

ÉCRANS ET CONFINEMENT

**POUR UN USAGE SÉCURISÉ
DU WEB EN PÉRIODE DE
CONFINEMENT**

PAR PATRICK MPONDO-DICKA

ÉCRANS ET CONFINEMENT

POUR UN USAGE SÉCURISÉ DU WEB EN
PÉRIODE DE CONFINEMENT



PAR PATRICK MPONDO-DICKA



Attribution - Pas d'Utilisation Commerciale - Partage dans les Mêmes Conditions 4.0 International (CC BY-NC-SA 4.0)

Conformément à la licence indiquée ci-dessus, ce guide est gratuit, libre, réutilisable et modifiable, dès lors que les modifications sont distribuées selon la même licence..

TABLE DES MATIÈRES

Pour un usage sécurisé du web en période de confinement	2
Mode d'emploi	6
Pourquoi ce document ?	6
À qui est destiné ce document ?	7
Comment l'utiliser ?	8
De quelques inconvénients du numérique	9
Le web, entre utopie et marché	10
Le web utopique	10
Le web mercantile	10
Nous sommes captés par les écrans de nos appareils parce qu'ils sont conçus pour ça !	12
Des outils sécurisés et respectueux de vos données	15
Une messagerie protégée	15
Des outils de web-conférence sécurisés	16
Des navigateurs qui respectent votre vie privée	17
Des moteurs de recherche respectueux de vos données	18
Des courriers électroniques protégés de bout en bout	19

Des ouvrages et des sites de référence	21
À propos de l'auteur	22

MODE D'EMPLOI

POURQUOI CE DOCUMENT ?

Depuis sa création, **le web n'a cessé de croître de manière exponentielle, plus vite que les usages, es besoins, et la compréhension sociale de son fonctionnement**, plus vite que la régulation économique et juridique, et de manière extrêmement lucrative pour les entreprises qui l'ont investi, et qui continuent d'y investir des sommes faramineuses pour en tirer le maximum de profit, basé sur un produit essentiel : les données des utilisateurs.

C'est pourquoi le web est aujourd'hui omniprésent, incroyablement indiscret, intrusif et manipulateur, de manière croissante depuis l'avènement du web 2.0 (le web des médias sociaux, Facebook, Twitter, etc.), et plus encore aujourd'hui avec le web 3.0 (le web des objets connectés).

Dans les circonstances exceptionnelles du confinement, on aura tendance à utiliser plus intensivement nos appareils numériques connectés, et à leur confier des données plus intimes (affects, maladies, états psychologiques, etc.) qui seront exploitées à plus ou moins long terme par les plateformes de médias sociaux, comme Facebook, WhatsApp, Messenger et Instagram (qui appartiennent à

Facebook), Google, le moteur de recherche, Youtube, Gmail et Chrome (qui appartiennent à Google), et quelques autres (notamment Snapchat et TikTok, très prisés par nos ados).

L'IDÉE DE CE DOCUMENT EST DE VOUS PROPOSER QUELQUES OUTILS AUSSI FACILES D'ACCÈS ET D'USAGE QUE CEUX QUE VOUS UTILISEZ HABITUELLEMENT MAIS CONÇUS POUR NE PAS S'APPROPRIER VOS DONNÉES.

À QUI EST DESTINÉ CE DOCUMENT ?

Ce document a été conçu à la suite d'un échange entre la directrice de la Maison des Adolescents de la Haute Garonne et l'auteur, qui intervient souvent auprès de l'organisme en tant que spécialiste des questions liées au numérique et à l'éducation.

Il s'adresse particulièrement aux parents d'enfants et d'adolescents en situation de confinement.

VOUS POUVEZ L'UTILISER POUR MIEUX COMPRENDRE ET AMÉLIORER LA PROTECTION DE VOS DONNÉES PERSONNELLES, ET DE CELLES DE VOS ENFANTS ET ADOLESCENTS.

Les conseils proposés ne sont pas limités au moment du confinement, vous pouvez les adopter pour tous vos usages numériques.

COMMENT L'UTILISER ?

C'est un document qui a vocation à rester numérique, disponible aux formats PDF et ePub, conçu pour être consulté sur un ordinateur, une tablette ou un téléphone. Il contient des liens cliquables vers les sources disponibles en ligne au moment de sa rédaction. L'ensemble des liens qu'il contient sont repérables à **leur couleur fuchsia**.

La table des matières est également manipulable : il suffit de cliquer sur une ligne pour accéder à la page correspondante. Les sections, les chapitres et les sous-chapitres y sont affichés, en gras pour les deux premiers.

Les **ÉLÉMENTS PRIMORDIAUX** sont en majuscule, gras et bleu, tandis que les **notions importantes** sont en gras et en orange. On retrouve ainsi facilement les choses les plus importantes à retenir.

DE QUELQUES INCONVÉNIENTS DU NUMÉRIQUE

Puisque nous sommes confinés, nous avons tendance à utiliser beaucoup plus que de coutume les outils numériques de communication à distance. Pourtant, il faut faire attention à ce que ces outils ne se retournent pas contre nous, en devenant de véritables aspirateurs à données personnelles, ou des portes ouvertes sur nos données, accessibles au moins doué des hackers.

Pour vous y aider, **voici un petit guide des services disponibles en ligne qui préservent vos données personnelles et votre vie privée, par choix éthique** (on appelle cela [Ethics By Design](#), ce qu'on peut traduire par éthique par conception).

Aucun des services présenté n'est difficile à installer, à configurer (il n'y a souvent rien à faire) ou à prendre en main, en tout cas pas moins facile que les plateformes que vous connaissez. Ils sont juste moins connus et moins publicisés, car ils disposent de budgets infiniment plus modestes que ceux des grandes multinationales.

LE WEB, ENTRE UTOPIE ET MARCHÉ

LE WEB UTOPIQUE

Le web a été pensé avec des principes issus de la contre-culture américaine et du milieu universitaire californien des années 70 : c'est ce soubassement culturel utopique qui a amené les associations que l'on peut faire entre numérique et partage, échange, bien commun, et *empowerment* (encapacitation, en français, c'est-à-dire qui donne de nouvelles capacités à ses usagers). **De cette origine utopique sont issus le web, les formats ouverts, les logiciels libres, les listes de diffusions, la possibilité de prise de parole publique de tous**, d'abord développées via les blogs, ensuite prise en charge (et *récupérée*) par les plateformes de réseaux sociaux.

LE WEB MERCANTILE

Mais le web a aussi engendré un marché immense, basé essentiellement sur les données personnelles et la captation de l'attention, dont profite de nombreuses entreprises internationales, au premier rang desquelles les GAFAM, Google Amazon, Facebook, Apple, Microsoft. La bascule s'est faite au début des années 2000, quand **les entreprises naissantes du web se sont**

demandées comment créer du profit tout en maintenant la gratuité des services : la contrepartie choisie a été l'utilisation des données personnelles, à des fins de ciblage des individus.

Après la crise spéculative de 2004 (la fameuse *explosion de la bulle internet*), les entreprises du web qui ont survécues et prospérées avaient toutes le caractère commun de capitaliser sur les données des usagers, ce qu'on a appelé le Web 2.0. C'est certes un web plus participatif, mais **c'est aussi un web plus intrusif et plus aspirateur de données**, qui a donné lieu au développement des plateformes de réseautage social, et s'est prolongé dans le Web 3.0, qu'on appelle également Internet des Objets (en anglais IoT, pour *Internet of Things*).

Pour donner un exemple d'intrusivité du Web 3.0,
LES ENCEINTES CONNECTÉES ONT POUR PRINCIPE DE FONCTIONNEMENT D'ÉCOUTER TOUTES VOS CONVERSATIONS ET DE LES TRANSMETTRE SUR LES SERVEURS DE LEURS FABRICANTS.

En clair, ça veut dire que tout ce que vous dites devant une enceinte connectée est écouté, enregistré et envoyé vers des serveurs étrangers américains (Google, Apple), coréens (Samsung) ou chinois (Huawei, Xiaomi), vos conversations courantes, comme vos conversations intimes.

Cette part cynique du web est à l'œuvre et agit pendant que vous cherchez simplement à maintenir le contact avec vos proches pendant le confinement.

C'est par exemple le cas de la plateforme Zoom, dont l'usage a explosé pendant le confinement, mais qui s'avère peu respectueuse des données personnelles de ses utilisateurs.

Mais c'est aussi Ice que fait Google, qui détient la plus grande base de données personnelles du monde. Vous avez un compte Google ? [cliquez ici](#) et accédez aux données que la plateforme a sur vous : vous allez voir, c'est très instructif.

NOUS SOMMES CAPTÉS PAR LES ÉCRANS DE NOS APPAREILS PARCE QU'ILS SONT CONÇUS POUR ÇA!

Les séries TV, les jeux vidéos, les réseaux sociaux numériques sont autant de programmes numériques conçus pour capter indéfiniment l'attention de leurs utilisateurs.

Netflix a par exemple systématisé à la télévision l'enchaînement entre deux épisodes ou entre deux séries, pour réduire au minimum le temps de réflexion qui nous permet d'arrêter le visionnage ; c'est encore

plus difficile d'y résister quand le confinement augmente le temps oisif passé à la maison.

C'est un principe similaire qui régit la fonction [pull to refresh](#) (tirer pour rafraîchir) de nombreuses applications sur nos téléphones, que regrette aujourd'hui son inventeur, Loren Brichter. [Et il n'est pas le seul !](#)

Deux notions peuvent vous aider à comprendre ce fonctionnement des interfaces numériques :

l'économie de l'attention, qui montre comment notre attention est devenue la ressource rare dans une économie de l'information et de la gratuité démultipliée par l'avènement du web (voici [un texte](#) ou [une courte vidéo](#) pour comprendre cette notion);

le web affectif, qui montrent comment les industries du numérique jouent sur les ressorts affectifs des internautes pour capter et monétiser leur attention (voici encore [un texte](#) ou [une courte vidéo](#) pour comprendre cette notion).

Nous ne sommes donc pas captés par nos écrans par hasard :

**LES PROGRAMMES AUXQUELS NOUS SOMMES
CONFRONTÉS ONT ÉTÉ ÉLABORÉS POUR CAPTER
NOTRE ATTENTION, ET, A FORTIORI, L'ATTENTION
PLUS LIBRE DE NOS ENFANTS ET ADOLESCENTS.**

Dans ces conditions, il est souvent difficile d'imposer des limites dans l'utilisation d'appareils connectés. Mais **la bonne nouvelle, c'est que le confinement nous donne du temps pour prendre ce problème à bras le corps** et le traiter en famille.

DES OUTILS SÉCURISÉS ET RESPECTUEUX DE VOS DONNÉES

Aussi voici quelques propositions que vous pouvez mettre en œuvre facilement chez vous et avec vos proches, et qui ont pour point commun d'être fonctionnelles, simples et le plus possible respectueuses de votre vie privée et de vos données personnelles.

UNE MESSAGERIE PROTÉGÉE

On utilise aujourd'hui très fréquemment une messagerie pour ses communications amicales, familiales et professionnelles. **Mais lorsqu'on utilise WhatsApp, c'est Facebook qui récupère ces données et les monétisent auprès de... n'importe quel demandeur !!** Cela a donné lieu à [plusieurs scandales](#) en 2018, et depuis...

IL EXISTE POUTANT D'AUTRES MESSAGERIES QUI PROTÈGENT LES DONNÉES DE LEURS USAGERS, ET VOICI LA PLUS SÛRE D'ENTRE ELLES :

Signal est une messagerie qui permet d'envoyer des messages chiffrés de bout en bout; les messages sont chiffrés même sur les serveurs de Signal ; c'est l'application de messagerie la plus sûre au monde, d'après plusieurs spécialistes (voir [l'histoire de sa](#)

création sur Wikipédia). L'application est de plus, multiplateforme (disponible sous iOS, macOS, Android, Windows et Linux), c'est-à-dire que vous pouvez utiliser Signal sur votre ordinateur, votre tablette et votre téléphone, quel que soit leur système d'exploitation.



DES OUTILS DE WEB-CONFÉRENCE SÉCURISÉS

Google, Apple, et Microsoft proposent des outils de vidéoconférences, sans compter les compagnies émergentes comme Zoom. Mais ces compagnies récupèrent vos données d'utilisation pour en faire commerce (Apple s'en sert pour son propre usage, mais ne gagne pas directement d'argent avec) ; **d'autres logiciels, issus de la mouvance du logiciel libre, se proposent de vous fournir un service équivalent sans se rémunérer en vendant ou louant vos données :**

- **Jitsi** est un service multiplateforme qui permet de créer des conversations en visioconférence depuis un navigateur ou une application (disponible sous iOS, macOS, Android, Windows et différentes distributions de Linux)
- **Jami** est un logiciel qui permet aux utilisateurs de passer des appels téléphoniques ou vidéo via Internet, ainsi que le partage d'écran ; open-source, il est disponible sur Windows, MacOs, Linux,



ainsi que sur Android et iOS. Jami utilise le chiffrement de bout en bout pour le chat, la vidéo et la voix.

DES NAVIGATEURS QUI RESPECTENT VOTRE VIE PRIVÉE

Non, Chrome n'est pas respectueux de vos données, qui sont la principale source de revenus de Google.

Dès lors que vous êtes associé à votre compte Google, tout ce que vous faites est enregistré par la compagnie et vient alimenter sa gigantesque base de données, et Chrome est truffé de traqueurs récupérant en permanence toutes vos données de navigation.

IL EXISTE D'AUTRES NAVIGATEURS, TOUT AUSSI FONCTIONNELS, QUI SONT CONSTRUITS POUR RESPECTER VOTRE VIE PRIVÉE PENDANT QUE VOUS LES UTILISEZ :

- **Firefox**, géré par la Fondation Mozilla, est le plus connu des navigateurs libres ayant pour vocation de protéger les données des utilisateurs.



- **Brave** est un navigateur libre open source qui utilise Chromium (le moteur de recherche libre de Chrome), lui ajoute des fonctions de sécurité et de protection des données personnelles, sans utiliser les outils de *tracking* de Google.



DES MOTEURS DE RECHERCHE RESPECTUEUX DE VOS DONNÉES

Oui **Google** est le moteur de recherche par excellence, mais **c'est aussi 80% des revenus de la maison mère Alphabet, gagnés en louant vos questions, les mots clés que vous utilisez, et surtout vos habitudes numériques aux plus offrants.**

D'AUTRES MOTEURS DE RECHERCHE SONT CONSTRUITS, POUR NE PAS ASPIRER VOS DONNÉES ET POUR RESPECTER VOTRE VIE PRIVÉE :

- **Startpage** a été créé par des anciens de Google qui ont quitté l'entreprise quand elle a pris un virage plus mercantile; c'est un métamoteur, qui utilise le moteur de Google en lui cachant vos données personnelles ; il vous rend anonyme lorsque vous faites des recherches en passant par lui ;



– **Qwant** est une initiative française, construite par défaut pour respecter vos données ;



– **DuckDuckGo** est aussi un moteur de recherche construit pour respecter votre privée ;



– **Lilo** est un moteur de recherche français dont les publicités servent en partie à financer des projets sociaux et environnementaux.

Vous pouvez aussi installer certains de ces moteurs de recherche sur vos téléphones et vos tablettes (seul DuckDuckGo est installable sur iOS).

DES COURRIERS ÉLECTRONIQUES PROTÉGÉS DE BOUT EN BOUT

On peut pousser cette réflexion en pensant au plus vieil outil de communication d'internet : le courrier électronique.

Quand vous créez une adresse Gmail, vous donnez l'autorisation à Google de se servir de tous les contenus de vos mails et des mails que vous recevez sur votre boîte.

MAIS IL EXISTE PLUSIEURS SERVICES DE MAILS QUI PROTÈGENT DE BOUT EN BOUT VOS DONNÉES ET CELLES DE VOS INTERLOCUTEURS POUR QU'ELLES NE SOIENT PAS ACCESSIBLES HORS DE VOS APPAREILS :

- [Tutanota](#) est un service de mails *open source* et crypté de bout en bout ;
- [ProtonMail](#) est un service identique, développé et hébergé en Suisse.

DES OUVRAGES ET DES SITES DE RÉFÉRENCE

Pour terminer ce petit guide, vous trouverez ci-dessous trois références à visée pratique pour vous aider à retrouver un usage libre du web, dans l'esprit de ses pionniers, et éloigné autant que possible de l'appétit vorace des entreprises qui prospèrent sur nos données personnelles.

- un ouvrage libre et gratuit, et s'intitule [Libertés numériques](#) ; il est écrit par Christophe Masutti, un des contributeurs réguliers de Framasoft, l'association bien connue de promotion du logiciel libre ;
- un ouvrage intitulé [surveillance://](#) , écrit par Tristan Nitot, qui a été à l'initiative de la création de la fondation Mozilla Europe qu'il a présidé plusieurs années ; l'ouvrage coûte moins de 10€ en version numérique ;
- enfin, je ne peux pas terminer ce guide sans mentionner [Dégooglisons Internet](#) l'initiative incroyable de l'association Framasoft qui a mis au point, en trois ans, un programme réussi de remplacement des services en ligne des multinationales du numérique par des services libres équivalents.

À PROPOS DE L'AUTEUR

Patrick Mpondo-Dicka est enseignant-chercheur en Sciences de l'Information et de la Communication à l'université Toulouse Jean-Jaurès.

Il enseigne au département [Art&Com](#), et officie en tant que chercheur au sein du [LERASS](#) (Laboratoire d'Etudes et de Recherches Appliquées en Sciences Sociales).

Il est co-directeur du colloque scientifique [Ludovia](#) depuis une quinzaine d'années.

Il intervient régulièrement auprès de la Maison des Adolescents de la Haute-Garonne sur les questions liées au numérique et à l'éducation.

Vous pouvez le joindre à l'adresse mail suivante :
patrick@mpondo-dicka.net