Juin 2020

La cage se referme...

Windows, Apple, Facebook, Google, GMail, Hotmail, Whatsapp…

- **Qu'avez-vous réellement accepté en cliquant < OK > la 1ère fois ?**
  => Vous n'imaginez même pas !
- **Qui sait quoi de vous ?**
  => Qui ? Les Etats, mais pas qu'eux ! Quoi ? Cela fait peur…
- **Vous n'avez rien à cacher ?**
  => On parie ?
- **La surveillance à la chinoise demain chez nous ?**
  => Le système est déjà vendu à plus de 60 pays !
  => La technologie se met actuellement en place !
- **Et s'il y avait pire encore ?**

Prendrez-vous la pilule rouge ?

8 pages pour le réveil !

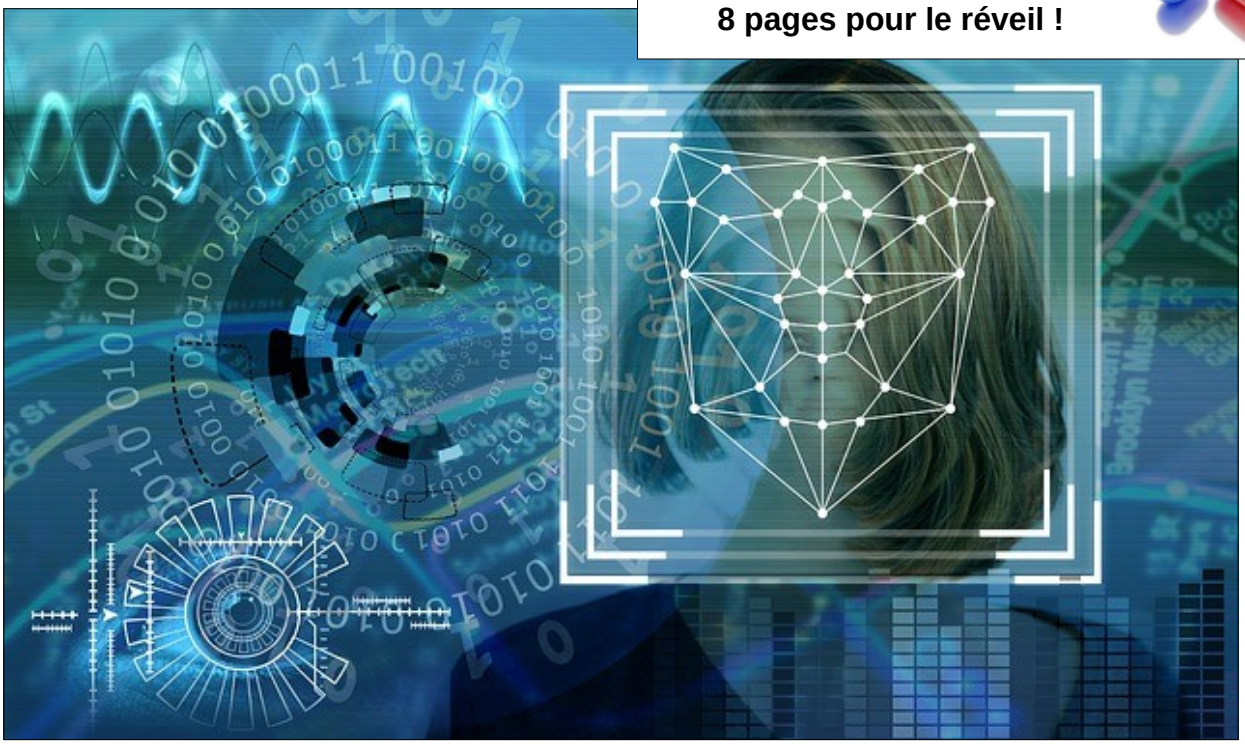


Table des matières

Tout était parfait dans le meilleur des mondes…

Google : Smartphone avec Android, GMail, YouTube, Google Drive, Google Doc, Google Agenda, Dropbox...

Apple : IOS, Mac-OS, iCloud, iPhone, iTunes…

Facebook : Messenger, Instagram, WhatsApp...

Microsoft : Windows, Outlook, Hotmail, Skype, OneDrive, LinkedIn, Office 365, Edge, …

Yahoo : Yahoo Mail...

On regroupe ces fournisseurs de produits et services sous l'acronyme GAFAM : Google-Apple-Facebook-Amazon-Microsoft. (Amazon n'est pas pris en compte ci-après mais Yahoo y est intégré).

Qui n'est pas concerné par ces systèmes et applications ? Voire certains en permanence ?

Les produits sont bien conçus, tellement utiles et pratiques qu'ils sont devenus incontournables, tant au travail que dans les loisirs et la vie sociale, de façon si agréable, ludique et divertissante que bon nombre ne peuvent plus vivre sans.

Tout pourrait donc être pour le mieux dans le meilleur des mondes !

Une question quand même...

A la première installation ou utilisation de ces produits, une longue page de texte bien compact s'affiche, avec tout en bas une case à cocher et un bouton < OK >.

Sans accepter ces conditions, on ne peut pas utiliser le produit… et donc quasiment tous les utilisateur.ice.s cliquent **< OK >** et donnent ainsi leur accord.

Mais leur accord pour quoi précisément ?

Pour le savoir, il faudrait lire le détail de cette fameuse page : le résumé des « Termes et conditions d'utilisation » (CGU) : des documents qui font parfois plus de 100 pages, en langage juridique… Autant dire que personne ne le fait !

Ces textes concernent, entre autres, les données personnelles et l'utilisation qui en est faite.

Les données personnelles ? C'est juste les " nom, l'adresse e-mail et le numéro de téléphone " ? Non, pas vraiment. En utilisant les produits et les services des GAFAM, les utilisateur·ice·s acceptent de donner, de plein gré, bien plus de données...

La page suivante les synthétise. Les détails diffèrent d'un produit à l'autre mais toutes ces infos proviennent directement des textes originaux[1].

Il est **vivement** conseillé de se pencher sur les annexes de cet article qui reprennent des extraits originaux et choisis pour les principaux fournisseurs (résumé de +- 5 pages par fournisseur).

Histoire d'avoir eu **au moins une fois dans sa vie** un aperçu détaillé des termes et conditions d'utilisation de ces produits utilisés chaque jour. Et de pouvoir ainsi, en **toute connaissance de cause**, continuer (ou pas) à livrer ses informations et sa vie.

Données personnelles récupérées, stockées, analysées...

Les détails diffèrent d'un produit à l'autre, mais globalement, **l'utilisateur autorise le fournisseur de service à récupérer ses données** ainsi que d'autres informations qui y sont liées.
L'utilisateur peut refuser de donner une partie des données (car ils en prennent quand même), en décochant des cases souvent cochées par défaut dans les produits. Dans certains cas, le prestataire continue à traiter les données même si le consentement de l'utilisateur a été retiré (raison légale) et peut aussi collecter des données même si l'utilisateur n'est pas connecté au service.

Données liées à la personne

- Coordonnées complètes (adresse, âge, sexe, langue)
- Coordonnées bancaires complètes (cartes et codes de sécurité)
- Ensemble des contacts et relations
- Données fournies sur les contacts
- Données sociales (interaction avec d'autres personnes, groupes ou organisations)
- Empreintes digitales et reconnaissance faciale (certains téléphones comme iPhone)

Données à propos de l'infrastructure

- Inventaire complet du matériel, du système d'exploitation, des logiciels et numéros de licences, qu'ils soient de l'entreprise concernée ou non
- Données sur les réseaux situés à proximité
- Données de géolocalisation (GPS, WIFI & Bluetooth à proximité de l'appareil, adresse IP)

Données d'activité

- Toute opération – mouvement de souris ou de fenêtre effectué sur l'appareil
- Historique de l'utilisation des applications utilisées, des fichiers ouverts
- Toutes les recherches sur le web, toutes les pages et sites consultés
- Données de consommation de contenus
- Données de SMS, d'entrées manuscrites et de frappe
- Durées des écoutes musicales-vidéos, des pauses-reculer-avancer, …

Données analysées

- Centre d'intérêt et activités favorites (collectés ou déduits et devinés)
- Communications de tous type (audio, vidéo, texte), message, mail & pièces jointes
- Le **CONTENU** (avec analyse automatisée ou manuelle) de tout document stocké ou transitant par le service concerné (cloud, etc.), de tout document créé ou modifié sur l'appareil (que ce soit avec le produit concerné ou non (Windows)), de tout document reçu par mail

Autres informations

Les fournisseurs **récupèrent des données via d'autres prestataires** et les **combinent** avec les données déjà récupérées :

- Publications sur les réseau sociaux
- Données de géolocalisation via les opérateurs téléphoniques
- Bases de données officielles (commerciales, gouvernementales...)

Utilisation des données

La collecte s'appuie sur « diverses raisons » et autorisations juridiques.

- Pour proposer des offres commerciales adaptées
- Pour servir les « intérêts légitimes » du prestataire et de ses partenaires
- Pour garantir la sécurité des utilisateurs, lutter contre la fraude
- Pour localiser un appareil éteint
- **Pour la nécessité d'exécuter des contrats et de se conformer à des obligations légales (obligations légales = collaboration avec les autorités)**

Tous les contenus sont analysés par sécurité. Le prestataire peut refuser d'effacer les données récoltées et peut les modifier. L'utilisateur confère aussi au prestataire une licence mondiale, gratuite, perpétuelle et non exclusive d'utilisation des éléments.

Transfert des données

Les données sont échangées entre les partenaires du prestataire et ses obligataires légaux.
Elles sont divulguées lorsque le prestataire « pense » qu'il est nécessaire de le faire, pour l'intérêt public entre autres. Les données peuvent être **transférées vers d'autres pays, dont certains sont explicitement mentionnés comme n'étant pas reconnus comme offrant un niveau de protection adéquat des données (noté noir sur blanc !)**.

Qui possède les données ? Les «justifications légales » des GAFAM…

Les services de sécurité américains...

- L'affaire Snowden[6] (2013) a révélé qu'outre l'écoute des lignes téléphoniques, les services de sécurité américains se procuraient des données **directement dans les bases de données des GAFAM** via des backdoors (« portes d'entrées discrètes »).

- En effet, en vertu du « **Patriot Act** »[2] (2001 & renforcé 2020) et du discret « **Cloud Act** »[2] (2018), les 17 services de sécurité américains (NSA, CIA, FBI...) peuvent **accéder aux données des particuliers et des entreprises américaines, sans autorisation et sans prévenir les utilisateurs**. Le « Cloud Act » étend l'accès aux serveurs hors USA !

  Les **cours fédérales américaines** estiment la surveillance **mondiale** sans autorisation (toutes données confondues : mail, téléphonie, données légales-médicales-bancaires...) comme **légales**, et d'autant plus en vertu des dernières lois approuvées par Donald Trump[43].

United States Intelligence Community

Les services de sécurités des pays alliés des USA...

- Le « **FISA Amendments Act** »[3] autorise les procédures de surveillance physique et électronique, la collecte d'information (espionnage) sur des puissances étrangères ainsi que l'**échange d'informations avec d'autres pays :** directement avec les pays des « Five Eyes » en vertu de l'« UKUSA Agreement » (USA, Canada, Royaume-Uni, Australie, Nouvelle-Zélande) et globalement les pays alliés (OTAN, etc.). C'est le programme **PRISM**[4].

- Le programme **XKeyscore**[5] est un autre programme de surveillance de masse de la NSA américaine, réalisé avec les « Five Eyes » : mails, pièces attachées, activité sur le web. Son outil « DNI Presenter » permet de lire les échanges privés sur les réseaux sociaux.

- Lors de l'affaire Snowden, les GAFAM ont clamé leur ignorance-innocence mais le service juridique de la NSA a déclaré qu'ils collaboraient activement avec les autorités[7] : Microsoft travaillait avec le FBI pour donner un accès direct aux messageries Outlook et Hotmail. Yahoo s'est dévoilé en 2015. Pressés par l'opinion, ils se sont ensuite justifiés par leurs « **obligations légales** » : les utilisateurs sont dûment avertis dans les « Terms & Conditions ».

  Qui garantit aujourd'hui que de nouveaux backdoors (légaux) ne sont pas en place ? Et que les GAFAM ne collaborent pas ouvertement ? Ils ne s'en sont pas privés par le passé.

Et en France ?

En France, la « **Loi de programmation militaire (LPM) 2019-2025** »[8] autorise la police, la gendarmerie, ainsi que les services habilités des ministères de la Défense, de l'Économie et du Budget à **surveiller les citoyens sur les réseaux informatiques sans l'autorisation d'un juge**.

Orange, la DGSE et le GCHQ britannique collaborent activement ensemble[9]. Un signe des alliances sous-jacentes : Snowden demande en vain l'asile politique à la France depuis des années… Ni Hollande ni Macron n'ont accepté.

Les photos ?

La start-up « Clearview AI » a collecté **3,5 milliards de photos** sur internet, dont Facebook, YouTube et Twitter (New-York Times du 18 janvier 2020[10]). Elle vend une application à l'efficacité redoutable pour **identifier une personne** et trouver d'autres clichés et liens d'informations la concernant.

L'application est **réservée à un usage professionnel de sécurité** (accès = 250.000 $ / an). Mais en février 2020[11], les noms des clients ont été piratés et publiés : 27 pays, 2.800 institutions dont **une série d'entreprises commerciales** dans le retail, le divertissement et la finance.

Pour résumer...

Les GAFAM, leurs partenaires et les Etats disposent d'une **immense base de données** avec profils détaillés et **photos**.

Les données sont **combinées** à d'autres sources d'informations (officielles, récupérées dans les entreprises, banques, etc.) par les services de sécurité occidentaux qui se les **échangent… et peuvent se faire pirater**.

Des **sociétés privées** achètent maintenant ces données.

« Je n'ai rien à cacher »

La justification officielle de la collecte de données est la sécurité et la lutte contre le terrorisme, avec l'idée sous-jacente et soutenue « qu'un citoyen qui n'a rien à cacher n'a aucun souci à se faire. »

La sécurité, prétexte au contrôle social

Des lanceurs d'alertes[12] (e.a. W. Binney, ex-directeur technique NSA et T. Drake, analyste US Army) clament haut et fort qu'aucun attentat n'a été évité par la surveillance de masse mais que celle-ci sert en premier lieu à contrôler la population, sous couvert de la sécurité : **Qui est qui, qui pense quoi ?**

Quelques exemples tirés de l'excellent documentaire « Nothing to Hide »[12] (A voir ! Source n°12) :

- Toutes les personnes du mouvement « Occupy Wall Street », classé pacifiste et non-violent par le FBI, **étaient surveillées par toutes les techniques anti-terroristes**, avec aval officiel.
- En France, Dominique Domenjoud[13] est **surveillé** car militant écologiste, agissant pacifiquement contre la COP-21 ou contre l'installation d'un aéroport près de Nantes… Son dossier officiel mentionne désormais « participe activement depuis plusieurs années aux actions menées contre les représentations de l'État ».
- Des chercheurs sur les droits humains qui sont surveillés.
- Le reportage illustre aussi le souvenir et le traumatisme de la STASI en Allemagne.

Le citoyen qui ne fait rien d'illégal peut être rattrapé par le fichage de masse :

- Une personne « suspecte » rend son entourage suspect ou complice potentiel.
- **Tout citoyen peut devenir militant** demain si sa voix est ignorée, si ses droits, ses biens, ses proches sont bafoués ou si l'on place un gazoduc dans son jardin...
- Les données permettent d'identifier groupes sociaux, leaders d'opinion, syndicalistes, lanceurs d'alerte et servir des intérêts politiques ou privés, des lobbies...
- **Un régime politique peut changer** et ce qui est autorisé aujourd'hui devient subitement illégal demain.
- Dans certains pays, l'appartenance à un groupe (syndicat, mouvement d'opinion, LBGT, …) peut signifier arrestation-déportation-mort…

Plus prosaïquement

- Les **données** peuvent être cédées, **vendues**, voire **piratées et servir au vol, au chantage.** *(Ex. Mai 2020 : Le groupe de hackers ShinyHunters a mis en vente les données de 73,2 millions d'internautes)*[14] Elles servent à **usurper une identité pour des achats, de faux contrats ou à perpétuer des vols, escroqueries et abus de confiance sous le nom d'un innocent** (le vôtre ?)**.**
- En fonction de votre profil, des sociétés privées proposent des **produits plus chers, refusent des prêts, des contrats d'assurance, une embauche...** (parce qu'un membre de la famille a des antécédents psychiatriques... que votre profil montre que vous aimez le sucre… que vous avez donné un avis sur quelque chose et qui bouscule un intérêt...).
- **Qui** possédera vos données **demain** ? (états, entreprises, pirates, employeurs, assureurs…)

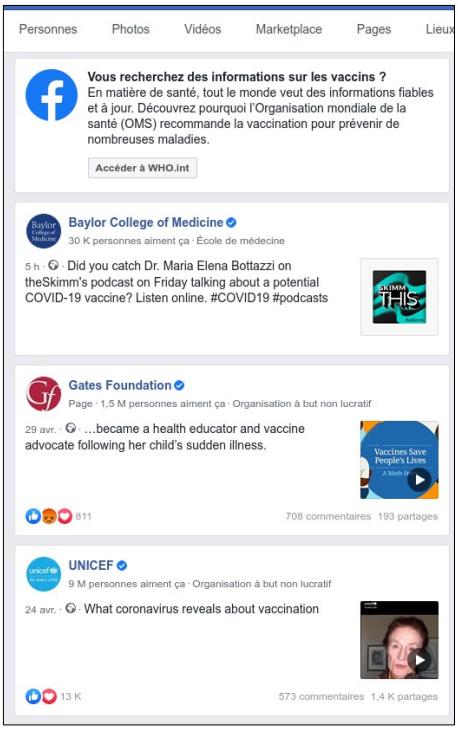
Manipulation de l'opinion

Les données et le profilage servent à **manipuler l'opinion publique, favoriser des choix politiques ou commerciaux...**

- La société « Cambridge Analytica »[15] a analysé les profils des utilisateurs Facebook et **a favorisé l'élection de Donald Trump**. Elle a proposé des publications adaptées aux profils, orienté les débats en renforçant la visibilité de liens (articles, spots, newsletters…), en likant des articles influençant les opinions, etc.
  La société aurait **influencé plus de 200 élections** et est impliquée dans la campagne des pro-brexit en Angleterre pour des agissements similaires. **SCL Group** (https://sclgroup.online) offre ses services d'**aide aux processus électoraux à l'échelle mondiale !**
- La Russie[16] est fréquemment accusée de manipuler les opinions via de faux comptes Facebook et la publication d'**articles déstabilisateurs**, favorisant ou défavorisant un candidat ou une opinion, et ciblant des **utilisateurs sélectionnés suivant leur profil**.
- L'élection de Bolsonaro a été influencée par des actions sur WhatsApp[17].
- Sur les réseaux sociaux, on utilise les « **trolls** » : des comptes qui propagent du **contenu orienté** pour créer le doute ou des polémiques en envoyant ces contenus aux utilisateurs ciblés comme réceptifs d'après leurs profils. Les « **bots** », comptes automatisés (intelligence artificielle) analysent les textes et crée des **contenus faux mais crédibles** ! Ils peuvent réagir aux messages de manière dynamique[18].
- Une recherche pour un billet d'avion montre que le prix monte à chaque heure...

La nouvelle arme de la pensée unique : le bannissement ou la mort digitale !

- **Facebook (2,6 milliards d'utilisateurs - 2020) et Youtube ont des équipes qui déterminent si un contenu** est conforme à la (leur !) « **morale** » et intérêts. Un encart apparaît sur une page « non fiable » et propose de « meilleurs » liens.
  Une recherche sur « Vaccin Infos France » (une page existante qui devrait donc apparaître en 1er lieu) reçoit un avertissement avec un lien vers l'OMS, suivi d'une vingtaine de liens (dont plusieurs fois la « Gates Foundation », 1er contributeur de l'OMS en 2020) avant d'afficher le bon résultat. Facebook choisit aussi ce qu'il affiche en provenance des pages des « amis »...



- **Le moteur de recherche Google (93 % des recherches sur internet hors Chine et Russie[36]) censure**[19] allègrement une série de sites, sur demande officielle ou suivant des règles liées à ses partenariats.

  Soit la recherche n'aboutira pas, soit la bonne réponse est catapultée dans les dernières pages de résultats. L'**ordre d'affichage** des résultats a également un rôle essentiel et est foncièrement **partial :** une même recherche avec Google et un autre moteur présentent des résultats nettement différents sur un plan documentaire mais aussi clairement sur le plan idéologique !

  Bref, Google montre ce qu'il veut bien que l'on voie. Un nombre croissant de personnes, d'associations et de journaux libres se plaignent de voir leurs audiences baisser drastiquement.
- **Google** a lancé un « Fond d'Aide à la Presse »[20] et **finance plusieurs grands journaux** dont « **Le Monde** ». Ce dernier propose le « Decodex »[21] : une page permettant de connaître la « fiabilité » d'un site ! La « fondation Gates » a versé 4 millions de dollars au journal « Le Monde »[40]. Et **Facebook** paie « le Monde », encore lui, pour filtrer les publications[41] de ses utilisateurs. **Où sont passées la liberté de la presse et de parole ?**

La Chine aujourd'hui

Le reportage « Tous surveillés – 7 milliards de suspects" sur Arte illustre la surveillance de masse en Chine[22] .
(A voir ! Source n° 22).

Tous les faits et gestes sur la voie publique sont filmés et les citoyens identifiés. Et aujourd'hui, même de dos, à leur démarche, masqués[23], dans une foule[24]...

Une expérience avec un journaliste a montré qu'un « suspect » avait été appréhendé par les autorités 7 minutes[25] après avoir été renseigné dans les bases de données comme étant "A arrêter".

Les données des tribunaux, de la police, des banques, des impôts et des employeurs, sont utilisées.

Un système de notation des citoyens[26] (crédit social) gère la vie en société : de mauvaises notes (opinions politiques dissidentes, recherches en ligne suspectes, trop de temps passé à jouer des jeux vidéos, passages piétons traversés à la hâte, retards de remboursement…) signifient la restriction ou l'interdiction de déplacement, la limitation d'accès à des prêts ou logement sociaux, des billets de trains plus chers, le refus d'inscrire les enfants à certaines écoles, le refus à l'embauche…

De bonnes notes : réductions pour divers services (chauffage, transports, prêts...), dispense de file à l'hôpital… Pour récupérer des points : faire du bénévolat, faire des dons caritatifs, donner son sang... En téléphonant à une personne à la note médiocre, l'appelant entendra une voix lui conseillant de ramener l'interlocuteur dans le droit chemin, ou de l'éviter…

La répression pure et simple
Prétextant en 2016 un programme de santé[27], les données biométriques de toute la population du Xinjiang, où vit une importante minorité musulmane, les Ouïghours, ont été enregistrées.

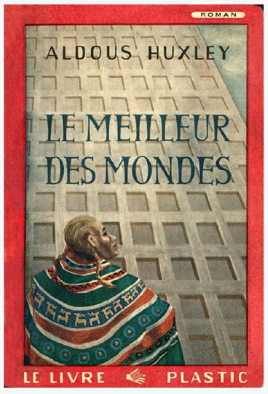
Aujourd'hui, arrestations « préventives » arbitraires et persécution systématisée (allant jusqu'à l'apposition d'un QR code sur la porte des appartements) est le quotidien des Ouïghours… dont un million de ressortissants sont aujourd'hui incarcérés en « camp d'études ».

Système à vendre !
Le système chinois est à vendre[28] et **plus de 60 pays** s'étaient déjà portés acquéreurs en 2019.
Des systèmes de surveillance des médias sociaux se vendent aussi très bien[29]...

Toute ressemblance...

« La dictature parfaite serait une dictature qui aurait les apparences de la démocratie, une prison sans murs dont les prisonniers ne songeraient pas à s'évader. Un système d'esclavage où, grâce à la consommation et au divertissement, les esclaves auraient l'amour de leur servitude... »

Erronément attribué à Aldous Huxley dans « Le Meilleur des mondes » 1932.
Il s'agirait d'un résumé du livre rédigé par un des éditeurs de l'ouvrage.



A découvrir :

- Un excellent article[34] de John Thomas sur l'**addiction au smartphone**, utilisée scientifiquement par les entreprises technologiques (voir lien 34 en dernière page).
- « **Tous surveillés** »[35], reportage vidéo d'Olivier Tesquet (A voir ! Source n° 35).
- Excellent site de suivi de la démocratie : https://freedomhouse.org/

Demain chez nous ?

Les lanceurs d'alertes déjà cités[12] (W. Binney, ex-directeur technique NSA et T. Drake, analyste US Army) avertissent que **tout est en place** dans bon nombre de pays **pour basculer facilement dans un état totalitaire et policier**. Seuls les dirigeants politiques font la différence. Le système chinois pourrait donc devenir assez rapidement une réalité répandue, d'autant qu'il se vend bien.

Que manque-t-il ?
Les databases et les images sont disponibles, il manque donc juste un système de **localisation**.

- **Le tracking téléphonique : déjà en place !**
  Avec la pandémie du Covid-19, des autorités ont proposé d'utiliser une application de tracking sur les téléphones, à installer de façon volontaire par les utilisateurs.

  Mais en Belgique, l'État a fait appel aux données des opérateurs téléphoniques pour mesurer les déplacements et le respect du confinement[30]. **Sans application ni accord** de l'utilisateur !

  Les données étaient anonymisées mais une petite loi d'exception pourrait régler ce « détail ». Si un petit pays comme la Belgique en dispose, cette technologie est bien sûr active ailleurs.

  Il faut savoir que **bon nombre de smartphones[44] ont des backdoors d'origine, à la construction**, permettant l'accès à l'entièreté du téléphone, sms, conversations, localisation...

- **Les caméras**
  Elles fonctionnent en permanence, contrairement au téléphone. Il faut juste les installer.

- **Un réseau de transmission**
  La reconnaissance faciale à grande échelle demande une infrastructure capable de transmettre de nombreuses images à grande vitesse…

  Autrement dit... **un réseau 5G**.

  - Un réseau terrestre : dans nombre de pays, ce déploiement est **imposé**. Aux USA, on parle de « Smart Cities »[31] : les villes du futur, hyper connectées avec les « avantages » en découlant.

    Pour éviter toute opposition au « progrès », la réglementation de **la FCC** (Federal Communications Commission) **interdit aux villes américaines de s'opposer au déploiement** pour des raisons de santé : elles ne peuvent émettre que des soucis d'esthétique ou pratiques de placement des équipements[31].
  - L'Europe publie (juin 2020) qu'il importe de lutter "contre les allégations fallacieuses (sic) selon lesquelles ces réseaux (5G) constitueraient une menace pour la santé" [33].
  - Un réseau satellitaire : 20.000 satellites sont en cours de déploiement[32]. Sans réseau terrestre, ils permettent néanmoins les opérations de base d'un téléphone, dont la localisation et donc de se passer des caméras si le téléphone est allumé.

- **Des éléments localisables**
  Le rêve pour un régime autoritaire ou sécuritaire serait de pouvoir marquer les individus. Une cerise sur le gâteau serait de pouvoir ensuite les repérer à distance.

  La puce RFID est souvent citée. La technique équipe des milliers d'animaux de compagnie et quelques humains aussi[32] ! Toutefois, ces puces RFID ne peuvent être lues que par un **lecteur disposé à proximité immédiate.** Elles sont aussi trop grandes pour être inoculées à l'insu du porteur.

  Il faut donc se tourner vers les **nanopuces** comme celles développées par IBM[38] ou les **nanotatouages** développés par le MIT et implémentables par exemple via un **vaccin**[39].

En conclusion…

Il y a donc tout lieu de s'interroger sur notre futur.

La face noire du numérique nous menace et **nos libertés pourraient rapidement devenir un souvenir**. L'histoire est un éternel recommencement.. mais on pourrait franchir une étape encore inédite : aujourd'hui, **les Etats possèdent les profils complets de la plupart des citoyens**.

Hitler avait annoncé son programme dès la fin des années vingt… Lois après lois, règlements après règlements, les libertés des Juifs furent réduites peu à peu, dans l'indifférence quasiment totale, l'inaction de la communauté internationale et le refus de croire chaque fois que cela irait « plus loin ».

Les Juifs se sont aussi fait recenser, sur base volontaire, auprès des autorités, un peu comme les Ouïghours il y a peu… Et en novembre 1938, la « Nuit de Cristal » les as rattrapés : plus de 32.000 personnes furent déportées ou assassinées. La suite de l'histoire, ce fut Auschwitz…

Restons vigilants à tout ce qui se passe !

La manipulation de l'opinion aux fins électorales, la censure sous toutes ses formes, le piratage de données, la reconnaissance faciale, la 5G, le tracking, la pensée unique...

Cette crise du Covid montre en filigrane la puissance de l'OMS et pourrait amener toutes sortes de décisions arbitraires sous couvert d'urgence sanitaire.

Il y a énormément de signes préoccupants pour la démocratie.

La porte de la cage dorée numérique dans laquelle nous nous trouvons est encore ouverte mais cela pourrait changer au moindre coup de vent...

Vous trouverez encore ci-après une première série de pistes pour sortir de cette cage. Cela demande un effort, de déranger un peu les habitudes et le confort quotidien… Mais le choix est encore possible... pour le moment.

Nos ancêtres ont donné leur sang et leur vie pour que l'on puisse vivre libres. Le petit effort nécessaire de la part nos générations est peu de chose en regard de leurs sacrifices !

Faites-vous aider au besoin !

Bon anonymat !

> **La seule chose qui permet au mal de triompher est l'inaction des hommes de bien.**
>
> Edmund Burke

Pistes pour tenter de sauver la vie privée…

N.B. : en règle générale, toute entreprise américaine est liée au Patriot Act et à la divulgation et / ou espionnage de ses données. En France, on est sur la même voie avec la LPM. Prudence donc !

6 étapes faciles à faire en urgence !

1. Utiliser des mots de passe plus sûrs !!!

Un mot de passe sûr doit répondre à ces règles : 12 caractères minimum, lettres majuscules-minuscules, chiffres, caractères spéciaux, pas de mots d'une langue existante (voir lien 45 !).

Et différent (si si !!) sur chaque application car un mot de passe craqué est immédiatement testé sur les autres applis ! Stocker les mots de passe en sécurité : KeyPassXC (https://keepassxc.org/)

2. Prendre un compte mail chez un fournisseur qui ne lit-donne pas vos mails !

Fini les @outlook.com, @hotmail.com, @gmail.com, @yahoo...

- **protonmail.com**, société suisse (https://protonmail.com/fr/).
  Elle propose une solution de cryptage des mails, automatique entre utilisateurs @protonmail.com mais qui permet aussi le cryptage vers les autres destinataires ! Ceux-là recevront un mail avec un lien vers un site sécurisé pour lire leur message et y répondre de façon sécurisée avec le mot de passe qu'on leur aura donné via un canal sûr !
  Gratuit en webmail et 500 mega. Sinon 48 € / an, en IMAP et un VPN inclus. Applis smartphone disponibles. Une dépense largement rentable **!**
- **tutanota.com**, société allemande (moins sûr que la Suisse), énergie 100 % verte. Moins cher - offres gratuites et payante (12 € ou 48 € par an). Fonctionnalités similaires à Proton Mail.

3. Une messagerie full-sécurisée sur le téléphone !

Terminé les Whatsapp et autres Messenger !
(Whatsapp est crypté mais donne ses données à Facebook (voir ses « Terms & Conditions » !)

- L'appli **Signal** (https://www.signal.org/fr/), sur PC, Android et iPhone.
  Textos, photos, voix, vidéo… comme Whatsapp ! (choix de Snowden :-))

  Similaire à Telegram mais considéré comme supérieur à ce dernier car il utilise des protocoles ouverts, ce qui signifie que les experts peuvent voir le code et le valider, contrairement à Telegram dont le cryptage est propriétaire et ne peut être vérifié. De plus, le cryptage de Telegram n'est pas activé par défaut et il est fréquemment ciblé par diverses autorités qui font pression sur lui.

4. Naviguer sur Internet sans laisser de traces !

- **TOR**, qui permet de surfer en étant anonyme : https://www.torproject.org/fr
  Avec certains moteurs de recherche, vous pouvez simuler l'origine (le pays) des demandes. **Disponible sur PC, Mac, Android et iPhone !**

5. La vidéoconférence sans espionnage

On oublie Skype, Teams, Messenger et même Zoom[42] (faux cryptage !)

- **Jitsi**, (meet.jit.si, www.infomaniak.com/fr/meet/)
  Le seul garanti confidentiel, sur smartphone (appli) et PC (web)

6. Utiliser des moteurs de recherche qui ne censurent pas !

Un web sans censure ? Il y a d'autres moteurs que Google !

- **duckduckgo.com ecosia.org lilo.org ecogine.org qwant.com…**

Pour aller plus loin...

Travail collaboratif sans Google Doc

- **CryptPad** (https://cryptpad.fr)
  Complètement anonyme et fichiers encryptés

Utiliser des logiciels open-source

Logiciels souvent gratuits et dont le code est vérifié :

- L'excellent **LibreOffice** (libreoffice.org) pour remplacer Word, Excel, Powerpoint...
  Tout aussi puissant. Si vous n'utilisez pas de macros, aucun souci (sinon il faut les reprogrammer avec l'un des 5 langages proposés)
- Une mine d'or de logiciels : **Framalibre** : framalibre.org
- Sur téléphone : charger des applis libres via F-Droid https://f-droid.org/
- Messagerie **Thunderbird** (https://www.thunderbird.net/fr/) en Windows-Mac-Linux
  Avec l'extension « Enigmail » pour encrypter ses mails en PGP (utilisateur averti !)
- **Messagerie K-9 Mail** sur Android, avec OpenKeyChain pour le PGP
- Navigateur Web : Firefox (https://www.mozilla.org/fr/firefox/new/), avec les extensions Ublock-Origin, HTTPS- Everywhere, ADBlock Plus…
- Infos que je donne à l'extérieur : https://lehollandaisvolant.net/tout/tools/browser/
  Vérifier son firewall : http://www.inoculer.com/scannerdeports.php
  Tests ports : https://www.grc.com/x/ne.dll?bh0bkyd2, https://www.whatsmyip.org/port-scanner/

Encrypter ses fichiers confidentiels

- Encrypter des fichiers ou des répertoires : **VeraCrypt** (veracrypt.fr)

Pour les plus aguerris

- Lâchez Facebook pour **Diaspora** (https://diaspora-fr.org/) et https://diasporafoundation.org/tutorials
- Migrer vers **Linux** : Ubuntu, Mint, Handy-Linux… (Tails pour l'anonymat complet !).

  Gravez Linux sur DVD, bootez sur le DVD et testez Linux sans modifier à votre machine !

  L'**Agenda du Libre** : des Linuxiens proches de chez vous pour vous aider, souvent gratuitement : https://www.agendadulibre.org
- Smartphone : supprimer Android et y installer un OS libre : contactez un groupe local Linux
- Alternatives aux logiciels et systèmes vulnérables à la surveillance : liste maintenue par Peng Zhong, web-designer japonais : https://prism-break.org/fr/
- D'autres projets : https://degooglisons-internet.org https://www.privacytools.io
  Un projet (coopérative) très prometteur ! : https://www.nubo.coop/fr/
- Guide d'autodéfense numérique (https://guide.boum.org/, https://guide.boum.org/tomes/1_hors_connexions/unepage/#index10h2)
- Cours : https://infokiosques.net/IMG/pdf/InformatiqueSeDefendreEtAttaquer-120pA5-fil.pdf

Sources

1. Conditions Microsoft : https://privacy.microsoft.com/fr-fr/privacystatement
   Conditions Apple: https://www.apple.com/befr/legal/privacy/fr-ww/
   https://www.apple.com/befr/legal/internet-services/icloud/fr/terms.html
   https://www.apple.com/befr/legal/internet-services/itunes/befr/terms.html
   Conditions Google : https://policies.google.com/privacy
   Conditions Yahoo : https://www.verizonmedia.com/policies/ie/fr/verizonmedia/privacy/index.html
2. Patriot Act – Cloud Act : https://www.fincen.gov/resources/statutes-regulations/usa-patriot-act
   https://en.wikipedia.org/wiki/CLOUD_Act
   https://www.msn.com/fr-fr/actualite/monde/le-s%C3%A9nat-des-usa-revoit-le-patriot-act-qui-va-%C3%A9tendre-la-surveillance-num%C3%A9rique-des-am%C3%A9ricains/ar-BB147jv1
3. Foreign Intelligence Surveillance Act
   https://www.intelligence.senate.gov/laws/fisa-amendments-act-2008
4. PRISM : https://www.washingtonpost.com/wp-srv/special/politics/prism-collection-documents/
   https://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data
   https://fr.wikipedia.org/wiki/PRISM_%28programme_de_surveillance%29
5. XKeyscore :
   https://www.lemonde.fr/technologies/article/2013/07/31/l-outil-qui-permet-a-la-nsa-d-examiner-quasiment-tout-ce-que-fait-un-individu-sur-internet_3455916_651865.html
   https://fr.wikipedia.org/wiki/XKeyscore
6. Affaire Snowden : https://fr.wikipedia.org/wiki/R%C3%A9v%C3%A9lations_d%27Edward_Snowden
7. Collaboration des GAFAM
   https://www.lefigaro.fr/international/2013/06/07/01003-20130607ARTFIG00428-l-amerique-d-obama-espionne-aussi-les-communications-internet.php
   https://www.lefigaro.fr/secteur/high-tech/2013/06/09/32001-20130609ARTFIG00159-les-geants-du-web-empetres-dans-des-accusations-d-espionnage.php
   https://www.theguardian.com/world/2013/jul/11/microsoft-nsa-collaboration-user-data
   http://paranoia.dubfire.net/2013/06/analyzing-yahoos-prism-non-denial.html
   https://www.theguardian.com/world/2013/jul/11/microsoft-nsa-collaboration-user-data
   https://www.silicon.fr/collectes-massives-donnees-industrie-savait-nsa-93376.html
8. Loi programmation militaire :
   https://www.defense.gouv.fr/portail/enjeux2/la-lpm-2019-2025/les-actualites2/loi-de-programmation-militaire-2019-2025-textes-officiels
9. Orange et DGSE :
   https://www.lemonde.fr/international/article/2014/03/20/dgse-orange-des-liaisons-incestueuses_4386264_3210.html
10. Clearview :
    https://ici.radio-canada.ca/nouvelle/1482143/clearview-reconnaissance-faciale-police-enquete-new-york-times
    https://en.wikipedia.org/wiki/Clearview_AI
11. Arte – Tous surveillés – 7 milliards de suspects :
    https://www.arte.tv/fr/videos/083310-000-A/tous-surveilles-7-milliards-de-suspects
12. Documentaire Nothing to hide : https://www.youtube.com/watch?v=djbwzEIv7gE
13. Dominique Domenjoud :
    https://www.humanite.fr/moi-joel-domenjoud-militant-assigne-residence-591565
    https://www.francetvinfo.fr/faits-divers/terrorisme/attaques-du-13-novembre-a-paris/etat-d-urgence-en-france/etat-d-urgence-un-militant-ecologiste-assigne-a-residence-en-pleine-cop21-denonce-une-mesure-d-intimidation_1194895.html
14. Hacking :
    https://www.zdnet.com/article/a-hacker-group-is-selling-more-than-73-million-user-records-on-the-dark-web/
    https://en.wikipedia.org/wiki/Yahoo!_data_breaches
15. Cambridge Analytica :
    https://www.sciencesetavenir.fr/high-tech/election-de-trump-facebook-bloque-cambridge-analytica_122162
    https://www.usine-digitale.fr/article/ce-qu-il-faut-savoir-sur-le-scandale-cambridge-analytica-qui-fait-vaciller-facebook.N669244
    https://www.theguardian.com/technology/2018/mar/17/facebook-cambridge-analytica-kogan-data-algorithm?CMP=share_btn_tw
16. Russie : https://www.ouest-france.fr/high-tech/facebook/elections-americaines-facebook-bloque-une-nouvelle-tentative-russe-de-manipulation-de-l-opinion-6575680

17. Bolsonaro : https://www.truthdig.com/articles/brazils-jair-bolsonaro-accused-of-widespread-electoral-fraud/
18. Manipuler l'opinion publique :
    https://www.latribune.fr/opinions/tribunes/manipuler-l-opinion-publique-sur-les-reseaux-sociaux-c-est-possible-794240.html
    https://freedomhouse.org/report/freedom-on-the-net/2019/the-crisis-of-social-media/social-media-surveillance
19. Censure Google : https://en.wikipedia.org/wiki/Censorship_by_Google
    https://www.agoravox.fr/actualites/technologies/article/google-censure-un-nouvel-195960
    https://www.bilan.ch/techno/google-et-autres-reseaux-prives-ont-bien-le-droit-de-censure
20. Google – presse
    https://www.lemonde.fr/actualite-medias/article/2016/11/17/google-finance-de-plus-en-plus-l-innovation-dans-les-medias_5032714_3236.html
    https://www.lemonde.fr/actualite-medias/article/2015/04/28/google-s-allie-avec-huit-medias-europeens-pour-elargir-son-fonds-pour-la-presse_4623776_3236.html
21. Decodex : https://www.lemonde.fr/verification/
22. Reportage Arte : https://www.arte.tv/fr/videos/083310-000-A/tous-surveilles-7-milliards-de-suspects/
23. Reconnaissance :
    https://www.clubic.com/technologies-d-avenir/intelligence-artificielle/actualite-889278-porter-masque-reconnaissance-faciale-chinoise.html
    https://www.01net.com/actualites/coronavirus-la-reconnaissance-faciale-chinoise-fonctionne-desormais-meme-si-vous-portez-un-masque-1873873.html
24. Caméra 500 Mpx : https://www.bfmtv.com/tech/en-chine-une-camera-de-500-millions-de-pixels-peut-reconnaitre-chaque-supporter-dans-un-stade-1777393.html
25. 7 minutes : https://www.bbc.com/news/av/world-asia-china-42248056/in-your-face-china-s-all-seeing-state
26. Surveillance : https://www.liberation.fr/evenements-libe/2019/07/26/surveillance-en-chine-le-pire-du-milieu_1742277
    https://www.lesechos.fr/2018/06/en-chine-14-milliard-de-suspects-sous-surveillance-991913
27. Ouïghours :
    https://www.bbc.com/news/av/world-asia-china-42248056/in-your-face-china-s-all-seeing-state
    https://www.france24.com/fr/20190218-chine-ouighour-surveillance-xinjiang-reconnaissance-faciale-qr-code-musulman
    https://www.lefigaro.fr/international/2017/12/15/01003-20171215ARTFIG00165-chine-la-population-du-xinjiang-fichee-sans-le-savoir.php
28. A vendre : https://korii.slate.fr/tech/chine-exporte-systeme-surveillance-high-tech-equateur
    https://www.nytimes.com/2019/04/24/technology/ecuador-surveillance-cameras-police-government.html?action=click&module=RelatedLinks&pgtype=Article
    https://fr.theepochtimes.com/controle-social-de-big-brother-de-chine-se-rend-australie-826518.html
    https://share.america.gov/fr/la-chine-exporte-ses-outils-de-repression-dans-le-monde/
29. Surveillance sociale : https://freedomhouse.org/report/freedom-on-the-net/2019/the-crisis-of-social-media/social-media-surveillance
30. Tracking téléphonique :
    https://www.rtl.be/info/belgique/societe/coronavirus-en-belgique-vos-deplacements-ont-ete-analyses-depuis-le-confinement-voici-le-resultat-1208291.aspx
    https://www.proximus.be/fr/id_b_cl_data_against_corona_taskforce/entreprises-et-secteur-public/blog/news-blog/innovation/data-against-corona-taskforce.html
    https://www.ehealth.fgov.be/fr/esante/task-force-data-technology-against-corona/le-role-de-la-task-force-data-technology-against-corona
31. 5G au sol – USA :
    https://www.nlc.org/sites/default/files/2018-08/CS_SmallCell_MAG_FINAL.pdf
32. 5G par satellites :
    https://www.01net.com/actualites/grace-a-la-5g-votre-futur-smartphone-pourrait-se-connecter-a-des-satellites-1477905.html
    https://www.technocracy.news/5g-from-space-20000-satellites-to-blanket-the-earth/
    https://worldhealth.net/news/thousands-satellites-set-launch-5g/
33. 5G et conseil de l'Europe:
    https://data.consilium.europa.eu/doc/document/ST-8711-2020-INIT/fr/pdf
34. Smartphone : https://healthimpactnews.com/2018/how-big-technology-companies-control-the-minds-of-the-masses-through-smart-phone-addiction/
35. Tous surveillés : https://www.rts.ch/info/monde/11124527--sur-internet-la-surveillance-devient-imperceptible-.html
36. Statistiques recherches : https://www.webrankinfo.com/dossiers/etudes/parts-marche-moteurs

37. Facebook -Monde : https://www.valeursactuelles.com/societe/facebook-paie-le-monde-et-ses-decodeurs-pour-traquer-les-fake-news-92092
38. Nanopuce IBM : https://www.newsweek.com/worlds-smallest-nano-chip-will-double-processing-power-smartphones-330062
39. Vaccin tatouage :
https://stm.sciencemag.org/content/11/523/eaay7162
https://www.lemonde.fr/afrique/article/2019/12/19/le-kenya-et-le-malawi-zones-test-pour-un-carnet-de-vaccination-injecte-sous-la-peau_6023461_3212.html
40. Le Monde financé par Gates : https://www.gatesfoundation.org/how-we-work/quick-links/grants-database?fbclid=IwAR3fcYgVIGJrcfhzyftpIWXfrY5GhAX3X70CmUoUd-wVF-qusMEEwA_msjQ#q/k=le%20monde&program=Global%20Policy%20%26%20Advocacy
41. Réseau Cochrane 2018 : https://www.lessymboles.com/menace-sur-lindependance-des-scientifiques-bill-gates-rachete-cochrane/
42. Zoom -Cryptage - Facebook https://theintercept.com/2020/03/31/zoom-meeting-encryption/
https://www.vice.com/en_us/article/z3b745/zoom-removes-code-that-sends-data-to-facebook
43. Espionnage mondial : http://www.alterinfo.net/Trump-signe-une-loi-autorisant-l-espionnage-de-masse-sur-les-citoyens-americains_a136128.html
44. Backdoors sur smartphone : https://ciso.economictimes.indiatimes.com/news/most-smartphone-apps-have-backdoor-secrets-for-hackers-researchers/74931801
https://thehackernews.com/2016/11/hacking-android-smartphone.html
https://www.bleepingcomputer.com/news/security/chinese-backdoor-still-active-on-many-android-devices/
45. Mot de passe : https://www.youtube.com/watch?v=Z8nGpUOQPaA
46. Yahoo : https://www.cnetfrance.fr/news/yahoo-espionne-ses-utilisateurs-pour-les-autorites-americaines-39842876.htm