

Choisir un nouveau fournisseur de mail

De quoi parle-t-on ?

Quitter les fournisseurs Google, Apple, Microsoft, Yahoo ... pour écrire des messages à sa famille, ses amis, ses fournisseurs, collègues ... la question semble étrange à certains ?

Et pourtant, cela relève à vrai dire du bon sens !

Pour mes usages personnels :

- les courriers que j'envoie et les personnes avec qui je corresponds font partie de mon intimité.
- pour la plupart, je ne les ferais pas lire, systématiquement au moins, à mes enfants ou aux personnes avec qui je partage ma vie.
- je ne donnerais pas à lire à mes amis les courriers de mon médecin, ni l'inverse

Pour les usages professionnels :

- je ne donnerais pas à lire les mails échangés avec mes clients à mes fournisseurs, ni l'inverse.
- je ne donnerais pas à lire mes messages avec mes élèves à d'autres enseignants, ni l'inverse.
- je ne donnerais pas à lire mes projets d'évolution, mes devis (à quoi peut donc servir un devis potentiellement partagé entre tous les concurrents prétendants).

Bref, l'énumération est sans fin. Pourtant, si je lis attentivement les conditions d'utilisation des services proposés "gratuitement" par les GAFAM et que je les accepte, je donne définitivement, totalement (ou parfois en partie), à ces entreprises un droit d'utiliser mes données à leur gré. Ajoutons à cela que leur rémunération des services qu'ils me proposent provient en grande partie de la vente de mes données à des fins commerciales, politiques, etc.

On entend souvent "mes données n'intéressent personne".

On entend moins souvent "Mon profil c'est à dire ma santé, mes opinions politiques, philosophiques, mes habitudes alimentaires, mon niveau de vie, ma vie sentimentale ... n'intéressent personne".

C'est de cela dont il est question ici : si en achetant des données à Google/Amazon/Microsoft/Apple, je peux vendre mon nouveau produit à la cible pour laquelle je l'ai fabriqué, cela vaut de l'or.

Alors, si vous préférez ne pas acheter, vendre, chercher un travail ou fréquenter vos amis à découvert, dégagez donc ces importuns et choisissez des fournisseurs plus vertueux !

Parmi ceux que vous pouvez dégager, les plus problématique sont Gmail de Google, Outlook de Microsoft, Yahoo et autres mastodontes de l'industrie informatique mondiale. A ce propos, vous pouvez lire le paragraphe Licence d'utilisation de vos contenus dans les [conditions d'utilisation Google/Gmail](#):



« Par le biais de cette licence, vous autorisez Google à utiliser vos droits de propriété



intellectuelle sur vos contenus (tels que les droits d'auteur et les marques enregistrées), ainsi que les droits immatériels que vous détenez sur vos contenus (tels que les droits à l'image).».

ceci sont les conditions que vous avez acceptées au moment où vous avez créé votre boîte Gmail; réfléchissez-y !.

Et le RGPD ?

Depuis 2018, le RGPD ou « Règlement Général sur la Protection des Données » (en anglais GDPR ou « General Data Protection Regulation » établit des règles strictes pour protéger les données des citoyens européens.

Un principe fondamental du RGPD est de demander un acquiescement conscient et éclairé des individus ou des entreprises pour l'exploitation de leurs données numériques. Ce règlement est valable pour tous les citoyens européens **et pour toutes leurs données hébergées sur le territoire européen.**

L'objet de cette publication n'est pas de rentrer dans le détail du RGPD mais de vous donner quelques indications pour respecter le RGPD et être protégé dans vos usages pour les boîtes mail:

- exclure tous les fournisseurs qui hébergent vos données hors du territoire européen : exit Gmail, Yahoo, etc
- exclure toutes les antennes européennes des entreprises dont la maison mère est hors-territoire européen (qui peuvent sauvegarder, répliquer, intervenir techniquement sur vos données) : exit Outlook, Hotmail, Live, Telegram, etc
- exclure tous les fournisseurs qui utilisent des logiciels dont ils ne maîtrisent pas le code source (ex: Outlook chez OVH, etc)
- des exceptions : certains territoires ont des règlements compatibles avec le RGPD et certaines entreprises font de la sécurité des données et de la protection de votre vie privée un métier (ex Riseup, Protonmail) 🤖

Et les boîtes mail proposées par mon fournisseur d'accès ?

Ces entreprises (Bouygue Télécom, Free, Orange, SFR) obéissent par nature à plusieurs exigences du RGPD puisqu'elles ont leur siège sur le territoire national et donc européen. Toutefois, la plupart ne sont pas vertueuses, elle ont souvent une relation incestueuse avec les institutions de l'État et font un usage commercial de vos données : je viens de changer de fournisseur d'accès tout en gardant ma boîte mail chez mon ancien FAI, je n'utilise plus cette adresse qu'en lecture et pourtant, en quelques semaines les spams ont décuplé ! Bizarre !

De plus, les serveurs des fournisseurs d'accès (FAI) nationaux qui hébergent ces boîtes mail collectent déjà beaucoup d'informations sur vos usages du Web et sur votre téléphonie ... pas la peine de leur en donner plus, *"ma vie privée est également (et surtout ?) privée pour les services de l'État où je vis !"*

Alors qui choisir ?

Vous commencez à vous demander si vous n'allez pas racheter un stylo-plume ?

Rassurez-vous, en étant très exigeant, vous avez toujours l'embarras du choix:

Fournisseur	Pays d'hébergement	Cloud associé	Chiffrement(1) transport / stockage	Coût
E foundation	France	oui	oui / ?	gratuit en version de base
Disroot	Pays-Bas associatif	oui	oui / oui	gratuit, dons souhaités
Zaclys	France associatif	oui	oui / ?	payant 5€/an ou 10€/an
Posteo	Allemagne	non	oui / oui sauf les sujets/objets/titres	payant €1.00/mois
Proton Mail	Suisse	non	oui / non chiffrement entre boîtes Proton sauf les sujets/objets/titres clés stockées chez Proton sur serveur distinct	gratuit jusqu'à 500 MB (hors SMTP) \$4.00/mo
Riseup	USA associatif	non	oui / non livraisons FAI destinataires via TOR	gratuit dons souhaités

(1) le chiffrement des mails couvre plusieurs réalités :

- chiffrement des mails pendant le transport de votre appareil au serveur de mail de votre fournisseur (par l'usage de protocoles chiffrés)
- chiffrement sur le serveur de votre fournisseur (avec des clés de chiffrement stockées chez vous ou des clés stockées chez ce fournisseur)
- chiffrement du transport depuis votre fournisseur jusqu'au fournisseur de votre correspondant
- chiffrement sur le serveur du fournisseur de votre correspondant (avec quelles clés, stockées où ?)
- chiffrement de la communication depuis le serveur du fournisseur de votre correspondant à l'appareil de votre correspondant



Où on s'aperçoit que ni vous, ni votre fournisseur ne maîtrise toute la chaîne et que les possibilités de fuites sont multiples.

Si vous manipulez des données sensibles, un bon choix serait d'utiliser un protocole de chiffrement que votre correspondant et vous maîtrisez de bout en bout. Cela existe (PGP) et vous pouvez l'utiliser à condition d'échanger une clé avec vos correspondants



(chacun sa clé), ajouter l'usage d'un VPN (pour que votre hébergeur ne connaisse pas l'adresse IP d'où vous écrivez et de mettre TOR par dessus l'ensemble pour que personne ne puisse sniffer vos échanges à la sortie du VPN. Cela est l'objet d'autres tuto 😊 !

Revenons au choix de votre fournisseur de boîte mail : nous conseillons **Disroot**, **e foundation** ou **Zaclys**. Protonmail peut aussi être un choix opportun.



Nous proposons de préférer les fournisseurs que qualifierons de **vertueux**, ils sont associatifs ou militants (dans l'ordre de mes préférences Disroot, E foundation, Zaclys, Proton Mail), parfois payants ou partiellement payants (ce qui peut bien paraître normal : imaginons-nous le courrier postal gratuit ?).

On aussi peut citer les professionnels sur-mesure comme OVH ou Gandi.

— [André Vanderlynden](#) 2022/02/10 21:00   

From: <https://informethic.net/dokuwiki/> - Ethique et Informatique ... dietétique

Permanent link: <https://informethic.net/dokuwiki/doku.php?id=clicsetdeclics:choisir-fournisseur-boite-mail&rev=1645532748>

Last update: 2022/02/22 13:25

