Dans l'ère électronique où nous vivons, le droit à une vie privée est un élément essentiel d'une société libre et ouverte. Le domaine du privé n'est pas celui de la dissimulation. Quelque chose relève du privé dès lors que nous ne souhaitons pas le rendre accessible au monde entier. Un secret désigne une chose que nous ne souhaitons communiquer à personne.

Le droit à la vie privée implique de pouvoir choisir ce que nous souhaitons révéler de nous-même au monde.

Lorsque deux personnes ou groupes entrent en relation, chacun va conserver une mémoire de cette interaction. Chacun pourra par la suite évoquer ce qu'il en a mémorisé. Comment pourrait-on l'empêcher ? On pourrait voter des lois pour l'interdire, mais la liberté de parole, plus encore que le droit à une vie privée, est un élément fondamental d'une société libre et ouverte ; il n'est pas envisageable de restreindre cette liberté de parole. Si plusieurs personnes s'expriment sur un même forum, chacun peut parler à tous les autres et la connaissance progresse à partir de tous les points de vue agrégés. La puissance des communications électroniques a rendu possible cette expression collective. Cela ne va pas disparaître juste parce que quelqu'un s'y opposerait.

Puisque nous désirons préserver notre vie privée, nous devons nous assurer que chaque intervenant d'une transaction n'ait connaissance que de ce qui est directement nécessaire à cette transaction. Etant donné que toute information révélée est en mesure d'être divulguée par la suite, nous devons veiller à ne révéler qu'un minimum.

Dans la plupart des situations, notre identité personnelle n'est pas un facteur essentiel. Lorsque j'achète un magazine et donne mes pièces au kiosquier, il n'a pas à savoir qui je suis. Lorsque je demande à mon fournisseur de courrier électronique d'envoyer et recevoir des messages, il n'a pas à savoir à qui je parle, ce que je raconte, ou ce que d'autres ont à me dire ; tout ce qu'il a besoin de savoir, c'est comment envoyer le message à bon port et combien je lui dois pour ce service. Lorsque mon identité est révélée par le mécanisme inhérent à ces échanges, je n'ai pas de vie privée. Je ne suis alors plus en mesure de révéler ce que je veux à mon sujet, je dois toujours révéler qui je suis.

Qu’en conclure ? Que la vie privée dans une société libre et ouverte nécessite des systèmes de transactions anonymes. Jusqu’à présent, le cash a été le principal système de ce type. Un système de transaction anonyme n’est pas un système de transaction secrète. Un système anonyme donne aux individus le pouvoir de révéler leur identité s’ils le souhaitent et seulement quand ils le souhaitent. Telle est l’essence du droit à une vie privée.

Dans une société ouverte, la vie privée a besoin de cryptographie. Si je dis quelque chose, je veux que cela ne soit reçu que par ceux auxquels je l’ai destiné. Si le contenu de mon discours est accessible au monde entier, je n’ai plus de vie privée. Le chiffrement sert à marquer ce désir pour une vie privée. Si le chiffrement est faible, cela indique que mon désir de vie privée l’est aussi. Et pour qu’il soit possible de révéler son identité avec assurance lorsqu’une communication est par défaut anonyme, il est nécessaire de détenir la signature cryptographique.

Nous ne pouvons pas attendre des gouvernements, des entreprises ou organisations sans visage de nous accorder le droit à la vie privée du fait de leur simple bienveillance. Il est dans leur intérêt de communiquer de l’information à propos de nous, et nous devons nous attendre à ce qu’ils le fassent. Essayer de les en empêcher serait s’abuser sur la nature de l’information. L’information ne cherche pas seulement à être libre, elle aspire de tout son être à être libre. Par nature, l’information cherche à occuper tout l’espace disponible. L’information est la cousine jeune et agile de la Rumeur. Elle a une démarche plus souple, elle voit partout, elle en sait davantage et comprend moins que la Rumeur.

Si nous souhaitons jouir d’une vie privée, nous devons la défendre. Nous devons nous rassembler et créer des systèmes qui permettent des transactions anonymes. Les gens ont défendu leur vie privée durant des siècles avec des chuchotements, de l’obscurité, des enveloppes, des portes closes, des salutations codées et des messagers. Avec ces techniques anciennes, protéger sa vie privée n’était pas aisé. Les technologies électroniques sont bien plus efficaces.

Nous, les Cypherpunks, sommes voués à l’édification de systèmes anonymes. Nous défendons notre droit à la vie privée avec la cryptographie, des systèmes de messagerie anonyme, des signatures numériques et de l’argent électronique.

Les Cypherpunks écrivent du code. Nous savons qu'il faut produire du logiciel afin de pouvoir protéger la vie privée, et nous allons le faire. Nous allons le publier afin que nos camarades Cypherpunks puissent l'utiliser et jouer avec. Notre code est libre d'accès, pour tous et partout. Cela nous est égal que vous l'approuviez ou non. Nous savons que le code est indestructible et qu'un système largement décentralisé ne peut pas être arrêté.

Les Cypherpunks s'opposent aux réglementations sur la cryptographie car le chiffrement est fondamentalement un acte privé. L'acte même de chiffrer soustrait l'information de la sphère publique. Même les lois contre la cryptographie s'arrêtent aux frontières d'une nation et à sa capacité de recours à la violence. Inéluctablement, la cryptographie se répandra sur la terre entière et avec elle, les systèmes de transactions anonymes qu'elle rend possible.

Pour que la vie privée soit universellement respectée elle doit faire partie du contrat social. Les gens doivent se rassembler et déployer ensemble ces systèmes dans l'intérêt commun. La vie privée de chacun ne sera protégée que si tous y contribuent. Nous, les Cypherpunks, sommes à l'écoute de vos questions et préoccupations. Nous espérons vous intéresser et vous impliquer, afin d'éviter de nous tromper. Que certains puissent désapprouver nos objectifs ne nous fera cependant pas changer de route.

Les Cypherpunks s'engagent activement à rendre les réseaux plus sûrs pour la vie privée. Agissons de concert, et avec promptitude.

En avant !

Eric Hughes

9 Mars 1993

<hughes@soda.berkeley.edu>

———

Traduction de « A Cypherpunk’s Manifesto » (9 Mars 1993) de Eric Hughes, par Daniel Ichbiah, Philippe Honigman et Nathan Sexer.

Source: https://www.activism.net/cypherpunk/manifesto.html