

La cage se referme...

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

- **Qu'avez-vous réellement accepté en cliquant < OK > la 1^{ère} 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 !

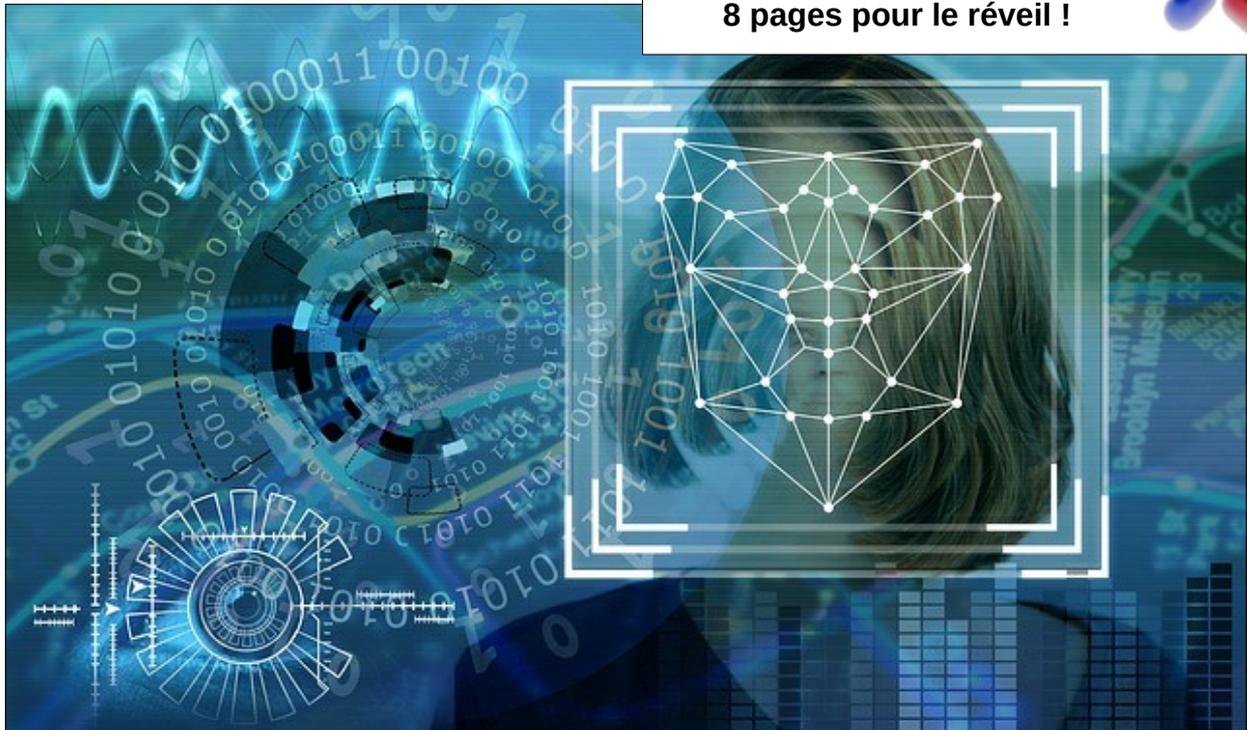


Table des matières

Tout était parfait dans le meilleur des monde	p. 1	Sources et liens	p. 12
Données personnelles ?	p. 2		
Qui possède les données ?	p. 3	<u>Annexes</u>	
Je n'ai rien à cacher	p. 4	termes_conditions_Microsoft.pdf	(5 pages)
Manipulation de l'opinion	p. 5	termes_conditions_Google.pdf	(4 pages)
La Chine aujourd'hui	p. 6	termes_conditions_Facebook.pdf	(7 pages)
Demain chez nous ?	p. 7	termes_conditions_Apple.pdf	(6 pages)
En conclusion	p. 8	termes_conditions_Yahoo.pdf	(3 pages)
Essayer de sauver la vie privée...	p. 9		

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 originaux¹.

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 réseaux 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 Snowden⁶ (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 **légal**, et d'autant plus en vertu des dernières lois approuvées par Donald Trump⁴³.



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 autorités⁷ : 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 ensemble⁹. 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 2020¹⁰). 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 2020¹¹, 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 **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'alertes¹² (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 Domenjoud¹³ 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 Russie¹⁶ 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 WhatsApp¹⁷.
- 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 dynamique¹⁸.
- Une recherche pour un billet d'avion montre que le prix monte à chaque heure...

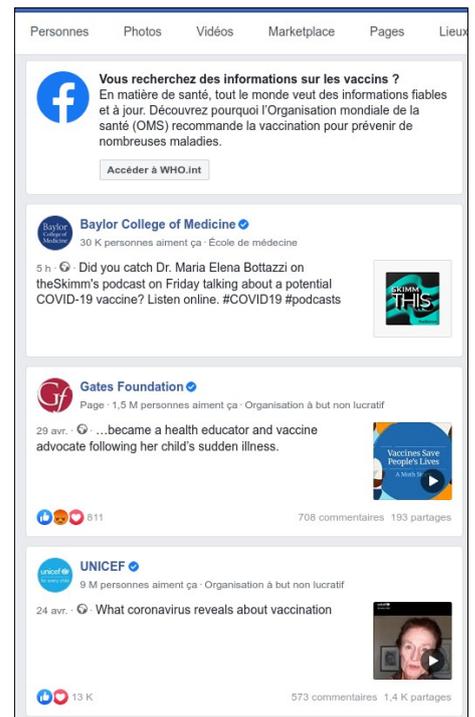
La nouvelle arme de la pensée unique : le bannissement ou la mort digitale !

- **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 1^{er} lieu) reçoit un avertissement avec un lien vers l'OMS, suivi d'une vingtaine de liens (dont plusieurs fois la « Gates Foundation », 1^{er} 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 Russie³⁶) censure¹⁹** 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 publications⁴¹ 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 Chine²². (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, masqués²³, dans une foule²⁴...

Une expérience avec un journaliste a montré qu'un « suspect » avait été appréhendé par les autorités 7 minutes²⁵ 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 citoyens²⁶ (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 santé²⁷, 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 ».

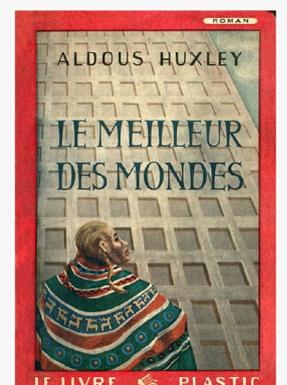
Système à vendre !

Le système chinois est à vendre²⁸ et plus de 60 pays s'étaient déjà portés acquéreurs en 2019. Des systèmes de surveillance des médias sociaux se vendent aussi très bien²⁹...

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... »

Erronéement 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 article³⁴ 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 cités¹² (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 bases 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 confinement³⁰. **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 smartphones⁴⁴ 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 équipements³¹.

- 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 déploiement³². 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 aussi³² ! 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 IBM³⁸ 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 \(https://keepassxc.org/\)](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](https://protonmail.com/fr/), 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 Zoom⁴² (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...](https://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=djwzElv7gE>
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-americales-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-privés-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-ouïghour-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=IwAR3fcYgVIGJrcfhzyftplWXfrY5GhAX3X70CmUoUd-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>

Déclaration de confidentialité Microsoft (extraits)

Applicable à tout produit Microsoft : Windows 10 – Outlook - Hotmail - Office 365 – Skype - LinkedIn *

* Liste complète des logiciels concernés sur :

<https://www.microsoft.com/en-us/servicesagreement/#serviceslist>

Source :

- <https://privacy.microsoft.com/fr-fr/privacystatement> (! Ne pas oublier le lien 'Développer tout' en haut à droite de la page !)

La page web imprimée en PDF fait **102 pages**... Les conditions ont été acceptées par les utilisateurs quand ils ont cliqué < OK >, sous peine de ne pas pouvoir utiliser le produit ou le service.

Beaucoup d'options sont cochées par défaut dans les configurations d'applications et bon nombre d'utilisateurs n'en ont pas conscience ou ne savent pas où les trouver.

Vous trouverez ci-après 5 pages avec les extraits les plus marquants.

Déclaration de confidentialité Microsoft

<https://privacy.microsoft.com/fr-fr/privacystatement>

(...)

Les références aux produits Microsoft dans cette déclaration comprennent les services, les sites web, les applications, les logiciels, les serveurs et les appareils Microsoft.

(...)

Cette déclaration s'applique **aux interactions entre Microsoft et vous-même, aux produits Microsoft** répertoriés ci-dessous, ainsi qu'à d'autres produits Microsoft entraînant l'affichage de cette déclaration.

Les données personnelles que nous recueillons

Microsoft recueille des données que vous lui fournissez dans le cadre de ses interactions avec vous et à travers ses produits (...).

Vous fournissez certaines de ces données directement (...). Nous recueillons également des données vous concernant **auprès de tiers**.

Nous nous appuyons sur diverses raisons et autorisations juridiques (parfois appelées « bases juridiques ») pour traiter les données, **notamment** avec votre consentement, aux fins d'assurer un équilibre entre les **différents centres d'intérêt légitimes**, la nécessité de conclure et d'exécuter des contrats et la conformité aux obligations légales (...).

Nous recueillons également des données reçues de tiers. (...) Ces sources tierces, qui peuvent varier au fil du temps, sont notamment les suivantes :

- (...)
- des services qui rendent accessibles à d'autres personnes des contenus générés par l'utilisateur à partir de leur service, par exemple, (...) **des publications publiques sur des réseaux sociaux**;
- des fournisseurs de services qui nous aident à déterminer la **localisation de votre appareil**
- (...)
- des sources accessibles au public, telles que les **bases de données gouvernementales** ouvertes.

(...)

Les données que nous recueillons peuvent inclure les éléments suivants :

- **Nom et données de contact.** Votre prénom et votre nom de famille, votre adresse e-mail, votre adresse postale, votre numéro de téléphone et d'autres coordonnées similaires.
- (...)
- **Données démographiques.** Données vous concernant telles que votre âge, votre sexe, votre pays et votre langue préférée.
- **Données de paiement.** Données nécessaires au traitement de vos paiements, comme le numéro de votre instrument de paiement (par exemple, un **numéro de carte de crédit**) et le **code de sécurité** associé à celui-ci.
- **Interactions.** Données sur votre utilisation des produits Microsoft. Dans certains cas, comme les requêtes de recherche, il s'agit des données que vous fournissez pour utiliser les produits.

- Autres exemples de données d'interactions :
 - **Données sur l'appareil et l'utilisation.** Données sur votre appareil et les produits et les fonctionnalités que vous utilisez, notamment des **informations sur votre matériel et vos logiciels**, les performances de nos produits, ainsi que vos paramètres.
Par exemple :
 - **Données sur les articles** que vous achetez et les activités liées à votre compte.
 - **Parcourir l'historique.** Données sur les pages web que vous visitez.
 - **Données sur l'appareil, la connectivité et la configuration.** Données sur votre appareil, la configuration de votre appareil **et les réseaux situés à proximité.**
Par exemple, **les données sur les systèmes d'exploitation et les autres logiciels installés sur votre appareil, y compris les clés de produit.** Également les adresses IP, les identificateurs des appareils (tels que le numéro IMEI pour les téléphones), les paramètres régionaux et linguistiques, ainsi que les informations sur les points d'accès WLAN situés à proximité de votre appareil.
 - (...)
- **Centres d'intérêt et favoris.** Données sur vos centres d'intérêt et vos favoris, comme les équipes de sport que vous soutenez, vos langages de programmation préférés, les actions que vous suivez ou les villes que vous ajoutez à un suivi de la météo ou du trafic.
En plus de ceux que vous avez explicitement fournis, vos centres d'intérêt et vos favoris peuvent également être devinés ou dérivés d'autres données que nous recueillons.
- **Données de consommation de contenu.** Informations sur les contenus multimédias (par exemple, TV, vidéo, musique, audio, livres électroniques, applications et jeux) auxquels vous accédez par le biais de nos produits.
- **Commandes et recherches.** Vos commandes et vos requêtes de recherche lorsque vous utilisez des produits Microsoft dotés de fonctionnalités de recherche ou de productivité.
- (...)
- **Données de SMS, d'entrée manuscrite et de frappe.** Données de SMS, d'entrée manuscrite, de frappe et informations associées. Par exemple, lorsque nous recueillons des données d'entrée manuscrite, nous recueillons des informations sur l'emplacement de votre instrument d'entrée manuscrite sur votre appareil.
- **Images.** Images et informations associées, telles que les métadonnées d'une image. Par exemple, nous recueillons l'image que vous fournissez lorsque vous utilisez un service Bing prenant en charge les images.
- **Contacts et relations.** **Données concernant vos contacts et vos relations** si vous utilisez un produit permettant de partager des informations avec d'autres, de gérer vos contacts, de communiquer avec d'autres personnes ou d'améliorer votre productivité.
- **Données sociales.** Informations sur vos relations et interactions avec d'autres personnes ou des organisations, comme vos types d'engagement (par exemple, ce que vous aimez ou non, les événements qui vous intéressent, etc.) liés à des personnes ou des organisations.
- **Données de localisation.** Données concernant la localisation de votre appareil, qui peuvent être soit précises soit imprécises. Par exemple, nous recueillons des données de localisation à l'aide d'un système mondial de navigation par satellite (GNSS) (par exemple, GPS), ainsi que des données concernant les antennes-relais de téléphonie mobile et les points d'accès Wi-Fi situés à proximité. La localisation peut également être dérivée de l'adresse IP d'un appareil ou des données de votre profil de compte qui indiquent avec moins de précision où il se trouve. Il peut notamment s'agir d'une ville ou d'un code postal.
- (...)
- **Contenu.** **Contenu** des fichiers et des communications que vous entrez, chargez, recevez, créez et contrôlez. Par exemple, si vous transmettez un fichier à l'aide de Skype à un autre utilisateur Skype, nous devons recueillir le contenu de ce fichier pour l'afficher sur votre écran et celui de l'autre utilisateur. Si vous recevez un e-mail en utilisant Outlook.com, nous devons recueillir le **contenu** de cet e-mail afin de le déposer dans votre boîte de réception (...)

Autres contenus que nous recueillons lorsque nous vous fournissons des produits :

- Communications, y compris les contenus audio, vidéo ou texte (saisis, manuscrits, dictés ou autres) figurant dans un message, un courrier électronique, un appel, une demande de réunion ou une conversation.
- Photos, images, morceaux, films, logiciels et autres média ou documents que vous stockez, récupérez ou traitez avec notre cloud.

(...)

Comment nous utilisons les données personnelles

(...)

Nous utilisons également les données pour mener nos activités, (...) nous conformer à nos obligations légales, (...) et effectuer des recherches.

(...) **nous combinons les données** que nous recueillons dans différents contextes (...) Cependant, nous avons intégré des dispositifs de protection technologiques et procéduraux, conçus pour empêcher certaines combinaisons de données si la loi l'exige. (...)

Notre traitement de données personnelles à ces fins inclut à la fois des méthodes de traitement automatisées et manuelles (humaines). (...). Pour (...) améliorer la précision de nos méthodes de traitement automatisées (notamment l'IA), nous examinons manuellement certaines des prédictions et déductions. (...). Par exemple, nous examinons manuellement les extraits de code courts d'un petit échantillon de données vocales. Nous avons suivi des étapes pour empêcher l'identification afin d'améliorer nos services vocaux, tels que la reconnaissance et la traduction.

Lorsque nous traitons des données personnelles vous concernant, nous le faisons avec votre consentement et/ou car nous en avons besoin (...) pour (...) respecter nos obligations contractuelles et légales, protéger la sécurité de nos systèmes et de nos clients, ou pour satisfaire d'autres intérêts légitimes de Microsoft, tel qu'indiqué dans cette section et dans la section Raisons pour lesquelles nous partageons vos données personnelles de la présente déclaration de confidentialité.

(...)

En savoir plus sur les finalités de traitement :

- (...)
- Sécurité. Nous utilisons les données pour protéger la sécurité de nos produits et de nos clients. (...) **certains de nos produits, tels qu'Outlook ou OneDrive, analysent systématiquement le contenu** (...) pour identifier (...) les URL qui ont été signalées comme frauduleuses (...). Nous nous réservons le droit de bloquer une communication ou de supprimer du contenu si ces derniers enfreignent les conditions générales.
- Mises à jour. (...) nous pouvons utiliser des informations sur les fonctionnalités de votre appareil, telles que la mémoire disponible, pour vous fournir une mise à jour de logiciel ou un correctif de sécurité.
- (...)
- **Nous pouvons utiliser des processus automatisés pour détecter et faire en sorte d'empêcher les activités** qui violent nos droits et ceux de tiers, telles que les fraudes.

Raisons pour lesquelles nous partageons vos données personnelles

Nous partageons vos données personnelles avec votre accord **ou** si celles-ci sont nécessaires pour effectuer une transaction ou pour fournir un produit que vous avez demandé ou autorisé.

(...)

En outre, **nous partageons des données personnelles parmi les filiales contrôlées par Microsoft**. Nous partageons également des données personnelles avec les prestataires et agents travaillant en notre nom aux fins décrites dans la présente déclaration.

(...)

Enfin, **nous conserverons, accèderons à, transférerons, divulguons et préserverons les données personnelles, notamment vos contenus (comme le contenu de vos e-mails dans Outlook.com, ou des fichiers de dossiers privés dans OneDrive), lorsque nous pensons de bonne foi qu'il est nécessaire de le faire** pour effectuer l'une des actions suivantes :

- lorsque cela est exigé par la loi en vigueur ou pour répondre à des requêtes légales valides, notamment celles émanant des organismes d'application de la loi **et d'autres organismes gouvernementaux** ;
- **pour protéger nos clients**, pour éviter le courrier indésirable ou les tentatives d'escroquer des utilisateurs de nos produits, ou pour empêcher les pertes de vie ou des blessures graves ;
- (...)

Pour plus d'informations sur les données que nous divulguons en réponse aux requêtes des agences d'application de la loi ou d'autres agences gouvernementales, consultez notre Rapport des demandes d'application de la loi. (<https://www.microsoft.com/en-us/corporate-responsibility/law-enforcement-requests-report>)

(...)

Cookies et technologies similaires

Microsoft utilise des cookies **et des technologies similaires** à diverses fins, en fonction du contexte ou du produit, dont :

(...)

- **Sécurité**. Nous utilisons des cookies pour traiter les informations qui nous permettent de sécuriser nos produits, ainsi que de détecter les fraudes et les abus.
- Stockage des informations que vous fournissez à un site web. Nous utilisons des cookies pour mémoriser les informations que vous avez partagées.
- Réseaux sociaux. Certains de nos sites Web incluent les cookies de réseaux sociaux, **notamment ceux qui permettent aux utilisateurs s'étant connectés sur le service de réseaux sociaux de partager du contenu** via ce service.

(...)

Pays de stockage et de traitement des données personnelles

Nous transférons des données personnelles issues de l'Espace économique européen, du Royaume-Uni et de Suisse **vers d'autres pays, dont certains n'ont pas encore été reconnus par la Commission européenne comme offrant un niveau de protection adéquat des données**.

Par exemple, **leurs lois peuvent ne pas vous garantir les mêmes droits, ou il est possible qu'il n'y ait pas d'autorité de contrôle en matière de protection des données personnelles** capable de traiter vos plaintes.

OneDrive

Lorsque vous utilisez OneDrive, nous recueillons des données sur votre utilisation du service, ainsi que **sur le contenu que vous stockez**, pour fournir, améliorer et protéger les services

Outlook

Outlook.com est le principal service de messagerie grand public de Microsoft. Il comporte des comptes de messagerie avec des adresses qui se terminent par **outlook.com, live.com, hotmail.com et msn.com**.

LinkedIn (<https://www.linkedin.com/legal/privacy-policy>)

(...)

Nous utilisons également une **technologie d'analyse automatique des messages** pour aider et protéger notre site. Par exemple, nous utilisons cette technologie pour suggérer des réponses aux messages et pour gérer ou bloquer du contenu en violation avec nos Conditions générales d'utilisation ou nos Politiques de la communauté professionnelle sur nos Services.

(...)

Nous partagerons vos données personnelles avec nos sociétés affiliées dans le cadre de la prestation et du développement de nos Services. **Nous pouvons regrouper les informations** en interne sur les différents Services couverts par cette Politique de confidentialité pour aider nos Services à être plus pertinents et utiles pour vous et les autres.

(...)

3.6. Divulgations légales

Nous devons éventuellement partager vos données si nous pensons y être obligés par la loi **ou** pour garantir nos droits et notre sécurité, ainsi que les vôtres et ceux des tiers.

Il est possible que nous devions divulguer des informations vous concernant lorsque nous y sommes tenus par la loi, en cas d'injonction ou de toute autre mesure judiciaire, **ou si nous croyons en toute bonne foi** qu'une telle divulgation est raisonnablement nécessaire pour (1) enquêter sur des activités illégales avérées ou suspectées, empêcher de telles activités ou prendre des mesures à leur rencontre, ou assister les institutions judiciaires ; (2) faire respecter nos contrats avec vous ; (3) enquêter sur des allégations et plaintes de tiers, et nous en défendre ; (4) garantir la sécurité ou l'intégrité de nos Services (par exemple, par un partage avec des entreprises faisant face aux mêmes menaces).

(...)

Windows

(...)

Afin de vous fournir cette expérience informatique, **nous recueillons des données sur vous**, votre appareil, et votre manière d'utiliser Windows

Historique d'activités

L'historique d'activités aide à assurer **le suivi des choses que vous faites sur votre appareil, par exemple des applications et services que vous utilisez, des fichiers que vous ouvrez et des sites web que vous consultez**. (...)

Si vous ouvrez une session sur votre appareil avec un compte Microsoft et que vous accordez votre autorisation, Windows envoie votre historique d'activités à Microsoft. (...)

L'historique d'activités est également créé et envoyé à Microsoft lorsque vous utilisez certaines applications Microsoft, **telles que Microsoft Edge** et des applications Office telles que Word, Excel et PowerPoint sur des appareils mobiles tels que des téléphones et tablettes iOS et Android. (...)

Vous pouvez activer ou désactiver les paramètres d'envoi de votre historique d'activités à Microsoft et de stockage local de l'historique sur l'appareil.

(...)

Confidentialité & conditions d'utilisation - Google

Applicable à tout produit Google : Google – Gmail – Google Drive – Android – YouTube *

* Liste complète des logiciels concernés sur : <https://about.google/intl/fr/products/?tab=wh>

Source :

- <https://policies.google.com/privacy>

La page web imprimée en PDF fait **43 pages**... Les conditions ont été acceptées par les utilisateurs quand ils ont cliqué < OK >, sous peine de ne pas pouvoir utiliser le produit ou le service.

Beaucoup d'options sont cochées par défaut dans les configurations d'applications et bon nombre d'utilisateurs n'en ont pas conscience ou ne savent pas où les trouver.

Vous trouverez ci-après 4 pages avec les extraits les plus marquants.

Règles de confidentialité et conditions d'utilisation (extraits)

<https://policies.google.com/privacy>

(...)

INFORMATIONS COLLECTÉES PAR GOOGLE

(...) Il peut s'agir d'informations de base, telles que la langue que vous utilisez, ou plus complexes, comme **les annonces que vous trouvez les plus utiles, les personnes qui vous intéressent le plus sur le Web ou les vidéos YouTube** qui sont susceptibles de vous plaire.

(...)

Lorsque vous n'êtes pas connecté à un compte Google, **nous stockons les informations collectées en les associant à des identifiants uniques liés au navigateur**, à l'application ou à l'appareil que vous utilisez.

(...)

Lorsque vous êtes connecté à votre compte, **nous stockons les informations collectées en les associant à votre compte Google** et les considérons comme des informations personnelles

Éléments que vous créez ou que vous nous fournissez

Lorsque vous créez un compte Google, vous nous fournissez des informations personnelles, dont votre nom et un mot de passe. Vous avez également la possibilité d'ajouter un numéro de téléphone ou des informations de paiement à votre compte. Même si vous n'êtes connecté à aucun compte Google, vous pouvez nous fournir des informations, telles qu'une adresse e-mail afin de recevoir des notifications relatives à nos services.

Nous collectons également le **contenu que vous créez, importez ou recevez de la part d'autres personnes via nos services**. Cela inclut par exemple **les e-mails que vous écrivez ou recevez, les photos et vidéos que vous enregistrez, les documents et feuilles de calcul que vous créez**, ainsi que les commentaires que vous rédigez sur YouTube.

Informations que nous collectons via nos services

Vos applications, navigateurs et appareils

(...)

Les informations que nous collectons incluent les **identifiants uniques, le type et les paramètres du navigateur, le type et les paramètres de l'appareil, le système d'exploitation, des données relatives au réseau mobile** (telles que le nom de l'opérateur et le numéro de téléphone) et le numéro de version de l'application.

Nous recueillons aussi des informations relatives **aux interactions entre vos applications, vos navigateurs, vos appareils et nos services**, telles que l'adresse IP, les rapports d'erreur, l'activité du système, ainsi que la date, l'heure et l'URL de provenance de votre demande.

(...)

Si vous utilisez un appareil **Android** sur lequel des applications Google sont installées, votre appareil contacte régulièrement les serveurs Google afin de nous fournir **des informations relatives à votre appareil et aux connexions à nos services, telles que le type d'appareil que vous utilisez, le nom de l'opérateur, des rapports d'erreur et les applications que vous avez installées**.

Votre activité

Nous collectons des informations relatives à votre activité au sein de nos services. (...) Les informations relatives à votre activité que nous recueillons peuvent inclure les éléments suivants :

- Les **termes** que vous recherchez.
- Les **vidéos** que vous regardez.
- Vos **vues de contenu et d'annonces** ainsi que vos interactions avec ces derniers.
- Des informations audio et vocales lorsque vous utilisez des fonctionnalités audio.
- L'activité relative aux achats.
- **Les personnes avec lesquelles vous communiquez ou partagez du contenu.**
- **L'activité sur des applications et sites tiers qui utilisent nos services.**
- L'historique de navigation Chrome que vous avez synchronisé avec votre compte Google.

Si vous avez recours à nos services pour passer et recevoir des appels ou pour envoyer et recevoir des messages, nous sommes susceptibles **de collecter des informations relatives aux communications téléphoniques, comme votre numéro de téléphone, celui de l'émetteur, celui du destinataire, les numéros de transfert, l'heure et la date des appels et des messages, la durée des appels, les données de routage et les types d'appels.**

Informations relatives à votre position géographique

Nous collectons des informations relatives à votre position géographique lorsque vous utilisez nos services (...).

Votre position géographique peut être déterminée avec des degrés de précision différents à l'aide des éléments suivants :

- Le GPS
- Adresse IP
- Les données des capteurs de votre appareil
- Des informations relatives à des éléments à proximité de votre appareil, tels que des points d'accès Wi-Fi, des antennes-relais et des appareils sur lesquels le Bluetooth est activé

Dans certains cas, **nous collectons également des informations vous concernant dans des sources accessibles publiquement.** (...) Nous pouvons également **recueillir des informations vous concernant auprès de partenaires de confiance, (...) des partenaires de sécurité** qui nous fournissent des données afin que nous puissions assurer une protection contre les abus.

(...)

Nous avons recours à plusieurs technologies pour collecter et stocker des informations, notamment les cookies, les tags de pixel, les éléments stockés en local (tels que le stockage sur les navigateurs Web ou les caches de données d'application), les bases de données et les fichiers journaux de serveur.

Les données nous permettent de concevoir des services de meilleure qualité

(...)

- les termes que vous avez recherchés

(...)

- la façon dont les utilisateurs organisaient leurs photos dans Picasa

(...)

- Le service Google Play exploite quant à lui des informations, telles que les applications que vous avez déjà installées et les vidéos que vous avez regardées sur YouTube

(...)

Sauf demande expresse de votre part, nous ne partageons pas d'informations qui permettent de vous identifier

(...)

Protéger Google, nos utilisateurs et le public

(...)

Nous utilisons **des systèmes automatiques qui analysent votre contenu**

(...)

Par ailleurs, nous avons recours à des algorithmes pour détecter des structures dans les données.

(...)

Nous pouvons **combinaison des informations** que nous collectons via nos services et sur vos appareils aux fins décrites ci-dessus.

(...)

Votre activité sur d'autres sites et dans d'autres applications peut être associée à vos informations personnelles

(...)

Si d'autres utilisateurs disposent déjà de votre adresse e-mail, ou de toute autre donnée permettant de vous identifier, **nous sommes susceptibles de leur montrer les informations de votre compte Google disponibles publiquement,**

Lorsque Google partage vos informations

(...)

Pour des besoins de traitement externe

Nous transmettons des informations personnelles à nos sociétés affiliées et autres sociétés ou personnes de confiance qui les traitent pour notre compte, selon nos instructions, conformément aux présentes Règles de confidentialité et dans le respect de toute autre mesure appropriée de sécurité et de confidentialité.

Pour des raisons juridiques

Nous ne partagerons des informations personnelles avec des personnes tierces que **si nous pensons en toute bonne foi** que l'accès, l'utilisation, la protection ou la divulgation de ces informations est raisonnablement justifiée pour effectuer les opérations suivantes :

- **Se conformer à des obligations légales, réglementaires, judiciaires ou administratives.**
(...)
- (...)
- **Décerner**, éviter ou traiter des activités frauduleuses, des atteintes à la sécurité ou tout problème d'ordre technique.
- **Se prémunir contre toute atteinte aux droits, aux biens ou à la sécurité de Google**, de ses utilisateurs ou du public, en application et dans le respect de la loi.

(...) Nous autorisons également des partenaires spécifiques à utiliser leurs propres cookies ou technologies similaires pour collecter des informations contenues dans votre navigateur ou dans votre appareil à des fins publicitaires et d'évaluation.

La sécurité fait partie intégrante de nos services en vue de protéger vos informations

Tous les produits Google intègrent de puissantes fonctionnalités de sécurité qui protègent vos informations en continu. Les renseignements que nous collectons via nos services nous permettent de **détecter et de bloquer automatiquement les menaces** qui pèsent sur votre sécurité. (...)

(...)

L'accès aux informations personnelles est strictement réservé aux employés, **sous-traitants** et agents de Google qui ont besoin d'y accéder afin de les traiter en notre nom.

Transferts de données

(...) Il est donc possible que **vos informations soient traitées par des serveurs situés en dehors de votre pays de résidence. Les lois sur la protection des données varient en fonction des pays. Dans certains pays, les données sont mieux protégées que dans d'autres.**

(...)

Lorsque nous défendons des intérêts légitimes

Nous traitons vos informations conformément à nos intérêts légitimes, ainsi qu'à ceux de tiers (...).

Cela signifie que nous traitons vos informations notamment pour effectuer les opérations suivantes :

- (...)
- (...) Nous pouvons par exemple **divulguer des informations aux organismes gouvernementaux.**
- **Remplir des obligations envers nos partenaires** (développeurs et détenteurs de droits, par exemple).
- **Faire respecter des décisions de justice**(...).

Lorsque nous nous conformons à des obligations légales

Nous traitons vos données **lorsque nous avons l'obligation légale de le faire**, par exemple **pour nous conformer à des obligations judiciaires ou administratives.**

Cas d'application des présentes règles

Les présentes Règles de confidentialité s'appliquent à tous les services proposés par Google LLC et par ses sociétés affiliées, y compris YouTube et Android, ainsi qu'aux services proposés sur des sites tiers, tels que les services publicitaires.

Mentions légales Apple

Mac – iCloud – Apple Media (Apple Store, iTunes)

Source :

<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>

Les pages web ci-dessus imprimées en PDF totalisent déjà **68 pages**... Et elles font elles-mêmes référence à d'autres pages.

Les conditions ont été acceptées par les utilisateurs quand ils ont cliqué « ok », sous peine de ne pas pouvoir utiliser le produit ou le service.

Beaucoup d'options sont cochées par défaut dans les configurations d'applications et bon nombre d'utilisateurs n'en ont pas conscience ou ne savent pas où les trouver.

Vous trouverez ci-après 6 pages avec les extraits les plus pertinents.

Engagement de confidentialité

<https://www.apple.com/befr/legal/privacy/fr-ww/>

(...)

Collecte et utilisation des données personnelles

(...) **Apple et ses sociétés affiliées peuvent s'échanger ces données personnelles** et les utiliser (...). (...) **Elles peuvent également les associer avec d'autres informations** afin de fournir et d'améliorer leurs produits, services, contenus et publicités.

(...)

Données personnelles que nous recueillons

(...) nous pouvons **collecter tout un ensemble d'informations**, telles que votre nom, votre adresse postale, votre numéro de téléphone, votre adresse e-mail, vos préférences de contact, vos identifiants d'appareils, votre adresse IP, vos informations de lieu, les données de votre carte bancaire et vos informations de profil **lorsque vous nous contactez par le biais des médias sociaux**.

Lorsque vous partagez votre contenu avec votre famille et vos amis via des produits Apple, (...) **Apple peut collecter les informations que vous fournissez sur ces personnes**, (...).

(...)

Utilisation de vos données personnelles

Nous pouvons traiter vos données personnelles (...) avec votre consentement, **pour nous conformer à une obligation légale** à laquelle Apple est soumise, (...) , **ou lorsque nous estimons que cela est nécessaire** pour atteindre les objectifs légitimes poursuivis par Apple ou un tiers à qui nous pouvons être amenés à divulguer ces données.

(...)

Nous pouvons aussi utiliser vos données personnelles dans des objectifs de sécurité des comptes et réseaux, notamment afin de protéger nos services pour le bénéfice de tous nos utilisateurs, ainsi que filtrer et **analyser tout contenu** chargé pour nous assurer qu'il ne contient pas de contenus illégaux,

(...)

Nous limitons notre utilisation des données à des fins de lutte contre la fraude aux données strictement nécessaires et **dans le cadre de nos intérêts légitimes estimés afin de protéger nos clients et nos services**.

(...)

Nous pouvons également utiliser les données personnelles **à des fins internes**, par exemple pour des audits, **analyses de données** et recherches dans le but d'améliorer les produits, services et communications clients d'Apple.

(...)

Source de vos données personnelles lorsque nous ne les collectons pas auprès de vous

Il peut nous arriver de recevoir des données personnelles vous concernant par le biais de tiers, si ces personnes partagent leur contenu avec vous à l'aide de produits Apple(...).

Nous pouvons également **vérifier les informations** que vous nous fournissez lorsque vous créez un identifiant Apple avec un tiers, **à des fins de sécurité** et de prévention de la fraude.

À des fins de recherche et développement, **nous pouvons utiliser des ensembles de données tels que ceux contenant des images, voix ou autres données pouvant être associées à une personne identifiable**.

Lorsque nous acquérons ce type d'ensemble de données, **nous le faisons conformément à la loi applicable dans la juridiction dans laquelle se trouve l'ensemble de données**.

(...)

Collecte et utilisation des données non personnelles

(...)

Nous pouvons **collecter des informations telles que le métier, la langue, le code postal, l'indicatif régional, l'identifiant unique de l'appareil, l'URL de référence, le lieu et le fuseau horaire dans lesquels un produit Apple est utilisé** afin de nous permettre de mieux comprendre le comportement du client et d'améliorer nos produits, services et publicités.

Nous pouvons recueillir des données concernant les activités du client sur notre site web, les services iCloud, l'iTunes Store, l'App Store, le Mac App Store, l'App Store de l'Apple TV, les iBooks Stores et à partir de nos autres produits et services.

(...)

Nous pouvons collecter et stocker des informations sur votre utilisation de nos services, **notamment les recherches que vous effectuez.**

(...) Elles ne sont pas associées à votre adresse IP, **excepté dans de rares cas** afin d'assurer la qualité de nos services sur Internet.

Cookies et autres technologies

(...)

Le fait de **savoir qu'une personne utilisant votre ordinateur ou appareil a acheté un certain produit ou utilisé un service particulier** nous aide à rendre nos communications publicitaires et électroniques plus pertinentes en fonction de vos centres d'intérêt.

(...)

Divulgence à des tiers

Apple peut parfois mettre certaines données personnelles à la disposition de tiers (...).

Fournisseurs de services

Apple partage des données personnelles avec des sociétés qui fournissent des services tels que le traitement d'informations, (...) la gestion et le développement de données clients (...). Ces sociétés sont dans l'obligation de protéger vos données et **peuvent se trouver dans tout pays dans lequel Apple exerce des activités.**

Autres

Apple pourra être amenée, du fait de la loi, dans le cadre d'une procédure en justice, d'un litige **et/ou d'une requête des autorités publiques de votre pays de résidence ou autre**, à **divulguer vos données personnelles**. Nous pouvons également divulguer des informations vous concernant **si nous pensons qu'à des fins de sécurité nationale, d'application de la loi ou autre sujet d'intérêt public, la divulgation est nécessaire ou appropriée.**

Nous pouvons également divulguer des informations vous concernant, mais uniquement si c'est légalement justifié, **si nous pensons que cette divulgation est raisonnablement nécessaire** pour faire valoir le respect de nos conditions générales d'utilisation, ou pour protéger nos activités ou nos utilisateurs. **Cela peut inclure fournir des informations aux autorités publiques ou gouvernementales.**

Intégrité et conservation des données personnelles

(...) **Nous conservons vos données** personnelles pendant la durée (...) **la plus courte possible** nécessaire à la réalisation de l'objectif de la collecte, **sauf si une durée de conservation plus longue est requise par la loi.**

(...)

Vos droits en matière de confidentialité

(...)

Nous vous donnerons un accès aux autres données à caractère personnel que nous détenons pour éventuellement nous demander de les corriger si elles sont inexactes ou de les supprimer, **à condition qu'Apple ne soit pas obligée de les conserver du fait de la loi** ou à des fins commerciales légitimes.

Nous pouvons également refuser certains aspects de demandes de suppression ou d'accès **si nous pensons que**, ce faisant, **nous nuirions à notre utilisation légitime des données** à des fins de lutte contre la fraude ou de sécurité, comme nous l'avons vu précédemment.

(...)

Services de géolocalisation

(...) **Apple et ses partenaires et licenciés**, (...) peuvent recueillir, utiliser et partager des données de localisation précises, **notamment la localisation géographique en temps réel de votre ordinateur ou appareil Apple.**

(...)

Transferts internationaux

Toutes les informations que vous fournissez peuvent être transférées à des entités à travers le monde, ou être accessibles à celles-ci.

(...)

Les données personnelles associées à Apple, à l'Apple Store en ligne et à iTunes peuvent également **être contrôlées par des entités juridiques en dehors des États-Unis**, (...)

Les images et toutes autres données associées collectées par Apple dans le monde entier pour améliorer l'app Plans d'Apple et pour la prise en charge de la fonctionnalité Vue à 360° sont transférées à Apple Inc. en Californie.

Ce que l'on nous demande fréquemment. (...)

<https://www.apple.com/befr/privacy/government-information-requests/>

Apple n'a jamais créé de porte dérobée (« backdoor ») ni de passe-partout pour permettre aux autorités d'accéder à ses produits ou ses services. Nous n'avons jamais laissé une quelconque autorité publique accéder directement aux serveurs Apple. Et nous ne le ferons jamais.

Bienvenue dans iCloud

<https://www.apple.com/befr/legal/internet-services/icloud/fr/terms.html>

(...)

Apple est le fournisseur du Service qui vous permet d'utiliser certains services Internet, y compris de **stocker vos données personnelles (telles que les contacts, calendriers, photos, notes, rappels, documents, données d'application et messagerie iCloud)** et les rendre accessibles sur vos appareils et ordinateurs compatibles, et certains services de géolocalisation, et ce conformément aux conditions générales du présent Contrat.

iCloud s'active automatiquement lorsque vous utilisez des appareils sous iOS 9 ou ultérieur et que vous ouvrez une session par le biais de votre identifiant Apple pendant la configuration de l'appareil, à moins que vous ne mettiez à niveau l'appareil après avoir choisi de ne pas activer iCloud.

(...)

Quand iCloud est activé, **vos données sont automatiquement envoyées et stockées par Apple**, afin que vous puissiez y accéder plus tard ou qu'il soit transmis via les réseaux sans fil (en mode push) vers vos autres appareils ou ordinateurs compatibles iCloud.

(...)

A. Utilisation des services de géolocalisation

Apple, ses partenaires et concédants peuvent fournir certaines fonctionnalités ou services qui s'appuient sur des informations de localisation provenant des appareils qui utilisent le système GPS (ou une technologie similaire, si disponible), ainsi que des points d'accès Wi-Fi publics et les localisations de tours de téléphonie mobile. Pour fournir ces fonctionnalités ou services lorsqu'ils sont disponibles, **Apple, ses partenaires et concédants doivent recueillir, utiliser, transmettre, traiter et conserver vos données de localisation, y compris, notamment, la localisation géographique de votre appareil** et de l'information liée à votre compte iCloud (« Compte ») et **tout autre appareil** enregistré ci-dessous, et, notamment, votre identifiant Apple, nom et identifiant d'appareil, et type d'appareil.

(...)

B. Localiser

Lorsque vous activez iCloud et le service de localisation (...), **Localiser (...) sera activé automatiquement sur cet appareil, ainsi que sur tous les accessoires Apple jumelés avec celui-ci.**

(...)

(...) Si la localisation hors ligne est activée sur un appareil, **celui-ci peut détecter la présence d'appareils hors ligne à proximité via Bluetooth (ou des technologies similaires). Si un appareil détecte un appareil hors ligne égaré, il utilise une connexion Wi-Fi ou mobile pour signaler de façon sécurisée la position approximative de l'appareil à l'identifiant Apple associé à l'appareil, afin que le propriétaire puisse voir sa position dans l'application Localiser.**

(...)

C. Sauvegarde

La Sauvegarde iCloud crée périodiquement et automatiquement le contenu des appareils iOS (...)

La sauvegarde peut inclure les paramètres de l'appareil, caractéristiques de l'appareil, photos et vidéos, documents, vos messages, sonneries, données de l'app Health et toute autre donnée d'app. (...)

D. Photos

1. **iCloud Photos.** Lorsque vous activez iCloud Photos, les photos, vidéos, métadonnées et toute modification que vous réalisez dans l'app Photos sur votre appareil iOS, votre ordinateur macOS ou PC Windows seront automatiquement transférées et stockées dans iCloud,

V. Contenu et Conduite

A. Contenu

(...)

Apple ne contrôle pas le Contenu (...)

C. Suppression de Contenu

(...)

Cependant, Apple se réserve le droit de déterminer à tout moment si le Contenu est approprié et conforme au présent Contrat, **et peut examiner, déplacer, refuser, modifier ou supprimer à tout moment du Contenu**, sans préavis et à son entière discrétion, si ce Contenu s'avère contraire aux dispositions du présent Contrat ou est autrement contestable.

E. Accès au Compte et au Contenu

(...)

Vous reconnaissez et acceptez qu'Apple peut, sans engager sa responsabilité à votre égard, **accéder, utiliser, préserver ou divulguer les informations relatives à votre Compte et Contenu** aux autorités, aux représentants du gouvernement ou à des tiers, **si Apple l'estime raisonnablement nécessaire ou approprié**, si la loi l'exige ou **si Apple a de bonnes raisons de croire** que cette accès, utilisation, divulgation ou préservation est raisonnablement nécessaire pour : (a) se conformer à la loi ou à toute demande d'une autorité; (b) faire appliquer le présent Contrat, y compris enquêter sur toute violation potentielle du Contrat ; (c) détecter, empêcher ou traiter des problèmes techniques, de sécurité ou de fraude ; ou (d) protéger les droits, la propriété ou **la sécurité d'Apple, ses utilisateurs, un tiers** ou le public, si la loi l'exige ou l'autorise.

H. Contenu publié ou mis à disposition par vous grâce au Service

(...) Cependant, en publiant ce Contenu sur des parties du Service accessibles au public **ou à d'autres utilisateurs avec lesquels vous acceptez de partager ce Contenu**, vous concédez à Apple **une licence pour le monde entier, à titre gratuit, non exclusive, d'utilisation, de distribution, de reproduction, de modification, d'adaptation, de publication, de traduction, d'exécution et de diffusion publique** du Contenu (...).

(...)

iTunes

<https://www.apple.com/befr/legal/internet-services/icloud/fr/terms.html>

(...)

VOS ENVOIS SUR NOS SERVICES

Nos Services peuvent vous permettre d'envoyer des éléments tels que (...) des photos, des vidéos et des podcasts (y compris les métadonnées et illustrations associées). (...) **Vous concédez par les présentes à Apple une licence mondiale, gratuite, perpétuelle** et non exclusive pour **utiliser** les éléments que vous soumettez dans les Services et à des fins marketing, ainsi qu'à des fins internes à Apple. Apple peut **contrôler** et décider de supprimer ou de **modifier tout élément envoyé**.

Instructions d'Envoi : Vous ne pouvez pas utiliser les Services pour :

- planifier ou entreprendre une activité illégale, frauduleuse ou manipulatrice.

(...)

CONTRAT DE LICENCE UTILISATEUR FINAL RELATIF À L'APPLICATION SOUS LICENCE

b. Consentement à l'utilisation des données : Vous acceptez que **le Concédant puisse collecter et utiliser des données techniques et toute information associée**, y compris, notamment, les informations techniques concernant votre dispositif, votre système et votre logiciel d'application, ainsi que les périphériques, **et qui sont recueillies périodiquement** afin de faciliter la fourniture de mises à jour de logiciels, de services d'assistance technique relative au produit, ainsi que d'autres services (le cas échéant) se rapportant à l'Application sous Licence.

BIBLIOTHÈQUE MUSICALE iCloud

(...) Lorsque vous utilisez la Bibliothèque Musicale iCloud, **Apple enregistre des informations telles que les pistes que vous écoutez, arrêtez ou passez, les appareils que vous utilisez et le moment et la durée des écoutes**.

(...)

AUTRES STIPULATIONS

Vous reconnaissez qu'Apple est en droit, sans engager sa responsabilité à votre égard, **de divulguer des données et/ou des informations aux forces de l'ordre, aux autorités publiques et/ou à des tiers, si Apple l'estime raisonnablement nécessaire ou approprié** pour faire appliquer et/ou vérifier le respect de toute disposition du présent Contrat (...)

Conditions et règlements Facebook – Messenger – Instagram - Whatsapp (extraits)

Source :

- <https://fr-fr.facebook.com/legal/terms>
- <https://fr-fr.facebook.com/about/privacy>
- <https://fr-fr.facebook.com/communitystandards/>
- <https://www.whatsapp.com/legal/?lang=fr>

Les pages web ci-dessus imprimées en PDF totalisent **80 pages**... faisant elles-mêmes référence à de nombreuses pages liées.

Les conditions ont été acceptées par les utilisateurs quand ils ont cliqué < OK >, sous peine de ne pas pouvoir utiliser le produit ou le service.

Beaucoup d'options sont cochées par défaut dans les configurations d'applications et bon nombre d'utilisateurs n'en ont pas conscience ou ne savent pas où les trouver.

Vous trouverez ci-après 6 pages avec les extraits les plus pertinents. Facebook a la particularité de partager des données avec ses partenaires commerciaux (entre autres les publicitaires et annonceurs) et de veiller à la bonne pensée de ses utilisateurs.

Conditions d'utilisation (Facebook – Messenger - Instagram)

<https://fr-fr.facebook.com/legal/terms>

(...)

En utilisant nos Produits, vous acceptez que nous vous montrions des publicités que nous croyons pertinentes pour vous en fonction de vos intérêts. **Nous utilisons vos données personnelles** afin de définir les publicités à vous montrer.

Nous ne vendons pas vos données personnelles aux annonceurs et ne partageons pas d'informations permettant de vous identifier directement (telles que votre nom, votre adresse e-mail ou toutes autres coordonnées) avec les annonceurs, **sauf autorisation expresse de votre part.**

(...)

Nous utilisons les données dont nous disposons, par exemple à propos des connexions que vous établissez, des options et des paramètres que vous sélectionnez, **et de ce que vous partagez et faites** sur nos Produits **et en dehors**, (...)

(...)

Nous employons des équipes dédiées à travers le monde et développons des systèmes techniques avancés afin de **détecter les mauvaises utilisations** de nos Produits, **les comportements préjudiciables** envers les autres et les situations dans lesquelles nous pourrions être en mesure de soutenir ou de protéger notre communauté. Si un tel contenu ou un tel comportement est porté à notre connaissance, nous prendrons les mesures appropriées, (...) **en supprimant le contenu, en bloquant l'accès à certaines fonctionnalités**, en désactivant un compte ou en contactant les autorités légales. **Nous partageons des données avec d'autres Entités Facebook** lorsque nous détectons une mauvaise utilisation ou un comportement préjudiciable de la part de quelqu'un qui utilise l'un de nos Produits.

(...) Enfin, nous développons des **systèmes automatisés** pour améliorer notre capacité à **détecter et à supprimer les activités abusives et dangereuses** qui pourraient porter atteinte à notre communauté et à l'intégrité de nos Produits.

(...) Cela inclut d'**analyser les données** que nous avons concernant nos utilisateurs et de comprendre comment les personnes utilisent nos Produits (...)

Nous permettons un accès mondial à nos services :

Pour que notre service mondial fonctionne, **nous devons conserver et distribuer du contenu** et des données dans nos centres de données et nos systèmes **dans le monde entier**, y compris en dehors de votre pays de résidence.

(...)

Vous ne pouvez pas utiliser nos Produits pour faire ou partager quoi que ce soit :

- qui est illégal, trompeur, discriminant ou frauduleux ;

(...)

Nous pouvons supprimer ou bloquer le contenu qui enfreint ces dispositions.

Si nous supprimons du contenu que vous avez partagé, (...), **nous vous en informerons** et vous expliquerons les options à votre disposition pour demander un réexamen, **à moins que vous n'enfreigniez gravement ou à maintes reprises les présentes Conditions ou en cas de restrictions techniques ou lorsqu'il nous est interdit de le faire pour des raisons légales.**

(...)

3. Les autorisations que vous nous accordez

(...) En particulier, lorsque vous partagez, publiez ou importez du contenu protégé par des droits de propriété intellectuelle sur ou en rapport avec nos Produits, **vous nous accordez une licence non exclusive, transférable, sous-licenciable, gratuite et mondiale pour héberger, utiliser, distribuer, modifier, exécuter, copier, représenter publiquement ou afficher publiquement, traduire et créer des œuvres dérivées de votre contenu** (conformément à vos paramètres de confidentialité et d'application). Cela signifie, par exemple, que **si vous partagez une photo sur Facebook, vous nous autorisez à la stocker, la copier et la partager avec d'autres personnes** (une nouvelle fois, conformément à vos paramètres), telles que des fournisseurs de services qui prennent en charge notre service ou les autres Produits Facebook que vous utilisez. Cette licence prend fin lorsque votre contenu est supprimé de nos systèmes.

Lorsque vous supprimez du contenu, (...) il peut perdurer ailleurs, dans nos systèmes, lorsque :
- lorsque la suppression immédiate limiterait notre faculté : de respecter une obligation légale, telle que la préservation des éléments de preuve ; **ou de respecter la demande d'une autorité judiciaire ou administrative, d'une autorité d'application de la loi ou d'un organisme gouvernemental ;**

Politique d'utilisation des données

<https://fr-fr.facebook.com/about/privacy>

La présente politique décrit les informations que nous traitons pour le fonctionnement de Facebook, Instagram, Messenger et d'autres fonctionnalités et produits proposés par Facebook (les Produits Facebook ou les Produits).

(...)

Quels types d'informations recueillons-nous ?

Ce que vous et d'autres personnes faites et fournissez.

- (...) Nous recueillons **le contenu, les communications** ainsi que d'autres informations que vous fournissez lorsque vous utilisez nos Produits, notamment lorsque vous créez un compte, **lorsque vous créez ou partagez du contenu, ou lorsque vous communiquez avec d'autres personnes ou leur envoyez des messages**. Cela peut comprendre des informations présentes dans le contenu que vous fournissez (par exemple, des métadonnées) ou concernant un tel contenu, telles que le lieu d'une photo ou la date à laquelle un fichier a été créé. (...) **Nos systèmes traitent automatiquement le contenu et les communications que vous et d'autres fournissez afin d'analyser le contexte et ce qu'ils contiennent aux fins décrites ci-dessous.**
- **Réseaux et connexions.**
Nous recueillons des informations sur les personnes, les Pages, les comptes, les hashtags et les groupes avec lesquels vous êtes en contact, ainsi que la manière dont vous interagissez avec eux sur nos Produits, par exemple, **les personnes avec lesquelles vous communiquez le plus ou les groupes dont vous faites partie.**
(...)
- **Votre utilisation.**
Nous recueillons des informations concernant la manière dont vous utilisez nos Produits, telles que **les types de contenu que vous consultez ou avec lesquels vous interagissez, les fonctionnalités que vous utilisez, les actions que vous réalisez, les personnes ou les comptes avec lesquels vous interagissez, et l'heure, la fréquence et la durée de vos activités.** (...)

Les activités d'autres personnes et les informations qu'elles fournissent **vous concernant. Nous recevons et analysons également le contenu, les communications et les informations que d'autres personnes** fournissent lorsqu'elles utilisent nos Produits.

(...)

Informations sur les appareils

Comme décrit ci-dessous, **nous recueillons des informations concernant les ordinateurs, téléphones, téléviseurs connectés et autres appareils connectés au web que vous utilisez** et qui s'intègrent à nos Produits et depuis lesdits appareils, et **nous combinons ces informations** sur les différents appareils que vous utilisez. (...)

Les informations que nous obtenons depuis ces appareils comprennent :

- **Attributs des appareils** : des informations telles que **le système d'exploitation, les versions matérielles et logicielles, le niveau de batterie, l'intensité du signal, l'espace de stockage disponible, le type de navigateur, le nom et le type des applications et des fichiers, ainsi que les plug-ins.**
- **Activités sur l'appareil** : les informations concernant **les opérations et les comportements sur l'appareil**, par exemple, lorsqu'une fenêtre est mise au premier plan ou en arrière plan, ainsi que les mouvements de la souris (permettant de différencier les humains des bots). (...)
- **Réseau et connexion** : des informations telles que le nom de votre opérateur mobile ou de votre fournisseur d'accès à Internet, votre langue, votre fuseau horaire, votre numéro de téléphone mobile, votre adresse IP, votre vitesse de connexion et, dans certains cas, **des informations concernant d'autres appareils situés à proximité** ou sur votre réseau afin que nous puissions, notamment, vous aider à diffuser une vidéo à partir de votre téléphone sur votre téléviseur.

Informations fournies par les partenaires.

(...) Ces partenaires communiquent **des informations concernant vos activités en dehors de Facebook** (notamment des informations concernant votre appareil, les sites web que vous consultez, les achats que vous effectuez, les publicités que vous voyez et votre utilisation de leurs services), **que vous possédiez ou non un compte Facebook ou que vous soyez connecté(e) ou non à Facebook.**

Comment utilisons-nous ces informations ?

Nous utilisons les informations à notre disposition (en fonction des choix que vous effectuez) de la façon décrite ci-dessous, afin de fournir et d'assurer le fonctionnement des Produits Facebook et les services associés décrits dans les Conditions d'utilisation de Facebook et les Conditions d'utilisation d'Instagram. Voici de quelle façon :

(...)

Proposer, personnaliser et améliorer nos Produits.

- **Informations géographiques** : nous utilisons des informations géographiques (comme **votre position actuelle, le lieu où vous résidez, les endroits où vous aimez aller** et les entreprises et personnes à proximité) afin de proposer, de personnaliser et d'améliorer nos Produits, notamment les publicités, pour vous et les autres. (...)
- **Favoriser la sûreté, l'intégrité et la sécurité.**
Nous utilisons les informations à notre disposition pour vérifier les comptes et les activités, pour lutter contre les comportements dangereux, **pour détecter et prévenir le contenu indésirable** et toutes autres expériences négatives, pour préserver l'intégrité de nos Produits et pour favoriser la sûreté et la sécurité sur les Produits Facebook et en dehors de ceux-ci. (...)

Comment ces informations sont-elles partagées ?

Vos informations sont partagées avec d'autres personnes des manières suivantes :

- **Partage sur les Produits Facebook**
(...) Par exemple, nous supprimerons **l'accès des développeurs à vos données Facebook et Instagram si vous n'avez pas utilisé leur application depuis trois mois** (...)
(...)
- **Partenaires avec des partenaires tiers**
 - **Forces de l'ordre ou demandes légales.**
Nous partageons des informations avec les forces de l'ordre ou en réponse à des demandes légales dans les circonstances décrites ci-dessous.

(...)

Comment les Entités Facebook collaborent-elles ?

Facebook et Instagram partagent leur infrastructure (...), leurs systèmes et leur technologie avec d'autres Entités Facebook (notamment WhatsApp et Oculus) . **Nous traitons également les informations vous concernant sur l'ensemble des entités Facebook** à ces fins, dans les limites prévues par la loi en vigueur et conformément à leurs conditions et politiques. Par exemple, **nous traitons les informations provenant de WhatsApp** concernant les comptes qui envoient du **contenu indésirable** sur son service afin de pouvoir prendre des mesures adéquates à l'encontre de ces comptes sur Facebook, Instagram ou Messenger.

(...)

Sur quel fondement juridique nous appuyons-nous pour traiter les données ?

Nous recueillons, utilisons et partageons les données en notre possession des manières décrites ci-dessous :

- dans la mesure nécessaire pour remplir nos obligations légales ;
- Pour protéger vos intérêts vitaux ou ceux des autres ;
- **dans la mesure nécessaire dans l'intérêt du public ;**

(...)

Conservation des données, désactivation et suppression d'un compte

Nous accédons à vos informations, les conservons et les partageons avec les organismes de réglementation, les autorités judiciaires ou d'autres :

- Pour répondre à une demande légale, **si nous pensons en toute bonne foi que la loi l'exige.**
(...)
- Lorsque nous avons des raisons de **penser en toute bonne foi que cela est nécessaire pour détecter, empêcher et maîtriser la fraude**, l'utilisation non autorisée des Produits, des violations de nos conditions ou règlements, ou toutes autres **activités dangereuses** ou illégales ;
- **pour nous protéger nous-mêmes** (notamment nos droits, notre propriété ou nos Produits), vous **ou d'autres**, notamment dans le cadre d'enquêtes **ou de demandes réglementaires** ; ou pour éviter tout décès ou toute blessure corporelle imminente. Par exemple, le cas échéant, **nous fournissons des informations à des partenaires tiers et nous recevons des informations desdits partenaires à propos de la fiabilité de votre compte** pour éviter une fraude, un abus ou toute autre activité dommageable dans nos Produits comme en dehors de ceux-ci.

Les informations vous concernant que nous recevons (notamment les données de transactions financières liées aux achats effectués avec Facebook) **peuvent être consultées et conservées pendant une période prolongée lorsqu'elles font l'objet d'une demande ou d'une obligation légale**, d'une enquête gouvernementale ou d'enquêtes sur d'éventuelles violations de nos conditions d'utilisation ou de nos règlements, ou pour éviter tout autre dommage. (...)

Comment gérons-nous et transférons-nous les données dans le cadre de nos services internationaux ?

Nous partageons des informations à l'échelle mondiale, à la fois en interne avec les Entités Facebook, et en externe avec nos partenaires et avec les personnes avec qui vous vous connectez et partagez du contenu dans le monde entier, conformément à cette politique. **Les informations contrôlées par Facebook Ireland seront transférées ou transmises, ou stockées et traitées, aux États-Unis ou dans d'autres pays en dehors de celui où vous vivez**, aux fins décrites dans la présente politique. (...).

Nous utilisons des clauses contractuelles standard approuvées par la Commission européenne et nous nous appuyons sur les décisions d'adéquation de la Commission européenne **concernant certains pays**, le cas échéant, pour les transferts de données de l'EEE vers les États-Unis et d'autres pays.

Standards de la communauté

<https://fr-fr.facebook.com/communitystandards/>

Alors que les populations du monde entier sont confrontées à cette urgence de santé publique sans précédent, nous voulons nous assurer que **nos normes communautaires protègent les personnes contre les contenus préjudiciables** et les nouveaux types d'abus liés à COVID-19. **Nous nous efforçons de supprimer les contenus susceptibles de contribuer à des préjudices réels**, notamment par le biais de nos politiques interdisant la coordination des préjudices, la vente de masques médicaux et de biens connexes, les discours de haine, l'intimidation et le harcèlement **et la désinformation** qui contribuent au risque de violence ou de préjudice physique imminent. Au fur et à mesure de l'évolution de la situation, **nous continuons à examiner le contenu de la plateforme**, à évaluer les tendances en matière de discours et à nous entretenir avec des experts, et **nous fournirons, le cas échéant, des orientations politiques supplémentaires pour assurer la sécurité des membres de notre communauté pendant cette crise.**

(ndlr : ce paragraphe est une traduction)

INTRODUCTION

(...)

C'est la raison pour laquelle nous avons créé un ensemble de Standards de la communauté qui expliquent ce qui est autorisé, ou non, sur Facebook. **Nos politiques sont fondées sur les retours de notre communauté et l'avis de spécialistes dans des domaines comme les technologies, la sécurité publique et les droits de l'homme.**

(...)

RÉITÉRER NOTRE ENGAGEMENT POUR L'EXPRESSION

(...)

Intégrité et authenticité

20. Fausses informations

(...)

Limiter la diffusion de fausses informations sur Facebook est une responsabilité que nous prenons très au sérieux. (...) Pour ces raisons, nous ne supprimons pas les fausses informations de Facebook, mais **en limitons significativement la diffusion en les affichant plus bas dans le fil d'actualité.**

(...)

(Lien vers <https://about.fb.com/news/2018/05/hard-questions-false-news/>)

Nous prenons également des mesures contre les pages entières et les sites web qui partagent régulièrement de fausses nouvelles, réduisant ainsi leur diffusion globale dans le fil d'actualité.)

(...)

Un autre volet de notre stratégie dans certains pays consiste à **établir des partenariats avec des vérificateurs de faits tiers pour examiner et évaluer l'exactitude des articles et des publications sur Facebook.** (...). **Lorsque ces organisations jugent un article comme faux, nous le classons nettement moins bien dans le fil d'actualité.** En moyenne, cela réduit de plus de 80 % le nombre d'opinions futures. Nous utilisons également les informations des vérificateurs de faits pour améliorer notre technologie afin de pouvoir identifier plus rapidement à l'avenir un plus grand nombre de fausses nouvelles potentielles

(...)

Nous travaillons pour créer une communauté plus informée et réduire la diffusion des fausses informations par de nombreux moyens, notamment :

(...)

- **En limitant la diffusion de contenus qualifiés comme faux par des médias de vérification tiers indépendants**

(...)

Mentions Légales de WhatsApp

<https://www.whatsapp.com/legal/?lang=fr>

(...)

Nous avons conçu WhatsApp en adoptant des principes de confidentialité et de sécurité majeurs, comme le chiffrement de bout en bout de vos messages et de vos appels, ce qui signifie que ni nous ni des tierces parties ne pouvons les lire ou les écouter. Voici quelques points importants :

Rien de ce que vous partagez sur WhatsApp, notamment vos messages, photos et informations de compte, ne sera communiqué sur Facebook ni aucune autre entité de la famille d'applications à la vue des autres, et rien de ce que vous publiez sur ces applications ne sera communiqué sur WhatsApp à la vue des autres, **à moins que vous n'y consentiez.**

Conditions d'utilisation de WhatsApp

(...) Vous acceptez nos Conditions en vous inscrivant, en installant, en consultant ou en utilisant nos applications, services, fonctionnalités, logiciels ou notre site web.

(...)

Sécurité.

Nous nous efforçons de garantir la sécurité de WhatsApp en prenant les mesures nécessaires face aux personnes et activités abusives et aux violations de nos Conditions. (...) Nous développons **des systèmes automatisés pour améliorer notre capacité à détecter et à supprimer du service WhatsApp les activités et personnes abusives qui pourraient porter atteinte à notre communauté et à la sécurité de nos Services.** (...).

(...)

Politique de confidentialité et données des utilisateurs

Nous partageons également des informations afin de lutter contre les indésirables, les menaces, les abus ou les violations et de promouvoir la sécurité et la protection dans les produits des entités Facebook. Cependant, vos messages WhatsApp ne seront pas partagés sur Facebook à la vue des autres. En effet, **Facebook n'utilisera pas vos messages WhatsApp** dans un but autre que celui de nous aider à exploiter et fournir nos services. ***(Facebook reçoit donc quand même les données, et en fait à priori donc aussi ce que les obligations légales lui imposent.. ou ce qu'il pense de toute bonne foi nécessaire de faire... ndlr)***

(...)

Tiers. **WhatsApp peut transférer des données au sein de la famille d'entreprises Facebook** et à des tiers, y compris des fournisseurs de service et d'autres partenaires. Conformément aux Principes du Bouclier de protection des données, WhatsApp est responsable de tout traitement de données personnelles par lesdits tiers non conforme aux Principes du Bouclier de protection des données, sauf si WhatsApp n'est pas responsable de l'événement à l'origine du préjudice allégué.

Demands légales. Les données personnelles transmises par nos Partenaires peuvent faire l'objet d'une divulgation dans le cadre de demandes légales ou conformément à d'autres procédures judiciaires ou gouvernementales, telles qu'une assignation à comparaître, un mandat ou une ordonnance du tribunal. Pour en savoir plus, consultez l'article « Droit et protection » de la Politique de confidentialité de WhatsApp.

Politique relative à la vie privée - Yahoo

Applicable à tout produit Yahoo : Yahoo – Yahoo Mail...

Source : <https://www.verizonmedia.com/policies/ie/fr/verizonmedia/privacy/index.html>

La page web imprimée en PDF fait **16 pages**... Les conditions ont été acceptées par les utilisateurs quand ils ont cliqué < OK >, sous peine de ne pas pouvoir utiliser le produit ou le service.

Beaucoup d'options sont cochées par défaut dans les configurations d'applications et bon nombre d'utilisateurs n'en ont pas conscience ou ne savent pas où les trouver.

Vous trouverez ci-après 3 pages avec les extraits les plus marquants.

Bienvenue sur la Politique relative à la Vie Privée de Verizon Media

<https://www.verizonmedia.com/policies/ie/fr/verizonmedia/privacy/index.html>

(...)

Nous fournissons des outils de contrôle pour vous aider à gérer votre expérience avec nous. Si vous avez déjà un compte Yahoo ou AOL, vous devez accepter cette Politique relative à la vie privée.

(...) Si vous êtes un utilisateur de HuffPost UK, Sky | Yahoo Mail or BT | Yahoo Mail, Verizon Media pourrait faire référence à d'autres entités en ce qui concerne qui contrôle vos données personnelles. **Les utilisateurs de HuffPost UK, Sky | Yahoo Mail or BT | Yahoo Mail peuvent obtenir plus d'informations en cliquant ici.** (ndlr : La page n'existe pas)

Dans certains cas, nous pouvons continuer à traiter vos informations après que vous ayez retiré votre consentement si nous avons une base légale pour le faire, ou si le retrait de votre consentement était limité à certaines activités de traitement. Par exemple, **nous pouvons conserver des informations si nous sommes dans l'obligation légale de le faire**, pour résoudre des litiges et pour faire respecter nos accords.

(...)

Collecte et utilisation des données - Informations générales

(...)

Nous collectons les informations que vous nous fournissez afin de nous permettre de faire fonctionner nos Services et de les mettre à votre disposition, notamment :

- Quand vous créez un compte à l'aide d'un Service ou d'une marque appartenant à Verizon Media. **(Veillez noter que lorsque vous utilisez nos Services, nous pouvons être en mesure de vous identifier ou d'identifier vos appareils, même si vous n'êtes pas connecté à nos Services.)**
- Verizon Media peut utiliser des identifiants d'appareil, des cookies et d'autres données d'identification, **notamment des informations obtenues auprès de tiers, pour vous associer à des comptes** et/ou des appareils.
- Lorsque vous utilisez nos Services d'une autre manière, comme **lorsque vous consultez le contenu** que nous mettons à votre disposition, **effectuez des recherches** ou **installez tout logiciel appartenant à Verizon Media**, comme des plug-ins.

Informations sur les appareils.

Nous collectons des informations à partir de vos appareils (ordinateurs, téléphones portables, tablettes, etc.) (...) qui nous permettent **d'identifier** et **d'associer** votre activité sur tous vos appareils et dans tous les Services.

Ces informations comprennent des identifiants et informations spécifiques aux appareils, comme **l'adresse IP**, les informations de **cookies**, les identifiants publicitaires et d'appareil mobile, la version du navigateur, le type et la version du système d'exploitation, les informations relatives au réseau mobile, **les paramètres de l'appareil, ainsi que les données logicielles.**

Informations de localisation.

Nous collectons des informations de localisation à partir de diverses sources. Pour obtenir des informations supplémentaires sur les autorisations de localisation et les gérer, consultez notre page Localisations et accédez aux paramètres de localisation sur vos appareils.

Informations provenant des cookies et d'autres technologies.

Nous **collectons des informations lorsque vous accédez à du contenu**, des publicités, sites, widgets interactifs, **applications et à d'autres produits (dans le cadre de nos Services et en dehors)** (...). Ces informations incluent **le type de publicité ou de contenu diffusé, visionné ou sur lequel vous avez cliqué**, la **fréquence** et la **durée** de vos activités, **les sites ou applications que vous avez utilisés avant d'accéder à nos Services et ce que vous avez consulté par la suite**, des données indiquant si vous avez consulté un contenu ou une publicité spécifique (...).

Informations provenant d'autrui.

Nous collectons des informations sur vous lorsque nous les recevons d'autres utilisateurs, tiers et affiliés, notamment :

- Lorsque vous liez votre compte à des services tiers **ou vous connectez à l'aide d'un partenaire (comme Facebook ou Twitter)**.
- Depuis des sources publiques.(...)

Ces informations peuvent inclure votre activité sur d'autres sites et applications, ainsi que des informations que ces tiers vous envoient ou nous envoient.

Utilisation de ces informations

(...) nous mettons en corrélation et utilisons les informations dont nous disposons sur vous (notamment les informations que nous recevons dans le cadre de nos Services **et en dehors**) pour comprendre comment vous utilisez nos Services et interagissez avec eux, **ainsi que les personnes ou choses qui vous intéressent et auxquelles vous êtes lié.**

Nous pouvons également utiliser les informations que nous détenons à votre sujet des manières et aux fins suivantes :

- **Pour analyser votre contenu et d'autres informations (incluant les e-mails entrants et sortants, les messages instantanés, les publications, les photos, les pièces jointes et autres communications) pour maintenir la sécurité de nos Services.**
- (...)
- Pour mener des recherches et soutenir l'innovation.
- **Pour effectuer des analyses et générer des rapports destinés à des acteurs extérieurs, (...).** Ces analyses et rapports **pourraient comprendre des informations pseudonymisées ou agrégées.**
- **Pour détecter toute activité frauduleuse, abusive ou illégale et vous en préserver, et garantir la sécurité de nos Services.**

Quelles sont nos bases juridiques pour l'utilisation de l'information

(...) Troisièmement, dans certains cas, **il est possible que nous traitions vos informations quand cela s'avère nécessaire pour défendre nos intérêts légitimes ou les intérêts légitimes de tiers,** dans les cas où vos droits ou intérêts ne prévalent pas sur nos intérêts légitimes. De temps à autre, **Verizon Media peut s'appuyer sur d'autres bases juridiques pour traiter vos informations, notamment pour protéger les intérêts vitaux d'un utilisateur** (comme en cas de risque de préjudice imminent) **ou pour se conformer à une obligation légale.**

Partage de ces informations

Verizon Media partage vos informations avec ses marques et sociétés affiliées, ainsi qu'avec Verizon. ...)

Nous ne vendons, n'autorisons ou ne partageons pas des informations permettant d'identifier individuellement nos clients avec des sociétés, organisations ou personnes externes à Verizon Media, à moins que l'une des circonstances suivantes ne se présente :

- **Avec votre accord.**
- (...)
- Avec nos partenaires. Nous pouvons partager vos informations avec des entreprises non affiliées à Verizon Media, comme décrit ci-après : **Partenaires fiables.**
- À des fins juridiques. **Nous pouvons accéder à des informations, les conserver et les divulguer** pour enquêter, prévenir ou prendre des mesures en rapport avec : (i) toute procédure judiciaire et **demande d'organismes gouvernementaux et juridiques** ; (...) (vi) **la protection des droits, des biens ou de la sécurité** personnelle de Verizon Media, de ses utilisateurs ou du public ; (vii) l'établissement ou l'exercice de droits légaux ou les mesures de défense contre des poursuites judiciaires ; ou (viii) **au titre des exigences prévues par la loi.** **Cela peut comprendre les réponses à des demandes gouvernementales légitimes.**

(...)

Traitement et transfert des données

Lorsque vous utilisez l'un de nos Services ou interagissez avec l'un d'eux, **vous acceptez le traitement, le partage, le transfert et l'utilisation de vos informations**, comme décrit dans la présente Politique relative à la vie privée.

Quel que soit le pays dans lequel vous résidez, **vous nous autorisez à transférer, traiter, stocker et utiliser vos informations dans des pays autres que le vôtre**, conformément à la présente Politique relative à la vie privée, et à vous fournir des Services. **Certains de ces pays ne disposent pas des mêmes garanties en matière de protection des données que le pays dans lequel vous résidez actuellement.**

Les États-Unis et d'autres pays ne faisant pas partie de l'EEE disposent de différentes lois sur la protection des données et de règles liées à l'accès du gouvernement aux informations.

Si vous résidez dans l'EEE, lorsque vos données sont transférées de votre pays d'origine vers un pays situé en dehors de l'EEE, **il se peut que certains pays ne disposent pas des mêmes garanties en matière de protection des données que votre pays d'origine.**

(...). Comme nous sommes présents dans des pays du monde entier (y compris aux États-Unis) et que nous utilisons une infrastructure technique dans ces pays, pour être en mesure de vous offrir nos Services conformément au contrat nous liant, **nous devons peut-être transférer vos informations vers d'autres juridictions si besoin est.** Nous ne pouvons pas vous fournir nos Services **sans transférer vos données d'un pays à l'autre.**