Ne plus nourrir les monstres

De toutes part des initiatives et des projets surgissent pour rendre aux utilisateurs la maîtrise de leurs usages numériques et de leur confidentialité. Mentionnons par exemple l'intérêt grandissant pour le réseau Tor (et l'usage de TorBrowser), les efforts pour démocratiser le chiffrement des communications, l'initiative de Mozilla pour conjuguer la décentralisation, le chiffrement et le logiciel libre ou encore la seconde jeunesse du projet caliop, bien d'autres encore…

Mais en attendant, que proposer aux utilisateurs qui sont encore très largement captifs des silos prédateurs ? Chez Framasoft, comme nous l'avons déjà fait à plusieurs reprises (framapad, framanews, framabag…), nous proposerons encore des solutions et services libres alternatifs utilisables par tout un chacun.

C'est un peu dans cette logique que s'inscrit la conclusion toute simple de l'article de Clochix ci-dessous. Comme la soumission au tyran exposée par La Boétie, notre servitude est volontaire : c'est nous qui avons alimenté délibérément le monstre qui nous effraie maintenant, et sa puissance (qui oserait défier Google tant son pouvoir est étendu ?) peut se désagréger si nous ne la reconnaissons plus pour telle.

> *D'où tire-t-il tous ces yeux qui vous épient, si ce n'est de vous ? (…) Soyez résolus à ne plus servir, et vous voilà libres. Je ne vous demande pas de le pousser, de l'ébranler, mais seulement de ne plus le soutenir, et vous le verrez, tel un grand colosse dont on a brisé la base, fondre sous son poids et se rompre.*

Nous reprenons ici l'article initialement publié par Clochix sur son blog. Clochix se présente modestement comme « un apprenti geek intéressé par la liberté ».

Diversifions

par **Clochix**

Souvent, lorsqu'un administrateur se connecte à une machine, celle-ci l'accueille d'un salutaire rappel : « un grand pouvoir donne de grandes responsabilités ». En informatique, les administrateurs (de réseaux, de machines, de bases de données, etc.) ont effectivement un grand pouvoir. Ils ont accès à de très nombreuses informations, directement à la source, sans être soumis à des restrictions d'accès. Ils ont souvent la capacité de lire la plupart des messages électroniques échangés et des documents internes de l'entreprise. Parfois, ils sont même amenés à le faire dans le cadre de leurs missions. Pouvoir accéder à des informations sensibles leur donne donc un certain pouvoir, et les soumet à une double responsabilité. Résister à la tentation d'abuser de leur pouvoir (aller lire des documents pour savoir si la direction prépare des licenciements ou si la jolie fille de la compta est célibataire), résister aux pressions (internes de sa hiérarchie qui voudrait fliquer un salarié, externes de personnes qui voudraient des renseignements sur la structure).

Tout pouvoir porte en lui la tentation de l'abus et le risque du détournement. Pour se protéger des abus, on ne peut se reposer uniquement sur la capacité des individus à résister à la tentation et à la pression. Et l'un des meilleurs garde-fous est à mon sens, non de contrôler les individus en situation de puissance, mais de limiter au maximum la concentration du pouvoir. Moins il y de pouvoir, moins on est tenté d'en abuser, et surtout moins les conséquences des abus sont dommageables. Il faut donc veiller à ne pas laisser trop de pouvoir s'accumuler entre les mêmes mains. Segmenter le

système d'information pour éviter qu'un unique individu ait toutes les clés. Diversifier l'environnement pour éviter les points individuels de défaillance, que cette défaillance soit un panne, une attaque ou une indiscrétion.

Il y a quelques jours, quelqu'un a signalé que pour utiliser Hangout, un service de visioconférence de Google, il fallait désormais obligatoirement utiliser Chrome (alors que le service semble parfaitement fonctionner dans Firefox). Devant le tollé, un ingénieur de Google a rétropédalé, invoquant une simple erreur de formulation. Mais les faits sont têtus : trois jours plus tard, la page n'a toujours pas été corrigée (et j'avoue avoir vraiment beaucoup de mal à croire au caractère non intentionnel de cette restriction).

Ça n'est bien sûr qu'une anecdote minuscule. Google triche un peu pour inciter les internautes à installer et utiliser son navigateur. Et cette ridicule malhonnêteté n'aurait guère de conséquences si son auteur n'était l'un des principaux fournisseur de logiciels et de services au monde. Mais dans la position où est Google, cette simple magouille va probablement se traduire par quelques milliers d'utilisateurs qui migreront, sans vraiment l'avoir voulu, vers Chrome. Et les petits réseaux faisant les grandes rivières, de démonstrations réservées à Chrome en installations cachées dans les bagages d'autres logiciels, le nombre d'utilisateurs des produits de Google s'accroît. La quantité d'informations que Google collecte et, partant, sa capacité d'action augmente. Plus une entité est en situation de pouvoir, plus grande est la tentation d'abuser un peu de ce pouvoir à la marge, sur des points qui semblent sans conséquences. Et plus vastes deviennent les conséquences de ces micro-abus.

Le pouvoir de Google est aujourd'hui gigantesque, probablement bien plus important que la majorité d'entre nous ne l'imagine. *Business Insider* a récemment publié une interminable liste des multiples racines qui chaque jour alimentent davantage en données le ventre de l'ogre insatiable. Google a des capteurs

partout. Sur internet, bien sûr, mais aussi dans le monde analogique, avec ses téléphones, ses satellites, demain ses voitures, lunettes, objets connectés… La quantité d'informations ainsi collectée dépasse l'imagination, tout comme les innombrables usages qu'il pourrait en faire. La puissance de Google est aujourd'hui terrifiante.

Et, sans vouloir retirer de mérite à ses ingénieurs, cette puissance, c'est en grande partie nous qui la confortons, qui la démultiplions chaque jour.

S'il est des individus qui cherchent explicitement la puissance, force est d'admettre que souvent c'est nous-mêmes qui déléguons notre pouvoir et créons les monstres devant lesquels nous tremblons ensuite. Les silos ne deviennent dangereux parce que nous leur en donnons les moyens. Personne ne nous oblige à abonder leur puissance, du moins au début. Mais chaque fois que nous utilisons Chrome, Gmail, Android, chaque fois que nous achetons un iGadget, racontons notre vie sur Facebook, commandons sur Amazon, nous leur donnons un tout petit peu plus d'informations, nous renforçons leur pouvoir, augmentons la tentation qu'ils en abusent, et les conséquences du moindre abus (et la liste de ces petits abus est déjà longue et publique, des censures d'Apple dans sa boutique aux pressions d'Amazon sur ses fournisseurs).

Le problème n'est donc pas Google ou Apple, Facebook, Microsoft ou Amazon, il est hors-sujet de disserter sur l'humanisme des intentions de leurs dirigeants ou leur capacité à résister à la pression de gouvernements ou de mafias. Inutile d'essayer de deviner comment toutes les informations que nous leur confions pourraient un jour se retourner contre nous. Non, l'unique question qui vaille est de savoir s'il est sain de laisser une aussi phénoménale puissance s'accumuler entre les mains d'un petit nombre d'acteurs, quels qu'ils soient.

Si vous pensez que la réponse à cette question est non, qu'il

n’est pas sain que quiconque dispose d’autant d’informations, donc de pouvoir, alors il est grand temps d’agir, pendant que nous le pouvons encore. Et ça tombe bien, car l’effort pour agir concrètement sur la situation n’est pas insurmontable. Il suffit de ne plus mettre tous nos œufs dans le même panier. Ne plus confier tous nos échanges électroniques à deux ou trois acteurs. Ne plus tous et toutes utiliser les mêmes logiciels, systèmes d’exploitation, navigateur, etc.

Diversifier à défaut de décentraliser

En matière d’information comme dans la nature, c’est la diversité qui fait la force et la résilience d’un système. Il ne s’agit pas forcément de reprendre nous-mêmes le contrôle de toutes nos données. Je suis bien conscient que peu de gens ont les ressources (temps, compétences…) et l’envie de le faire. Mais de ne pas tout confier au même prestataire. De bâtir le meilleur garde-fou contre le totalitarisme, un réseau divers.