habitudes d'achat de la jeune fille, pour déterminer qu'il y avait une probabilité élevée qu'elle attende un bébé, et lui fournissait donc des publicités ciblées[1].

Cette anecdote réelle nous montre l'actualité de ce thème, et nous incite à réfléchir sur la nécessité pour notre société et notre école d'agir face à cette situation, et à développer quelques pistes de réflexion.

Données personnelles: de quoi parle-t-on?

La loi fédérale sur la protection des données définit les données personnelles comme: "toutes les informations qui se rapportent à une personne identifiée ou identifiable"[2].

Au premier abord, on se dit alors que les données personnelles sont des informations telles que le prénom, le nom, l'adresse, le numéro de téléphone et d'autres données similaires. Pas de quoi fouetter un chat. Mais la suite est intéressante.

"Une personne est identifiable lorsque, par corrélation indirecte d'informations tirées des circonstances ou du contexte, on peut l'identifier (…)"[3].

Les techniques d'analyse statistique et les capacités de calcul des ordinateurs actuels permettent dorénavant cette *corrélation indirecte d'informations*, puisées à de nombreuses sources: l'utilisation de réseaux sociaux (Facebook, Twitter) et de services divers (stockage de fichiers avec Dropbox, courriel avec Gmail, vidéo sur Youtube, guidage GPS), l'emploi de moteurs de recherche (Google), mais aussi les cartes de fidélisation (Supercard, Cumulus, Manor, Club Fnac) et les objets dits intelligents, dotés de capteurs miniaturisés, tels les capteurs d'activité. Cette masse d'informations, c'est ce que l'on appelle aujourd'hui les *big data* – un ensemble d'informations si volumineux qu'il est difficile de les exploiter avec des outils classiques.

Ainsi, par exemple, les habitudes d'achat d'une personne, les titres et contenus de ses courriels, les sites web qu'elle visite, les centres d'intérêt de ses recherches, les lieux qu'elle fréquente, les produits qu'elle consomme, les informations et messages qu'elle échange sur les réseaux sociaux, sont désormais des données personnelles.

De telles sources de données sont également présentes dans le domaine de l'éducation. Les plateformes d'apprentissages ou celles fournissant des MOOCs détiennent une masse énorme d'informations sur les étudiants et les enseignant-e-s, pouvant être exploitées et traitées de la même manière, à l'aide d'outils adéquats. Si ces plateformes sont en mains privées, qu'advient-il de ces données personnelles?

Les exemples ci-dessus montrent pourquoi la question des données personnelles est devenue aujourd'hui importante.

Avant l'explosion de l'utilisation du web, au milieu des années 1990, il était coûteux et difficile – voire impossible – de collecter de telles données. Il y a encore une quinzaine d'années, l'exploitation et le traitement des informations générées au fil du temps par les personnes durant leur vie n'étaient pas praticables, faute de moyens de calcul suffisants. C'est donc l'hyper-connectivité et les progrès techniques de l'informatique qui ont changé radicalement la donne, et la question de la protection des données est devenue un sujet de préoccupation important de notre XXIème siècle.

"Internet nous a ouvert le monde, mais il a également ouvert chacun de nous au monde"[4]. Le prix que l'on nous demande pour accéder à cette hyper-connectivité est de plus en plus celui de notre sphère privée; chaque achat, chaque clic de souris laisse des traces de nos données personnelles.

Mais ne soyons pas paranoïaques: ce n'est pas le partage d'informations qui est mauvais par essence. Si je sais lesquelles de mes données sont partagées et si j'ai donné mon accord de façon explicite – bien entendu –, cela peut m'aider pour obtenir par exemple des conseils sur un livre à lire ou un film que j'aimerais voir. Mais si je ne suis pas au courant et qu'on ne m'a même pas demandé mon accord, il y a un problème.

Note

1
Samuel Greengard, *Advertising Gets Personal*, Communications of the ACM, August 2012, Vol. 55, No. 8.

2
Loi fédérale sur la protection des données (LPD), art. 3, https://www.admin.ch/opc/fr/classified-compilation/19920153/index.html#a3

3
Message du 23 mars 1998 concernant la loi fédérale sur la protection des données, http://www.edoeb.admin.ch/org/00129/index.html?download=NHzLpZeg7t,lnp6I0NTU042l2Z6ln1ae2IZn4Z2qZpnO2Yuq2Z6gpJCDdYN5fmym162epYbg2c_JjKbNoKSn6A--&lang=fr

4
Gary Kovacs, *Tracking our online trackers*, http://www.ted.com/talks/gary_kovacs_tracking_the_trackers

La collecte des données est devenue systématique

Internet a été conçu pour résister à une attaque nucléaire. À ses débuts, on avait l'habitude de le représenter comme un filet ou un entrelacement de filets de pêche. Le réseau devait continuer à fonctionner, même si plusieurs centres de données étaient rasés par un bombardement. Il devait donc être décentralisé. À ses débuts, le web reflétait cette organisation: c'était un ensemble de pages liées entre elles de manière chaotique à l'aide de liens hypertextes.

Peu à peu, le web est devenu différent, et on a assisté à une centralisation; certains sites web sont devenus incontournables: Google, Facebook, Twitter, Amazon, WhatsApp pour ne citer que certains d'entre eux. Ces sites ont des quasi-monopoles, ce qui a pour conséquence que le web se présente aujourd'hui plutôt comme une toile d'araignée ou un ensemble de toiles d'araignées, avec des points centraux. Le problème avec la centralisation, c'est qu'elle nous rend plus faciles à pister, grâce à ces points centraux vers lesquels convergent les informations, et qui attirent des individus pas toujours recommandables.

Les raisons pour lesquelles la collecte des données est devenue systématique sont multiples et dépendent de l'entité qui collecte les données.

Ce n'est pas parce que l'on cache quelque chose que l'on a quelque chose à cacher

Depuis la nuit des temps, les pays du monde entier collectent des données sur leurs citoyens et les personnes qui résident chez eux. Dans les pays totalitaires, la raison en est simple: il faut contrôler les personnes, et de préférence avoir un contrôle absolu sur le peuple. Il est bien connu que Louis XIV interceptait et lisait le courrier de suspects ou personnes désignées comme tels[5]. De même, le décryptage des lettres chiffrées était déjà pratiqué, dès le règne de Louis XIII[6]. Dans notre monde moderne, les pays totalitaires détournent internet pour l'utiliser à la surveillance de tout un chacun. Toutes les transmissions internet sont passées au peigne-fin. Cela permet en outre d'effectuer une censure plus ou moins efficace. Dans les pays plus démocratiques, l'objectif annoncé est de prévenir les attaques terroristes et d'améliorer la sécurité des citoyens honnêtes. C'est pourquoi on assiste maintenant à une volonté généralisée d'obtenir les bases légales jugées nécessaires pour pratiquer une surveillance de masse, y compris des gens qui n'ont rien à se reprocher. Les États-Unis ont déjà une expérience assez longue de cette pratique, légalisée par le *Patriot Act*[7].

Malheureusement, le bilan de cette surveillance généralisée est mitigé: depuis 2001, elle n'a pas permis aux États-Unis de trouver des informations exploitables autres que celles que les forces de l'ordre avaient déjà obtenues par d'autres moyens légaux[8]. De plus, cette surveillance n'a pas réussi à empêcher l'attentat de Boston en 2013. L'Histoire nous enseigne en outre que lorsque des pouvoirs trop importants sont donnés, les hommes en abusent. En Suisse, on se souviendra notamment de l'Affaire des fiches de 1989[9].

Pire encore, les citoyens qui veulent protéger leur sphère privée sont suspectés d'être des criminels, comme le montrent les récentes déclarations du ministre américain de la justice Eric Holder ou celles du chef enquêteur de la police de Chicago John Escalante, pour lequel, en raison de sa grande sécurité et de la volonté affichée par Apple de protéger la sphère privée de ses consommateurs, l'iPhone est "le téléphone du pédophile"[10].

L'État ne doit pas être paranoïaque lui non plus. Ce n'est pas parce que l'on cache quelque chose que l'on a quelque chose à cacher. Comme le disait Benjamin Franklin en 1755 déjà: "Ceux qui veulent renoncer aux libertés fondamentales pour obtenir une petite sécurité provisoire ne méritent ni liberté, ni sécurité"[11].

Bien entendu, les gouvernements doivent avoir accès aux données personnelles des malfaiteurs et le pouvoir d'y accéder; ce pouvoir doit cependant être strictement encadré et protéger le droit à la vie privée des citoyens honnêtes, ce que la surveillance de masse ne respecte pas.

Si c'est gratuit, c'est vous le produit!

Les motivations des entreprises privées pour collecter nos données personnelles sont différentes, mais tout aussi claires: en un mot, l'argent.

En 2010, *The Economist* estimait le marché des données à plus de 100 milliards de dollars[12]. Les revenus de ce marché sont essentiellement des revenus publicitaires d'une part, et d'autre part les bénéfices supplémentaires de la grande distribution, gagnés grâce à un meilleur ciblage des consommateurs.

"À l'avenir les données seront une ressource de base, comme le gaz, l'essence et l'électricité […]. Avec les données, nous pouvons innover énormément. On peut mieux comprendre les habitudes de consommation, et

Note

5
Duc de Saint-Simon, *Mémoires*, volume 24, Imprimerie Schneider et Langrand, Paris, 1840.

6
Karl Maria Michael de Leeuw, Jan Bergstra (ed.), *The History of Information Security: A Comprehensive Handbook*, Elsevier, Amsterdam, 2007.

7
Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001, http://www.gpo.gov/fdsys/pkg/PLAW-107publ56/html/PLAW-107publ56.htm

8
https://www.newamerica.org/international-security/do-nsas-bulk-surveillance-programs-stop-terrorists/

9
D'autres exemples sont plus anciens, par exemple dans l'Antiquité grecque avec Solon et surtout Alcibiade.

10
"Apple will become the phone of choice for the pedophile", http://www.washingtonpost.com/business/technology/2014/09/25/68c4e08e-4344-11e4-9a15-137aa0153527_story.html

11
"Those who would give up essential Liberty, to purchase a little temporary Safety, deserve neither Liberty nor Safety.", *Lettre au gouverneur de la Pennsylvanie (11 novembre 1755)*, Benjamin Franklin, http://franklinpapers.org/franklin/framedVolumes.jsp?vol=6&page=238a

12
"This industry [of information management] is estimated to be worth more than $100 billion and growing at almost 10% a year, roughly twice as fast as the software business as a whole.", *Data, data everywhere*, The Economist, 27 février 2010, http://www.economist.com/node/15557443.

mieux appréhender l'économie en général. […] On calcule automatiquement le crédit possible que l'on peut allouer à un utilisateur, sans aucune étude préalable, aucune intervention humaine"[13].

Vous n'êtes pas convaincus? Voici alors d'autres chiffres. Le rapport financier de Google pour l'année 2014[14] indique un revenu publicitaire de 45 milliards de dollars. Celui de Facebook[15] indique pour cette même rubrique 11.5 milliards de dollars. Vous pensez que Google est une entreprise fournissant gratuitement un moteur de recherche performant et d'autres services très utiles sur internet? Vous avez tort. Google est une entreprise publicitaire: en 2014, 89.5% de son revenu est produit par la publicité. Vous pensez, comme Mark Zuckerberg tente de nous le faire croire, que Facebook est une entreprise philanthropique mettant à disposition gratuitement un réseau social performant? Là encore, vous avez tort: les rentrées publicitaires formaient en 2014 plus de 92% de son chiffre d'affaires. Internet n'est pas le pays des bisounours, c'est le monde impitoyable de la finance. Quand vous utilisez les services de Google, Facebook, Twitter et autres, vous fournissez, de votre plein gré ou non, une masse d'informations sur vos comportements. Ces informations sont analysées et vendues très cher à la grande distribution afin d'optimiser leurs profits. Nos données sont le prix que l'on paie pour les services obtenus. Si c'est gratuit, c'est vous le produit!

Bien sûr, si vous avez donné votre accord explicite et savez quelles données vous fournissez, tout cela est parfaitement acceptable. Mais est-ce vraiment toujours le cas?

Depuis quelques années, le web lui aussi a bien changé. Les pages web ne sont plus constituées d'éléments hébergés sur un même site web. Elles comprennent désormais également des éléments provenant de nombreux sites web externes. Ces éléments, le plus souvent de petits programmes écrits en Javascript, recueillent des informations sur vos habitudes de navigation, sans que vous vous en aperceviez. L'observation de cette pratique est édifiante.

À l'aide d'outils appropriés, il est possible de se rendre compte de la transmission de données qui nous concernent lorsque nous naviguons sur le web. L'outil *Lightbeam*[16], développé par la fondation Mozilla, permet de visualiser et de mettre en évidence où vont vos données sur le web. Il montre les sites que vous visitez, et ceux qui pratiquent l'analyse comportementale de vos habitudes, sans rien vous demander. Par exemple, vous n'avez pas besoin d'avoir un compte Facebook pour que Facebook collecte vos données, de manière illégale[17].

Le résultat est impressionnant: lors d'une simple session de quelques minutes, durant laquelle j'ai visité moins d'une dizaine de sites web[18], j'ai constaté que près de 120 autres sites me pistent, sans que je les aie visités et sans que j'aie donné mon accord. Une seule visite à la page d'accueil du *Corriere del Ticino* transmet des informations à plus de 30 autres sites!

Pourquoi ces mouchards? Parce qu'ils permettent d'en apprendre tellement sur nous qu'ils peuvent connaître nos envies et nos besoins, et donc modifier notre consommation.

Par exemple, lorsqu'une femme achète des compléments vitaminés, de la lotion pour le corps, du désinfectant pour les mains et un grand sac à main, il y a une probabilité extrêmement élevée pour qu'elle soit enceinte. Les techniques d'analyse sont si sophistiquées qu'il est même possible d'estimer la date de l'accouchement dans un intervalle de quelques semaines[19]. Les femmes enceintes sont par ailleurs très intéressantes pour les publicitaires, car elles dépensent en moyenne pour les préparatifs du futur bébé 15 fois plus qu'un autre consommateur[20].

Ces informations ont donc de la valeur pour la grande distribution, ce qui explique les montants faramineux mentionnés plus tôt. C'est ainsi que Facebook et Google engrangent leurs importants revenus.

On peut sans difficulté imaginer que de telles techniques de profilage permettent de détecter si une personne est atteinte d'une pathologie grave, par exemple le VIH, avec toutes les conséquences possibles. Les compagnies d'assurances maladie sont certainement intéressées par des informations de ce type, susceptibles de diminuer leurs mauvais risques.

Dans le domaine de l'éducation, des entreprises commerciales fournissent, surtout aux écoles du degré tertiaire, des plateformes d'apprentissage ou, plus récemment, permettant de proposer des MOOCs. Ces dernières années, Blackboard a par exemple investi dans l'assistance et la fourniture de plateformes Open Source comme Moodle ou Sakai[21]. Il est vraisemblable que ces acquisitions aient pour objectif l'exploitation des informations et métadonnées que les étudiant-e-s laissent sur ces plateformes, afin de maximiser leur modèle commercial.

Note

13
James Chu, responsable de la gouvernance internationale chez Alibaba (Chine), *Interview diffusée sur la RTS, 22 juin 2015*, http://download-audio.rts.ch/la-1ere/programmes/le-journal-du-matin/2015/le-journal-du-matin_20150622_standard_1er-developpement_9c5f35b5-c8f7-4359-afe4-3be2ec956155-128k.mp3

14
Rapport financier de Google 2014, p. 23, 6 février 2015. http://www.sec.gov/Archives/edgar/data/1288776/000128877615000008/goog20141231l0-k.htm#sA63A6AA08C0C233E7C90A6358CB77158

15
Rapport financier de Facebook 2014, p. 43, 29 janvier 2015. http://www.sec.gov/Archives/edgar/data/1326801/000132680115000006/fb-12312014x10k.htm#sCB17083EFDC66A4C66A9AA564DC1F226

16
Lightbeam, un coup de projecteur sur ceux qui vous surveillent, https://www.mozilla.org/fr/lightbeam. Lightbeam est un module complémentaire à installer dans le navigateur Firefox.

17
http://www.theguardian.com/technology/2015/mar/31/facebook-tracks-all-visitors-breaching-eu-law-report

18
Sites visités le 13 juillet 2015 (4 journaux quotidiens, 2 gros distributeurs, 1 magasin en ligne): gdp.ch, cdt.ch, repubblica.it, corriere.it, migros.ch, coop.ch, leshop.ch.

19
Samuel Greengard, *op. cit.*

20
http://www.theguardian.com/world/2014/may/11/anonymous-web-nsa-trail-janet-vertesi

21
http://www.blackboard.com/news-and-events/press-releases.aspx?releaseid=1676738

Les liens entre la surveillance effectuée par les États et la collecte des données par des entreprises privées sont par ailleurs étranges. Connaissant la plus-value d'une femme enceinte pour les distributeurs, une professeure de sociologie de l'université de Princeton a cherché à cacher sa grossesse des entreprises de marketing. Pour éviter d'utiliser sa carte de crédit, elle a acheté avec de l'argent liquide des bons d'achat Amazon pour une valeur de 500 dollars. Cette simple transaction a déclenché une alerte auprès des organes étatiques de surveillance, sous prétexte que de telles pratiques sont celles de blanchisseurs d'argent[22]. Une situation vraiment troublante: en prenant de façon tout à fait justifiée des mesures pour diminuer la collecte de ses données par des entreprises, elle a déclenché sa propre surveillance par les services de l'État.

Il est tout à fait inadmissible qu'une activité légale – la protection de sa sphère privée – suscite la suspicion et déclenche une surveillance étatique. Il faut espérer qu'en Suisse, nous n'en soyons pas encore là.

Autre élément à considérer: la surveillance est un marché juteux. Suite au piratage en juillet dernier de l'entreprise italienne Hacking Team, des fuites ont montré que pour certaines entreprises, il n'est pas tabou de faire du profit en vendant des procédés illégaux de surveillance, tels que des logiciels espions, des virus, des chevaux de Troie ou des failles de sécurité découvertes secrètement. Ces entreprises ne sont pas regardantes vis-à-vis de leurs clients, parmi lesquels on trouve des États répressifs, tels le Soudan, l'Ouzbékistan et l'Arabie saoudite, mais aussi des organismes plus honorables, comme la police cantonale zurichoise[23].

Ce n'est pas l'analyse et l'exploitation des données qui est problématique, mais le manque d'encadrement

La collecte et le traitement d'informations personnelles n'ont pas que des côtés obscurs. Ils peuvent rendre d'importants services. À titre personnel, en analysant mes goûts et affinités, ils aident à choisir judicieusement un article à acquérir ou une émission à voir.

Dans le domaine de la santé, ils permettent à Google de suivre quasiment en temps réel la propagation mondiale d'épidémies, grâce à l'analyse des recherches effectuées par les internautes, plus vite que l'OMS[24].

En circulation routière, grâce aux *big data* récoltés au moyen des appareils GPS, on comprend mieux la formation des bouchons, ce qui permet de développer des algorithmes pour faire des prévisions fiables de l'engorgement du trafic[25], d'optimiser la circulation dans les grandes agglomérations et de diminuer ainsi la production de gaz carbonique.

De plus, les nouvelles technologies et l'analyse des données modifient profondément la vie des personnes handicapées, en leur permettant de se déplacer plus facilement dans notre monde, en leur donnant plus d'autonomie[26]. Grâce à ses nombreux capteurs – caméra, microphone, puce GPS, gyroscopes – un smartphone est capable d'analyser les données qu'il capte et de les comparer avec des informations disponibles récoltées grâce au *big data*, afin par exemple de guider une personne aveugle dans une ville, de reconnaître un bâtiment, un visage[27] ou même une émotion sur un visage, de lire à haute voix les panneaux d'information rencontrés et de les traduire, tout cela en temps réel.

Ces exemples d'utilisation utile et raisonnable d'informations récoltées via les technologies modernes nous montrent qu'il est important de ne pas en faire une obsession; ce n'est pas tant l'analyse et l'exploitation des données qui est problématique, mais le manque d'encadrement. C'est avant tout le fait que nous, les citoyens, nous ne soyons pas au courant de la collecte de nos données, que nous ne sachions pas lesquelles sont collectées et que nous n'ayons pas explicitement donné notre autorisation de les récolter.

Que peut-on faire?

"Imaginez que nous n'ayons pas à nous préoccuper de confidentialité, que nous ayons de solides garanties que nos inventions ne soient pas utilisées contre nous"[28].

J'ai pris conscience récemment que depuis trop longtemps, je regarde chaque nouvelle innovation technologique avec un sentiment de prudence et d'appréhension, alors qu'elle devrait avant tout m'émerveiller. Cet état d'esprit suspicieux m'est peu à peu devenu naturel en réaction à la difficulté de notre monde à gérer ces questions de données personnelles. Alors que faire pour changer cela?

En tant que citoyen, notre rôle est d'être vigilant, sans paniquer, ni sombrer dans la paranoïa. La question est certes importante et il est facile de verser dans le sensationnalisme; et certains médias cèdent trop facilement à cette tentation[29].

Bien entendu, en attendant que la législation évolue

Note

22
http://www.theguardian.com/world/2014/may/11/anonymous-web-nsa-trail-janet-vertesi

23
http://www.kapo.zh.ch/internet/sicherheitsdirektion/kapo/de/aktuell/medienmitteilungen/2015_07/1507071c.html

24
https://www.google.org/flutrends/ch/

25
http://www.lemonde.fr/technologies/article/2012/05/11/mobiles-facebook-gps-vos-donnees-valent-de-l-or_1699424_651865.html

26
Voir les travaux de Robin Christopherson, http://www.abilitynet.org.uk/robinchristopherson

27
Par exemple au moyen de DeepFace, https://research.facebook.com/publications/480567225376225/deepface-closing-the-gap-to-human-level-performance-in-face-verification

28
"Imagine if we didn't have to worry about privacy, if we had strong guarantees that our inventions wouldn't immediately be used against us", Maciej Cegłowski, http://idlewords.com/bt14.htm

29
https://www.techn0polis.net/2015/01/03/crypto-on-est-fichus-oupas

 Orlando Brunner
2° anno di Grafica – CSIA

pour une meilleure protection, on peut déjà se protéger à l'aide de logiciels adéquats. J'ai parlé plus haut du module complémentaire *Lightbeam*. D'autres outils de ce type permettent de contrôler la diffusion des informations récoltées par les mouchards. J'utilise *Ghostery*[30].

"Cet outil vous indique toutes les sociétés qui vous surveillent lorsque vous vous rendez sur un site Web. *Ghostery* vous permet d'en savoir plus sur ces sociétés et sur le type de données qu'elles recueillent. Cette application vous permet même de les empêcher de recueillir des données si vous le souhaitez"[31].

Après avoir installé ce module dans mon navigateur et activé la protection, plus aucun site tiers n'a accès à mes données de navigation sans que je ne l'accepte explicitement. Je contrôle ainsi mieux ce que je veux diffuser. *Ghostery* fonctionne avec tous les navigateurs actuels, quelle que soit votre plateforme.

Note

30
Téléchargeable à l'adresse https://apps.ghostery.com/fr/home

31
https://apps.ghostery.com/fr/faq#q1-general

32
"(…) leadership needs to recognize that current advertising practices that enable "free" content are in direct conflict with security, privacy, stability, and performance concerns", http://monica-at-mozilla.blogspot.ch/2015/05/tracking-protection-for-firefox-at-web.html

Nous pouvons aussi, grâce à notre prise de conscience de la situation, avoir une influence sur nos élus, et faire en sorte de ne pas lâcher face aux intérêts commerciaux, dont les objectifs sont en contradiction avec notre besoin de contrôler où vont nos données personnelles. Des pressions sont faites pour entraver le développement des logiciels permettant ce contrôle, comme *Ghostery* ou *Lightbeam*. Ainsi, le développement de *Lightbeam* a été stoppé par Firefox. L'ingénieure responsable de ce développement a alors quitté l'entreprise[32].

Finalement, nous pouvons aussi demander à nos élus de défendre notre liberté démocratique fondamentale à la protection de la vie privée, en s'opposant à la légalisation de la surveillance de masse.

La législation suisse en matière de protection des données nous protège bien. Il y reste cependant des zones d'ombre, principalement en lien avec internet. L'État doit prendre le problème en main et compléter cette régulation. Il ne s'agit pas de tout interdire, mais d'offrir une réponse à certaines questions, par exemple:

– est-il normal que la collecte et le stockage permanent de n'importe quelles données issues de l'analyse comportementale sur le web soient autorisés, sans le consentement des personnes concernées, alors même que ces données sont issues de la "corrélation indirecte d'informations tirées des circonstances ou du contexte" citée dans la législation? (on pourrait imaginer que la loi dresse une liste de ce qui n'est pas permis, et exige que les données autorisées soient détruites au bout d'un certain temps);
– est-il normal que les entreprises puissent partager ces données avec d'autres entités, sans aucune limite, également lors d'une faillite, d'un rachat d'entreprise? (on pourrait imaginer que la loi exige que ces données ne soient pas transférables, sauf accord exprès des personnes concernées);
– est-il normal qu'il soit si difficile d'obtenir les données enregistrées à son propre sujet par des entreprises? (on pourrait imaginer que la loi exige que les entreprises fournissent systématiquement un lien permettant de télécharger ces données facilement);
– est-il nécessaire d'autoriser la surveillance de masse des citoyens, sans égard pour la présomption d'innocence? (on pourrait imaginer qu'il est normal pour un citoyen d'avoir son jardin secret sans être surveillé comme un criminel).

En tant qu'enseignant-e-s et parents, nous avons le devoir de former nos enfants à la problématique de l'exploitation des données personnelles, et à les protéger.

À l'heure du *cloud computing*, nous devons nous assurer que les plateformes, environnements d'apprentissage, moyens d'enseignement numériques et autres outils en ligne que nous mettons à disposition des élèves et des enseignant-e-s respectent la législation en matière de protection des données, surtout si ces outils sont fournis par des prestataires privés.

L'école doit mieux sensibiliser les élèves à la valeur des informations qu'ils laissent sur le web et plus généralement à l'éducation aux médias. On sait que la presque totalité des élèves utilisent les technologies et les nouveaux médias[33], la plupart avec une bonne habileté technique. Mais leur esprit critique et leur capacité à les utiliser de manière raisonnée doivent être développés. Le Plan d'études romand (PER) et le Lehrplan 21 (LP21) mentionnent ces compétences à acquérir. Il est toutefois nécessaire de sensibiliser les enseignant-e-s, de leur fournir de la formation, des moyens et du temps pour leur permettre d'aborder ces questions de manière adéquate.

Paranoïaque? Non! Vigilant? Oui!

La surveillance et la collecte des données sont en train de transformer le web, de façon peu réjouissante. Mais ce n'est pas une raison pour être paranoïaque. En revanche, il est important d'être et de rester vigilant pour appréhender les développements et l'évolution des technologies dans ce domaine.

Je ne sais pas comment infléchir la tendance actuelle à négliger notre sphère privée. Mais je sais qu'une prise de conscience est nécessaire, afin d'éviter que notre monde ne se transforme peu à peu en un simple réservoir de consommateurs et de citoyens lambda.

Note

33
Daniel Süss, Gregor Waller. *Étude James 2014*, http://psychologie.zhaw.ch/de/psychologie/forschung/medienpsychologie/mediennutzung/james.html