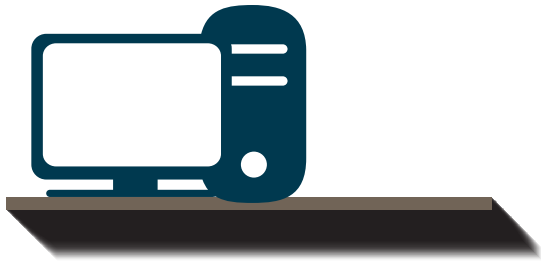
Collection “ **Au Quotidien** ”

La protection des données

La liberté sur écoute ?

Cpcp



INFOS

Toutes nos publications sont disponibles gratuitement :

- En téléchargement, depuis l'adresse internet de notre ASBL :

  www.cpcp.be/etudes-et-prospectives

- En version papier, vous pouvez les consulter dans notre Centre d'Archives et de Documentation situé :

  Rue des Deux Églises, 45 - 1000 Bruxelles
  T : **02/238 01 27 -** M : **info@cpcp.be**

INTRODUCTION

Gérer son compte en banque, lire la presse, communiquer à travers les réseaux sociaux, réserver un hôtel, acheter un ticket de train, retrouver son chemin grâce à une carte sur son smartphone… nous utilisons aujourd'hui Internet pour de nombreux aspects de nos vies. Et c'est terriblement pratique !

Nous le faisons sans trop y penser, cela fait partie de la vie de tous les jours. Et pourtant, malgré une apparente gratuité, nous payons le prix de ces services. Entre collecte, vente et exploitation de nos données personnelles, nous donnons graduellement accès à une mine d'informations aux propriétaires de ces sites et applications. Comment cela fonctionne-t-il ? Quels types d'informations sont collectés ? À quelles fins ? Quelles implications cela représente-t-il pour notre vie privée ? Avons-nous les moyens de la protéger ? Les questions sont nombreuses et la technicité des solutions proposées demeure un obstacle pour beaucoup de personnes.

I. COMMENT ÇA MARCHE ?

Les sites et services que nous utilisons sont, pour la plupart, mis gratuitement à notre disposition sur Internet. Mais ces services engagent des frais pour la création de leur site, son hébergement, sa maintenance, etc. En grandissant, ils commencent également à employer du personnel. Tout cela a un coût. Pour y faire face et même devenir lucratifs, ces services ont donc dû trouver des sources de revenus. Prenons l'exemple le plus emblématique, celui de Facebook, qui promet sur sa page d'accueil que « C'est gratuit, et ça le restera toujours. ». Le réseau social a permis à des marques de faire apparaître leurs publicités sur les fils d'actualités de ses utilisateurs. De fil en aiguille, Facebook a vendu à ces marques de plus en plus d'informations sur les préférences de ses membres afin que la publicité puisse être ajustée en fonction de leurs goûts. Les données personnelles sont devenues des « marchandises » qui se vendent à prix d'or car elles permettent au marketing d'atteindre un niveau de précision encore inégalé. On appelle ce procédé le marketing direct.

« En utilisant ce site, vous acceptez l'utilisation des cookies pour améliorer votre navigation. » Vous avez certainement déjà vu cette phrase lors de vos navigations sur Internet. Les cookies sont une technologie très largement utilisée permettant d'enregistrer les données de navigation d'un internaute (quelle page il visite, à quelle heure, à partir de quel ordinateur, etc.). Ce petit fichier stocké sur votre ordinateur retient aussi vos choix de langue, vos identifiants de connexion, etc., et les transmet au serveur lorsque c'est nécessaire. Le fonctionnement de certains sites s'en trouve ainsi facilité. Ce ne sont pas des logiciels espions mais ils emmagasinent néanmoins de nombreuses informations. La plupart des navigateurs modernes permettent aux usagers de désactiver les cookies ou de limiter la durée du stockage des informations que ces fichiers contiennent. Cependant, la maîtrise de ces paramètres demande des connaissances encore trop peu répandues chez les utilisateurs.[1]

[1] M. Paquay, « Cookies : la vie privée des internautes n'est pas assez respectée », *RTBF Info,* 10 avril 2015, http://www.rtbf.be/info/societe/detail_cookies-la-vie-privee-des-internautes-n-est-pas-assez-respectee?id=8952503, consulté le 10 avril 2015.

II. MA VIE PRIVÉE DANS UN MOUCHARD DE POCHE

Ces informations, nous les donnons parfois volontairement, parfois de manière inconsciente. Reprenons l'exemple de Facebook. Bien sûr, il y a déjà les informations de base requises pour créer un profil sur le site. Mais ces informations en disent finalement bien peu sur nous. Elles servent uniquement à dresser un portrait factuel (nom, âge, genre, etc.) accessible à tous. Ensuite, au cours de notre navigation, nous cliquons sur certains liens qui nous intéressent plus que d'autres. Toutes ces actions seront soigneusement enregistrées afin d'établir un profil très pointu de nos goûts et préférences (politiques, cinématographiques, musicaux, vestimentaires, etc.). Même une fois la fenêtre du réseau social fermée, nos déambulations sur Internet continuent d'être répertoriées et analysées.[2] Car Facebook n'est malheureusement pas le seul à être friand d'informations personnelles : Google, Yahoo !, Amazon et leurs applications et services tels que Youtube, Gmail, Google Maps[3] sont connus pour leur politique de confidentialité peu regardante en matière de vie privée.

> *« Il suffit en réalité d'un clic, d'un like, d'une recherche Google pour connaître les endroits que nous fréquentons, les personnes que nous appelons, et même les questions que nous n'osons poser qu'à Google, discrètement. »*

Les applications mobiles ne sont pas en reste. (Attention, néologismes barbares à venir.) Se *foursquarer* en arrivant à un endroit que vous aimez pour le renseigner à vos amis, choisir un restaurant grâce aux avis des autres usagers de TripAdvisor, exprimer ses centres d'intérêt sur Pinterest et y puiser des idées, *liker* des articles politiques sur Facebook, *follower* des personnes ou des associations sur Twitter pour suivre leur actualité, trouver des personnes qui correspondent à vos critères amoureux grâce à Tinder, etc. Il existe aujourd'hui une foultitude d'applications qui nous rendent service au quo-

---

2 « Vie privée : même quand vous êtes déconnecté, Facebook peut vous traquer », *L'Express*, 11 avril 2015, http://lexpansion.lexpress.fr/high-tech/vie-privee-meme-quand-vous-etes-deconnecte-facebook-peut-vous-traquer_1670230.html, consulté le 13 avril 2015.

3 *Dégooglisons Internet*, http://degooglisons-internet.org, consulté le 7 avril 2015.

tidien, et via lesquelles nous révélons volontairement nos goûts, préférences, recherches, etc. De plus, la plupart de ces applications demandent, pour leur bon fonctionnement, à avoir accès à notre position géographique. Ce système de géolocalisation aide à récolter encore de nouvelles informations sur nos faits et gestes.

Si nous ne sommes pas tous accros à nos applications mobiles, il suffit en réalité d'un clic, d'un like, d'une recherche Google, d'une connexion WiFi, voire même d'un simple appel pour que notre téléphone se connecte aux serveurs ou aux réseaux locaux, permettant ainsi de nous localiser très aisément, et donc de connaître les endroits que nous fréquentons, les personnes que nous appelons, et même les questions que nous n'osons poser qu'à Google, discrètement.[4] Et cela, malgré nous.

Les objets eux-mêmes sont de plus en plus connectés ! L'abonnement de transport en commun que vous scannez en montant dans le bus, le tram ou le métro révèle vos trajets et laisse deviner vos activités. La « smart TV » de Samsung change de chaîne quand elle reconnaît votre voix, mais enregistre et transmet les conversations qu'elle « entend » si elle est mal paramétrée.[5] Une nouvelle balance calcule instantanément votre poids, masse corporelle et autres données ; elle vous reconnaît d'une pesée à l'autre et vous envoie automatiquement le graphique de l'évolution de votre poids sur votre ordinateur. Difficile aujourd'hui de ne laisser filtrer aucune information sur nous-même, si ce n'est en restant éloigné de la technologie (ordinateur, téléphone, télévision et balance incluse !) Le tout dans l'optique de collecter toujours plus d'informations à marchander.

---

4 Par exemple, en fonction des recherches effectuées sur son moteur de recherche, on estime que Google pourra détecter le début d'une épidémie comme la grippe avant même les autorités sanitaires publiques. http://www.slate.fr/story/36851/vie-privee-google-utile

5 M. Rundle, « Samsung Smart TV Voice Recognition Privacy Policy Reads Like George Orwell's '1984' », *The Huffington Post*, 9 février 2015, http://www.huffingtonpost.co.uk/2015/02/09/samsung-smart-tv-privacy-1984_n_6642934.html, consulté le 1er avril 2015. Il est normal qu'un appareil basé sur la reconnaissance vocale capte une voix et envoie systématiquement les données enregistrées pour analyse afin de savoir quel ordre exécuter. Cependant, si les informations sont envoyées à un tiers pour analyse, nous ne savons pas de qui il s'agit. Toutefois, il faut mentionner que Samsung s'engage dans sa politique de confidentialité à ne pas vendre ou communiquer les informations collectées. Si elle se tient à cette déclaration, nous n'avons donc rien à craindre. Si ce n'est que les règles peuvent changer, que des hackers ont déjà dévoilé bon nombre d'informations jugées sensibles et qu'un futur gouvernement pourrait demander/exiger l'accès à ces données au nom de la sécurité de ses ressortissants.

Une étude de l'université de Cambridge indique que, désormais, notre ordinateur nous connaît mieux que nos amis ou colocataires. En agrégeant nos données, notre ordinateur est plus à même de déterminer notre caractère et de prévoir nos réactions. Pour les plus connectés d'entre nous, l'ordinateur surpasse même le conjoint à ce jeu ![6]

III. QUELLES CONSÉQUENCES ?

Cela ne va pas sans poser des questions éthiques. Dans une société qui mise principalement sur l'avoir et le consommable, difficile de résister aux sirènes de la publicité.[7] Certaines personnes sont plus vulnérables que d'autres face à cette publicité ultra-ciblée. Sans compter les situations dramatiques auxquelles une trop grande consommation peut mener comme la précarité et le surendettement. Par ailleurs, ce ciblage vise également à nous proposer une « meilleure expérience utilisateur ». Grâce à ce qu'ils savent de nous, les géants d'Internet s'engagent à nous faciliter la vie en nous proposant en priorité les produits qui devraient rencontrer nos goûts précédemment enregistrés. En effet, selon qu'il vous estime pro-nucléaire ou militant écologiste, Google présentera des résultats différents pour une même recherche sur le nucléaire.[8] Il en va de même avec l'algorithme sur lequel se base Facebook pour proposer du contenu dans notre fil d'actualité, avec comme conséquence le risque de rester dans une zone de confort, sans chercher d'informations ni d'opinions différentes des nôtres. Confortés dans nos idées, nous tournons en rond, au risque de radicaliser nos points de vue.

---

6 Press Association, « Your computer knows you better than your friends do, say researchers", *The Guardian*, 13 janvier 2015, http://www.theguardian.com/technology/2015/jan/13/your-computer-knows-you-researchers-cambridge-stanford-university, consulté le 1er avril 2015.

7 On estime qu'une personne dans un pays occidental est soumise à environ 10.000 contacts publicitaires par jour. Bien sûr, toutes ne sont pas conscientes, mais notre cerveau enregistre parfois à notre insu les publicités qu'il rencontre. Pour plus de précisions, consulter : http://trends.levif.be/economie/entreprises/la-pub-parle-a-votre-inconscient/article-normal-181729.html

8 *Dégooglisons Internet*, *op. cit.*

On ne peut pas s'attendre à une amélioration de la situation. À travers les dernières mises à jour de ses « paramètres de confidentialité », Facebook s'octroie toujours plus de pouvoir dans la collecte de nos données personnelles. Aujourd'hui, le réseau social peut librement s'approprier vos photos, vos données bancaires, etc. L'application Facebook installée sur notre smartphone, peut maintenant lire nos SMS. Comment l'utilisateur a-t-il pu avaler cela ? En réalité, il ne s'est rendu compte de rien : en créant un compte sur le réseau social, les utilisateurs doivent accepter les conditions d'utilisation. Celles-ci comprennent une clause disant que l'utilisateur accepte automatiquement les conditions, même si celles-ci devaient changer. Le seul moyen de refuser ? Supprimer définitivement son compte sur Facebook. Mais la plupart des utilisateurs ne sont plus prêts à faire ce choix, le réseau social faisant désormais partie intégrante de leur vie.

> *« Facebook s'octroie toujours plus de pouvoir dans la collecte de nos données personnelles. »*

Les conditions d'utilisation des différents logiciels que nous utilisons sont très souvent (certains disent « à dessein ») particulièrement ardues à lire. C'est pourquoi une réflexion du style « si tout le monde a accepté, c'est qu'il n'y a pas de problème, je ne suis pas obligé de lire les conditions » est fréquente. Une expérience menée récemment en Grande-Bretagne dans un centre commercial montrait que les passants, pour se connecter au réseau, acceptaient sans les lire les conditions d'utilisation alors que celles-ci comprenaient une clause stipulant qu'ils devaient céder leur premier enfant. L'expérience faisait évidemment partie d'une campagne de sensibilisation, les enfants n'ont donc pas été réclamés.[9]

[9] C. Richard, « Ils cèdent leur premier-né pour du wifi gratuit… », *Rue 89*, 14 décembre 2014, http://rue89.nouvelobs.com/2014/12/14/conditions-dutilisation-ils-cedent-premier-wifi-gratuit-256560, consulté le 7 avril 2015.

Soulignons également que l'anonymat de nos données est précaire. Ainsi les sites récoltant des données personnelles précisent systématiquement que les informations collectées et envoyées le sont de manière anonyme de sorte qu'elles ne sont pas associées à notre nom. Cependant, l'agrégation de données est devenue tellement efficace, rapide et fiable qu'il est possible, à partir d'à peine deux ou trois informations accumulées sur une personne, de l'identifier précisément, et cela en un temps record.[10]

IV. UNE SURVEILLANCE QUI VA TOUJOURS PLUS LOIN

Malheureusement, ce ne sont pas là les seuls problèmes posés par ces pratiques de collecte et de vente des données personnelles. En 2013, l'affaire Snowden (voir encadré) a révélé que Facebook, ainsi que d'autres géants d'Internet tels que Google, Yahoo ! et Amazon, collaboraient avec l'agence nationale de sécurité américaine, la NSA.[11] Ces données personnelles ne seraient donc pas uniquement revendues pour des raisons publicitaires, mais seraient également utilisées par les États à des fins de surveillance.

En 2013, Edward Snowden, ancien employé de la National Security Agency (NSA), révèle que cette dernière enregistre des communications téléphoniques et électroniques, non seulement des citoyens américains mais également de personnes du monde entier. Les chiffres avancés sont hallucinants : mi-2012, il était question de 20 milliards de communications

...

[10] D. Boullier, « Tout devient-il donnée personnelle ? », in O. Coutor, *et alii*, *Vie privée à l'horizon 2020. Paroles d'experts*, Paris, Commission nationale de l'Informatique et des Libertés (CNIL), « Cahiers IP », n°1, 2012, p. 33.

[11] « Comprendre le programme 'Prism' », *LeMonde.fr*, 11 juin 2013, http://www.lemonde.fr/international/infographie/2013/06/11/le-programme-prism-en-une-infographie_3427774_3210.html, consulté le 1er avril 2015. Pour plus d'information, voir l'article : http://www.rtbf.be/info/monde/detail_affaire-prism-snowden-les-dix-grandes-revelations-qu-il-faut-en-retenir?id=8178443

collectées par jour à travers le monde.[12] L'affaire Snowden dévoile notamment la collaboration des grands services Internet qui communiquent les informations qu'ils ont récoltées auprès de leurs utilisateurs à la NSA, que celle-ci stocke et analyse à l'aide d'un programme appelé « PRISM ».[13]

Malgré des accusations aussi graves, l'affaire Snowden n'a eu que peu d'impact sur les comportements des internautes. Il est intéressant d'observer que beaucoup se disent inquiets pour leurs droits et libertés individuels, pour leur vie privée, mais n'hésitent pas à répandre une multitude d'informations les concernant dès qu'il s'agit d'être présent et actif sur un réseau social.

V. JUSTIFICATION DE LA SURVEILLANCE POUR DES RAISONS SÉCURITAIRES

Comment ce contrôle a-t-il pu prendre une telle ampleur ? Il existe un lien étroit entre la surveillance des citoyens et la réduction des libertés individuelles d'une part, et les préoccupations sécuritaires de l'autre. À la suite des attentats du 11 septembre 2001, et d'autres événements meurtriers qui se sont produits ces dernières années, de nombreux gouvernements à travers le monde ont progressivement introduit des mesures liberticides, légitimées par des discours sécuritaires. Qui s'étonne aujourd'hui de voir une caméra de surveillance à chaque coin de rue ou presque ? Nous savons également qu'il y a eu une extension des autorisations d'écoutes téléphoniques.[14] Prochainement, les passagers aériens transitant par l'espace Schengen seront peut-être au-

[12] G. Greenwald, « L'affaire Snowden racontée par celui qui l'a révélée", *LeMonde.fr*, 13 mai 2014, http://www.lemonde.fr/technologies/article/2014/05/13/l-affaire-snowden-racontee-par-celui-qui-l-a-revelee_4415920_651865.html, consulté le 1er avril 2015.

[13] T. Soulcier, M Untersinger, « Big Brother : Souriez, vous êtes fichés ! », *La Revue Dessinée*, n°4, 2014, p. 10-29.

[14] W. Fayoumi, « Chambre: projet d'élargissement des écoutes téléphoniques confirmé », *RTBF Info*, 15 janvier 2015, http://www.rtbf.be/info/belgique/detail_securite-et-renseignement-au-menu-des-deputes-ce-jeudi?id=8779767, consulté le 10 avril 2015.

tomatiquement repris sur une base de données commune compilant bon nombre de données personnelles (âge, mode de paiement utilisé, itinéraire, etc.).[15] Tout cela au nom de la sacro-sainte sécurité.

Par ailleurs, on observe une certaine apathie de la part des citoyens. Pour ceux qui s'y intéressent, le débat est très polarisé. D'un côté ceux qui par manque d'intérêt ou parce qu'ils affirment n'avoir rien à cacher, disent ne pas se soucier de cette surveillance. Parmi eux, certains sont prêts à perdre une partie de leur intimité pour se protéger d'une potentielle attaque terroriste. *D'ailleurs, des attaques ont déjà été évitées grâce à cette surveillance accrue, alors, pourquoi leur donner tort ?* De l'autre côté, leurs opposants tentent de nous mettre en garde : (pour eux) nous nous dirigeons, au nom du principe de sécurité, vers une société de surveillance généralisée qui nuit aux libertés individuelles.

> *« Nous ne tolérerions jamais d'être surveillés dans la vie « réelle ». Alors, pourquoi l'accepter dans la vie « virtuelle » ? »*

Arrêtons-nous donc un moment sur cette position : « Je n'ai rien à cacher ». Si, à première vue, notre sécurité nous paraît valoir quelques intrusions dans notre vie privée, on peut néanmoins se demander si l'argument n'affiche pas ses limites.

Premièrement, parce que nous ne tolérerions jamais d'être surveillés dans la vie « réelle ». Alors, pourquoi l'accepter dans la vie « virtuelle » ? En effet, comment réagirions-nous si en rentrant à notre domicile nous y trouvions quelqu'un occupé à lire notre courrier dans la boîte aux lettres, analyser notre répertoire de contacts, voire même nous suivre pour relever avec précision nos habitudes de déplacements ou d'achats ?

Ensuite parce que plusieurs acteurs surveillent ces comportements d'achats, communications, relations, déplacements, et ce, nous l'avons vu, pour des raisons différentes. Si toutes ces données personnelles devaient se retrouver un jour dans les mains d'un seul, il serait alors possible par exemple pour notre

[15] Un PNR existe déjà pour les citoyens européens qui se rendent aux États-Unis. Le projet ici est d'élargir cette pratique à tous les vols intra-européens. Pour plus d'informations à ce sujet, voir http://www.rtbf.be/info/dossier/euranetplus/detail_ue-la-commission-veut-un-pnr-europeen-le-plus-rapidement-possible?id=8820156

assurance santé de rendre notre alimentation responsable de nos problèmes de santé, avec pour preuve les achats enregistrés sur notre carte de fidélité d'un supermarché. Le nombre de débordements possibles est vertigineux.

Enfin, tout simplement car l'argument « je n'ai rien à cacher » contribue à définir la défense de la vie privée comme une tentative de cacher des choses mauvaises par essence en assimilant la vie privée à la malhonnêteté. Or, le droit à la vie privée fait partie des libertés fondamentales et doit être protégé.

CONCLUSION

Nous n'en sommes encore qu'aux prémices de la marchandisation de nos données personnelles. Les renseignements se contentent d'engranger des données sans pouvoir toujours les analyser, faute de moyens techniques. Les réseaux sociaux devraient encore prendre de l'ampleur, et avec eux, l'enregistrement de nos données.

Si nous nous obstinons dans cette voie sans garde-fou, difficile d'écarter définitivement le scénario catastrophe. La France manque de peu d'illustrer ces craintes. La loi « Renseignement » actuellement examinée par le Sénat vise à protéger les citoyens en permettant au Premier ministre d'intercepter toutes les communications électroniques des Français, et ce sans décision de justice. En cas de scanning suspect, un citoyen français pourra faire l'objet d'une surveillance rapprochée sans aucune forme de procès.[16] Selon le journal *Le Monde*, le Gouvernement avait, en réalité, déjà recours à ce type de pratiques. En effet, il semblerait que des milliards de données soient déjà interceptées et stockées par la Plateforme nationale de Cryptage et de Décryptement (PNCD). Ces données seraient non seulement utilisées par les services de renseignement français mais également comme monnaie d'échange avec les services de sécurité étrangers pour l'obtention d'informations sensibles.[17]

Par ailleurs, les marges de liberté concernant la vie privée s'amenuisent aussi au rythme du développement des nouvelles technologies : la connexion permanente devient la norme, entraînant la nécessité de se justifier d'un trop long délai de réponse à un mail ou un message. Parallèlement, la géolocalisation se fait de plus en plus fréquente. Si cette tendance se maintient, « s'y opposer [à la géolocalisation constante] risque de devenir synonyme d'incivilité. Suspect, car dans un environnement où la norme deviendrait la géolocalisation généralisée, s'y refuser entraînerait immanquablement soupçons et suspicions. »[18]

[16] J.-G. Santi, « Loi renseignement : une surveillance de masse ? », *LeMonde.fr*, 10 avril 2015, http://www.lemonde.fr/pixels/video/2015/04/02/loi-renseignement-une-surveillance-de-masse_4608783_4408996.html, consulté le 13 avril 2015.

[17] G. Poncet, « France : terribles révélations sur la surveillance massive », *Le Point*, 13 avril 2015, http://www.lepoint.fr/chroniqueurs-du-point/guerric-poncet/france-terribles-revelations-sur-la-surveillance-massive-13-04-2015-1920630_506.php, consulté le 13 avril 2015.

[18] C. Balagué, « Géolocalisation : où allons-nous ? », in O. Coutor, *et alii*, *op. cit.,* p. 23.

Quel sera demain le visage de notre liberté ? La marginalité trouvera-t-elle encore à s'exprimer sans éveiller les soupçons ? À l'image de Winston, le héros du terrible roman d'anticipation de George Orwell « 1984 », nous pourrions être traqué en permanence, perdre la liberté de fréquenter qui l'on veut, de dire ce que l'on veut et de faire ce que l'on veut.

Heureusement, tout n'est pas perdu d'avance ! Il existe certaines tentatives de régularisation, notamment au niveau européen. La Commission européenne a récemment commandé une enquête afin d'estimer si la réglementation européenne en matière de protection de la vie privée sur Internet était suffisante, démontrant ainsi son intérêt pour la question.[19] De même, les gouvernements nationaux n'auront pas accès aux données des passagers aériens. Alors que cette proposition devait servir la lutte anti-terroriste, le Parlement européen l'a déboutée, privilégiant le respect de la vie privée des citoyens.[20]

Bien sûr, il va sans dire que des individus suspectés (sur la base d'indices fondés) de représenter une menace pour la sécurité d'autres personnes peuvent faire l'objet d'une surveillance particulière. Ce que nous cherchons à éviter à tout prix, par contre, est une surveillance généralisée des habitants, sans soupçon préalable d'une quelconque mauvaise intention. Le rôle des politiques est maintenant de trouver un juste milieu pour protéger au mieux leurs citoyens, tout en préservant leurs droits fondamentaux, et éviter ainsi de tomber dans une psychose générale. Restons vigilants, citoyens et dirigeants quant aux dérives liberticides déjà expérimentées ailleurs.

[19] M. Paquay, *op. cit.*

[20] C. Vallet, « PNR, le Big Brother de l'air », *Slate*, 20 janvier 2015, http://www.slate.fr/story/96961/pnr-le-big-brother-de-l%E2%80%99air, consulté le 13 avril2015.

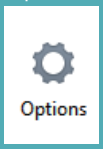
HUIT CONSEILS POUR PROTÉGER SA VIE PRIVÉE

1. Paramétrer l'enregistrement des cookies sur son navigateur web (Mozilla Firefox, Google Chrome, Internet Explorer, Opéra ou Safari). La plupart des navigateurs proposent désormais une navigation privée pour surfer sur Internet. Cela signifie qu'ils s'engagent à ne pas conserver les historiques de navigations et à supprimer tous les cookies après la fermeture de la fenêtre. Attention, cela ne signifie pas pour autant que vous naviguez de manière anonyme : les sites que vous visitez, votre fournisseur d'accès et même votre patron peuvent, eux, garder vos données de connexion.

Firefox **version 38.0.1**

1 > Ouvrir le **menu**

2 > cliquer sur **options**

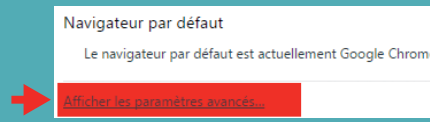


3 > cliquer sur **Vie privée** > a. cocher l'unique case dans **Pistage**
> b. dans **Historique**
> **Règle de conservation**
> **Utiliser les paramètres personnalisés...**
> c. **Accepter les cookies tiers** > **jamais**

Google Chrome **version 43.0.2357.81**

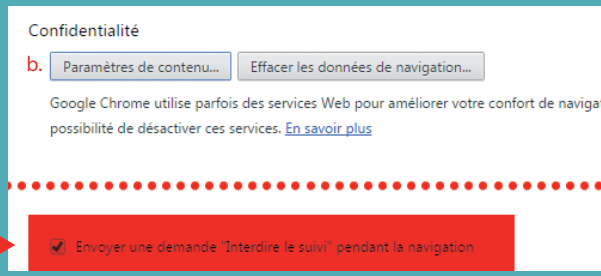
1 > Ouvrir le **menu**
> cliquer sur **Paramètres**

2 > cliquer sur **Paramètres avancés**

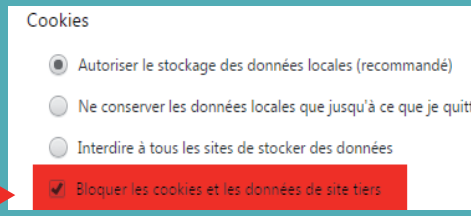


3 > dans **Confidentialité**
a. > cocher **Envoyer une demande « Interdire le suivi » pendant la navigation**
b. > cliquer sur **Paramètres de contenu**
> dans **Cookies** > cocher **Bloquer les cookies et les données de site tiers**

a.



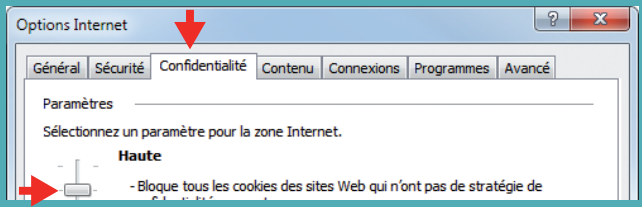
b.



Internet Explorer 11 **version 11.0.9600.17591**

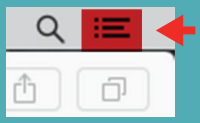
1 > Ouvrir **Outils**
> ouvrir **Sécurité**
> cliquer sur **Activer les demandes Do Not Track**

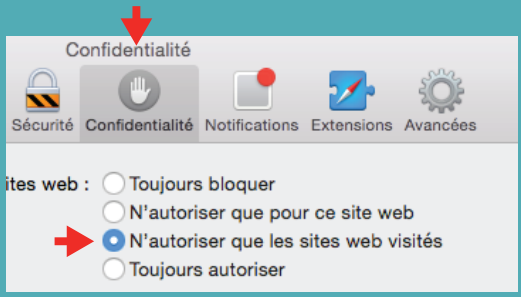
2 > Ouvrir **Outils**
> cliquer sur **Options internet**
> sélectionner l'onglet **Confidentialité**
> placer le curseur sur **Haute**



Safari **version MacIntosh 8.0.4**

> cliquer sur **Menu**
> ouvrir **Préférences**
> sélectionner l'onglet **Confidentialité**
> **Cookies et données de sites web**
> cocher **N'autoriser que les sites web visités**





2. Utiliser un navigateur plus respectueux de la vie privée : Mozilla Firefox et Internet Explorer ont bonne réputation à ce niveau. Il est même possible de télécharger Dooble, un navigateur qui propose les fonctionnalités de base d'un navigateur et qui efface toute information sur votre navigation une fois la fenêtre fermée.

3. Activer la géolocalisation sur son téléphone uniquement quand c'est nécessaire. Bien penser à la désactiver juste après.

4. Trouver des alternatives à Google. Par exemple, le moteur de recherche Duckduckgo promet de ne collecter ou partager aucune donnée personnelle. (https://duckduckgo.com/)

5. Choisir un mot de passe plus complexe. Selon Edward Snowden, il est plus efficace de penser en phrase plutôt qu'en mot, en y incluant des chiffres et des majuscules (il suggère par exemple : « MargareThatcheri s110%SEXY ») ; et le changer régulièrement.

6. Prendre le temps de contrôler ses paramètres de confidentialité sur Facebook et les vérifier régulièrement.

7. Faire attention à ce que l'on divulgue volontairement, par exemple au travers des réseaux sociaux. Écrire son adresse, payer en ligne sur un site commercial, poster une photo de son enfant sont des choix à considérer attentivement, en mesurant les conséquences possibles.

8. Pour les plus convaincus, il est aussi possible de crypter ses mails en téléchargeant par exemple le programme Thunderbird et de naviguer sur Internet via Tor, un réseau qui transmet vos requêtes par un chemin aléatoire, rendant ainsi difficile la tâche de remonter jusqu'à votre ordinateur.

Ces conseils ne transformeront pas votre vie privée en forteresse impénétrable, mais y rendront l'accès beaucoup moins aisé. Cela demandera plus de temps et de moyens pour une firme ou une agence de renseignement de récolter vos données. En espérant que si suffisamment d'utilisateurs s'y attellent, ils n'auront plus les ressources nécessaires (en personnel et financières) pour maintenir ces pratiques.

BIBLIOGRAPHIE

1. Monographie

– Coutor O., *et alii*, *Vie privée à l'horizon 2020*. Paroles d'experts, Paris : Commission nationale de l'Informatique et des Libertés (CNIL), « Cahiers IP », n°1, 2012.

2. Presse

– « Comprendre le programme 'Prism' », *LeMonde.fr*, 11 juin 2013, http://www.lemonde.fr/international/infographie/2013/06/11/le-programme-prism-en-une-infographie_3427774_3210.html, consulté le 1er avril 2015.

– Fayoumi W., « Chambre: projet d'élargissement des écoutes téléphoniques confirmé », *RTBF Info*, 15 janvier 2015, http://www.rtbf.be/info/belgique/detail_securite-et-renseignement-au-menu-des-deputes-ce-jeudi?id=8779767, consulté le 10 avril 2015.

– Greenwald G., « L'affaire Snowden racontée par celui qui l'a révélée », *Le Monde*, 13 mai 2014, http://www.lemonde.fr/technologies/article/2014/05/13/l-affaire-snowden-racontee-par-celui-qui-l-a-revelee_4415920_651865.html, consulté le 1er avril 2015.

– Paquay M., « Cookies : la vie privée des internautes n'est pas assez respectée », *RTBF Info*, 10 avril 2015, http://www.rtbf.be/info/societe/detail_cookies-la-vie-privee-des-internautes-n-est-pas-assez-respectee?id=8952503, consulté le 10 avril 2015.

– Poncet G., « France : terribles révélations sur la surveillance massive », *Le Point*, 13 avril 2015, http://www.lepoint.fr/chroniqueurs-du-point/guerric-poncet/france-terribles-revelations-sur-la-surveillance-massive-13-04-2015-1920630_506.php, consulté le 13 avril2015.

- Press Association, « Your computer knows you better than your friends do, say researchers », *The Guardian*, 13 janvier 2015, http://www.theguardian.com/technology/2015/jan/13/your-computer-knows-you-researchers-cambridge-stanford-university, consulté le 1er avril 2015.
- Richard C., « Ils cèdent leur premier-né pour du wifi gratuit… », Rue 89, 14 décembre2014, http://rue89.nouvelobs.com/2014/12/14/conditions-dutilisation-ils-cedent-premier-wifi-gratuit-256560, consulté le 7 avril 2015.
- Rundle M., « Samsung Smart TV Voice Recognition Privacy Policy Reads Like George Orwell's '1984' », The Huffington Post, 9 février 2015, http://www.huffingtonpost.co.uk/2015/02/09/samsung-smart-tv-privacy-1984_n_6642934.html, consulté le 1er avril 2015.
- Santi J.-G., « Loi renseignement : une surveillance de masse ? », *LeMonde.fr*, 10 avril 2015, http://www.lemonde.fr/pixels/video/2015/04/02/loi-renseignement-une-surveillance-de-masse_4608783_4408996.html, consulté le 13 avril 2015.
- Soulcier T., Untersinger M., « Big Brother : Souriez, vous êtes fichés ! », *La Revue Dessinée*, 4, 2014.
- Vallet C., « PNR, le Big Brother de l'air », *Slate*, 20 janvier 2015, http://www.slate.fr/story/96961/pnr-le-big-brother-de-l%E2%80%99air, consulté le 13 avril 2015.
- « Vie privée : même quand vous êtes déconnecté, Facebook peut vous traquer », *L'Express*, 11 avril 2015, http://lexpansion.lexpress.fr/high-tech/vie-privee-meme-quand-vous-etes-deconnecte-facebook-peut-vous-traquer_1670230.html, consulté le 13 avril 2015.

3. Site Internet

- *Dégooglisons Internet*, http://degooglisons-internet.org, consulté le 7 avril 2015.

Auteur : Nathalie Dufays

DÉSIREUX D'EN SAVOIR PLUS !

Animation, conférence, table ronde… n'hésitez pas à nous contacter,
Nous sommes à votre service pour organiser des activités sur cette thématique.

www.cpcp.be

FÉDÉRATION
WALLONIE-BRUXELLES

Avec le soutien du Ministère de la Fédération Wallonie-Bruxelles

E.R. : Eric Poncin - Rue des Deux Églises 45 - 1000 Bruxelles

Centre Permanent pour la Citoyenneté et la Participation

Rue des Deux Églises 45 - 1000 Bruxelles
T : 02/238 01 27
info@cpcp.be

© CPCP asbl - 2015