Surveillance:// par Tristan Nitot

« […] contrôler l'outil informatique pour éviter qu'il ne nous contrôle ou permette à d'autres de nous contrôler. » ainsi est résumé l'intention de l'auteur. Souvent représenté comme obscure et technique, Tristan Nitot s'attache dans ce petit ouvrage à rendre accessible les mécanismes qui nous traquent sur Internet ainsi que les raisons sous-jacentes à toute personne utilisant quotidiennnement un PC ou un smartphone. Son ouvrage est découpé en 4 parties qui nous guident progressivement de la compréhension à l'action. Ses premiers chapitres sont consacrée à « Pourquoi ? ». Pourquoi et dans quels buts sont captées et analysées des données constituant notre profil virtuel ? Ensuite pourquoi devrions nous se protéger de cette captation ? Une question qui reste sujet à débat dans la société, il est en effet courant de croiser des personnes qui seront d'autant plus prompt à légitimer certains dispositifs, certaines pratiques, quelles se sentiront « innocentes ». Des personnes « qui n'ont rien à cacher » d'autant plus insupportable que la problématique ne se limite pas à une question de flicage contre des méchants (terroristes ou non). C'est un peu ce qui apparaît comme une faiblesse mais qui dessine l'intérêt réel du livre : Tristan Nitot centre avant tout son propos sur le marchandage de nos données par les entreprises proposant des services sur Internet. Et les réponses apportées pour justifier le besoin de se protéger contre ces pratiques sont assez forte de ce point de vue puisqu'elles laissent de coté les pratiques « subversives ». Centrer ne signifit cependant pas nier. La surveillance étatique est évoqué mais sans s'octroyer une place dédiée, particulière, qui permettrait d'en comprendre aussi bien les ressorts techniques que pour les entreprises.

En même temps, il ne s'agit pas d'un ouvrage destiné à des utilisateurs ou utilisatrices avancées. Il s'adresse à des personnes n'ayant aucune notion de la gestion de leur trace sur Internet. Une fois parcouru les débats et principes des questions de surveillance, une seconde partie plus technique s'ouvre pour décrire la manière, les méthodes, les techniques et l'usage qu'ont les entreprises sur Internet des données récupérées. Ici l'auteur propose un éclairant renversement de perspective : nous avons l'impression de consommer Internet, de consommer ses services de partages, d'échanges, d'e-mail, de réseaux sociaux etc. Des services généralement gratuit auquel nous succombons assez simplement. Sauf que « si c'est gratuit c'est vous le produit » et Tristan Nitot nous décrit à la fois les subtilité des contrats d'utilisation indigestes (qu'il résume à chaque fois en 2 lignes) ainsi que ce qu'un serveur distant peut apprendre de notre ordinateur, smartphone, de notre navigation sur Internet…

La seconde moitié du livre s'attache à tracer les solutions pour limiter fortement ce type de surveillance. La troisième partie est centré sur la description et l'explication de principes directeurs telles que l'usage de logiciel libre et opensource, la préférence pour des services décentralisées et la technique de l'auto-hébergement. La 4e partie est une explication technique et une présentation de solutions logiciels pour agir sur les points évoqués dans les chapitres précédents. Les limites apparaissent clairement : il s'agit vraiment de limiter nos traces. Exit donc la navigation anonyme sur Internet via TOR, le chiffrement des données en locale est uniquement évoqué sous forme de liste de solution logiciel et de liens, le chiffrement des e-mails est également renvoyé à un tutoriel extérieur au livre. C'est le résultat du parti pris de l'auteur contre les principales entreprises du net (abrégé GAFAM = Google, Amazon, Facebook, Microsoft). Cela n'en fait pas un livre inutile car appliquer ses conseils c'est déjà diminuer sensiblement ses traces sur les réseaux, et le comprendre c'est être capable d'aller plus loin.

Frédérick Lorie, le 4 mai 2017