Un manifeste des données utilisateurs, aujourd'hui ?

Le User Data Manifesto a été initié par Frank Karlitschek un militant du logiciel libre qui a fondé Nextcloud et Owncloud et participé à d'autres projets open source.
La source de cette traduction française figure sur ce dépôt Github, la dernière traduction que je reprends ici avec quelques modifications mineures date de 2015 et semble essentiellement due à Hugo Roy. Le dernier contributeur en date est Philippe Batailler.

> ***[EDIT]*** *Hugo Roy nous apporte cette précision :*
> *hello – la traduction est bien de moi, mais le texte en anglais aussi la version actuelle du manifeste est une œuvre collaborative avec Frank et @jancborchardt*

À la lecture on est frappé de la pertinence des propositions, cependant malgré quelques avancées du côté des directives de l'Union européenne, certains droits revendiqués ici sont encore à conquérir ! Et après 4 ans il faudrait peut-être ajouter d'autres éléments à ce manifeste : le droit d'échapper au pistage publicitaire, le droit d'anonymiser vraiment sa navigation, le droit de ne pas fournir ses données biométriques etc.

Mais c'est plutôt à vous de dire ce qui manque ou est à modifier dans ce manifeste pour qu'il soit solidement inscrit dans les lois et les usages. Comme toujours, le commentaires sont ouverts et modérés.

Manifeste des données utilisateur

Ce manifeste a pour but de définir les droits fondamentaux des utilisateurs sur leurs données à l'ère d'Internet. Chacun devrait être libre sans avoir à faire allégeance aux fournisseurs de service.

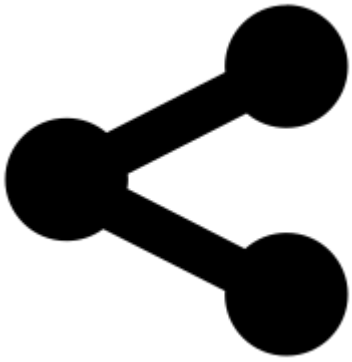
Par **données utilisateur**, on entend les données envoyées par un utilisateur ou

une utilisatrice pour son propre usage.

Par exemple, les données utilisateur comprennent :

- les fichiers qu'un utilisateur ou qu'une utilisatrice synchronise entre plusieurs appareils ou qu'il ou elle partage avec un·e proche
- une bibliothèque d'albums photos, de livres ou d'autres fichiers qu'un utilisateur envoie depuis son appareil afin de pouvoir lire, voir, et modifier tout cela en ligne
- les données générées par un appareil de l'utilisateur (comme un thermostat ou une montre connectée) et envoyées vers un serveur
- les requêtes d'un utilisateur à un moteur de recherche, si de telles requêtes sont enregistrées comme telles

Ainsi, les utilisateurs devraient pouvoir…



1. Maîtriser leur accès à leurs données

Les données explicitement et volontairement envoyées par une utilisatrice devraient être sous la pleine maîtrise de l'utilisatrice. Les utilisateurs devraient être capables de décider à qui accorder un accès direct à leurs données et avec quelles permissions et licences cet accès devrait être accordé.

Lorsque les utilisateurs maîtrisent l'accès aux données qu'ils envoient, les données censées restées privées ou partagées à un cercle restreint ne devraient pas être rendues accessibles au fournisseur du service, ni divulguées aux États.

Cela implique que le droit d'utiliser le chiffrement ne devrait jamais être bafoué.

Cela implique également que lorsque des utilisateurs n'ont pas la pleine maîtrise sur l'envoi de leurs données (par exemple s'ils n'utilisent pas le chiffrement avant l'envoi) un fournisseur de service **ne** doit **pas** :

- forcer les utilisateurs à divulguer des données privées (ce qui inclut la correspondance privée) pour eux, ni
- imposer des conditions de licence (ex. : de droit d'auteur ou d'exploitation des données personnelles) qui vont au-delà de ce qui est nécessaire pour l'objectif du service.

Lorsque les utilisateurs rendent des données accessibles à d'autres, qu'il s'agisse d'un groupe de gens restreint ou d'un groupe plus large, ils devraient pouvoir décider sous quelles permissions l'accès à leurs données est autorisé. Cependant, ce droit n'est pas absolu et ne devrait pas empiéter sur le droit des tierces personnes à utiliser et exploiter ces données une fois qu'elles leur ont été rendues accessibles. Qui plus est, cela ne signifie pas que les utilisateurs devraient avoir le droit d'imposer des restrictions injustes à d'autres personnes. Dans tous les cas, les systèmes techniques ne doivent pas être conçus pour faire appliquer de telles restrictions (par exemple avec des DRM).

Les données reçues, générées ou collectées à partir de l'activité des utilisateurs dans l'utilisation du service (ex. : les métadonnées ou les données du graphe social) devraient leur être rendues accessibles et être également sous leur maîtrise. Si cette maîtrise n'est pas possible, alors ce type de données devrait être anonyme ou bien ne pas être stockée pour une période plus longue que nécessaire.

Certains services permettent aux utilisateurs de soumettre des données avec l'intention de les rendre publiquement accessibles à toutes et à tous. Y compris dans ces cas de figure, quelques données utilisateur restent privées (ex. : les métadonnées ou les données du graphe social). L'utilisatrice et l'utilisateur devraient pouvoir contrôler aussi ces données.

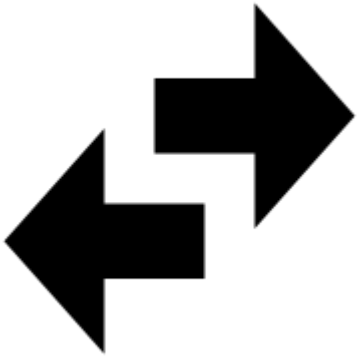
2. Savoir comment les données sont stockées

Quand les données sont envoyées à un fournisseur de service particulier, les utilisateurs et utilisatrices devraient être informé·e·s du lieu de stockage des données du fournisseur de service, de la durée, de la juridiction dans laquelle le fournisseur de service particulier opère et des lois qui s'y appliquent.

Lorsque les utilisateurs utilisent des services centralisés pour envoyer leurs données à un fournisseur de stockage particulier plutôt que de reposer sur des systèmes pair à pair, il est important de savoir où les fournisseurs pourraient stocker ces données car ils pourraient être obligés par les États à divulguer ces données qu'ils ont en leur possession.

Ce point est sans objet si les utilisateurs sont capables de stocker leurs propres données sur leurs appareils (ex. : des serveurs) dans leur environnement personnel et sous leur contrôle direct ou bien s'ils font confiance à des systèmes sans contrôle centralisé (ex. : le pair à pair).

Les utilisateurs ne devraient pas reposer sur des services centralisés. Les systèmes pair à pair et les applications *unhosted* sont un moyen d'y arriver. À long terme, tous les utilisateurs devraient être capables d'avoir leur propre serveur avec des logiciels libres.



3. Être libres de choisir une plateforme

Les utilisatrices devraient toujours être en mesure d'extraire leurs données d'un service à tout moment sans subir l'enfermement propriétaire.

Les utilisateurs ne devraient pas être bloqués par une solution technique particulière. C'est pourquoi ils devraient toujours être capables de quitter une plateforme et de s'installer ailleurs.

Les formats ouverts sont nécessaires pour garantir cela. Évidemment, sans le code source des programmes utilisés pour les données utilisateurs, cela n'est pas pratique. C'est pourquoi des programmes devraient être distribués sous une licence libre.

Si les utilisateurs ont ces droits, ils ont la maîtrise de leurs données plutôt que d'être sous la coupe des fournisseurs de service.

De nombreux services qui gèrent les données utilisateur à ce jour sont gratuits, mais cela ne signifie pas qu'ils soient libres. Plutôt que de payer avec de l'argent, les utilisateurs font allégeance aux fournisseurs de services pour que ceux-ci puissent exploiter les données utilisateurs (par ex. en les vendant, en offrant des licences ou en construisant des profils pour les annonceurs publicitaires).

Abandonner ainsi la maîtrise de sa vie privée et d'autres droits semble être un acte trivial pour de nombreuses personnes, un faible prix à payer en échange du confort que ces services Internet apportent.

Les fournisseurs de service ont ainsi été obligés de transformer leurs précieux services Internet en systèmes massifs et centralisés de surveillance. Il est crucial

que chacun réalise et comprenne cela, puisqu'il s'agit d'une menace importante pour les libertés de l'humanité et le respect de la vie privée de chacun.

Enfin, pour assurer que les données utilisateurs soient sous la maîtrise des utilisateurs, les meilleurs conceptions techniques incluent les systèmes distribués ou pair-à-pair, ainsi que les applications *unhosted*. Juridiquement, cela signifie que les conditions générales d'utilisation devraient respecter les droits des utilisateurs et leur donner la possibilité d'exercer leurs droits aux données définis dans ce manifeste.

Illustration réalisée avec https://framalab.org/gknd-creator/