




Entretien avec Technopolice



mené le 05.04.23 à Bruxelles

~ Est-ce que tu peux rappeler ce qu'est Technopolice ?

Technopolice est un collectif hétérogène composé de gens ayant des parcours différents : militant·e·s, universitaires, juristes, artistes, technicien·ne·s de l'informatique issu·e·s du logiciel libre qui se sont réuni·e·s. On a repris l'intention de la campagne Technopolice lancée en France par la Quadrature du Net, mobilisé sur des questions liées à la surveillance policière, en transposant ces principes à Bruxelles. Avec Technopolice, on a voulu amener un débat public qui était inexistant sur la surveillance, mais aussi sur la course en avant de la technologie, les systèmes de reconnaissance faciale, les drones et autres outils numériques liés à la 'Smart City'. Bruxelles a un contexte politique particulier, mené par des technophiles pour qui la technologie est la solution à tout, et pour qui c'est un outil neutre.

~ Quelle est votre définition de l'autodéfense numérique ?

Cette notion d'autodéfense numérique vient de l'autodéfense classique, c'est l'idée qu'il y a une attaque, ou du moins quelque chose de l'ordre de l'injustice. On a l'espace numérique, qui peut être un espace de liberté, mais dont le lien avec l'espace physique et sa transformation en grand supermarché pose problème. Ce n'est plus un univers de partage, mais un univers de commerce.

Dans ces pratiques d'autodéfense, on accompagne les personnes dans des changements concrets sur comment se protéger en ligne, la question de la légalité et de l'évolution des droits est quand même présente sur certaines de nos actions puisque nous avons des juristes au sein du collectif. On met par exemple en place des pétitions comme celle contre la reconnaissance faciale à Bruxelles avec la Ligue des droits humains (LDH). (NDLR : pétition 'Protect my face' disponible sur technopolice.be, faite avec une coalition d'associations, dont Collectif Mémoire coloniale et Lutte contre les discriminations, CIRé, Genres Pluriels, Ligue des droits humains, Liga voor mensenrechten, MRAX, Tactic)

~ Quels types d'actions vous menez ? Comment vous vous financez ? Et pourquoi ce modèle ?

Nous mettons en place une multiplicité d'actions, allant de l'édition d'articles critiques, de guides pratiques, mais aussi de cartographies de dispositifs de surveillance

(caméras publiques et privées, ANPR - détectant les plaques d'immatriculation, etc.). Ces dispositifs agissent d'ailleurs de pair avec des dispositifs anti sans-abris, des endroits utilisant la Footfall Analytics (analyse de fréquentation d'un espace), la traque du wifi pour voir combien de temps tu passes devant une vitrine, etc. Autour de ces cartographies, on fait des balades dans la ville (pour faire du repérage avec les membres / usager·e·s / publics d'association qui veulent faire de la sensibilisation), pour ouvrir un dialogue autour des technologies, ce qui se cache derrière et les pouvoirs politiques qui sont en jeu. Ce type de dispositifs est principalement mis en place par les administrations publiques, qui permettent aussi au privé d'établir leurs propres dispositifs de surveillance peu ou pas encadrés.

Au sein de Technopolice, nous introduisons des recours légaux comme la pétition, mais aussi les demandes CADA (Commission d'accès à des documents administratifs). Il s'agit d'une requête que n'importe quelle personne peut adresser à sa commune ou administration pour avoir une transparence sur les détails de travaux, chantiers de l'espace public, donc les montants investis, mais aussi les études menées au préalable. Les autorités répondent avec plus ou moins de bonne volonté, mais la Commission peut les y obliger. Cette démarche les force à prendre du temps pour réfléchir à tout ça, et à réunir des documentations, des archives. Au-delà de ces recours légaux, on apporte aussi notre soutien à des collectifs militants dans le cadre de l'autodéfense numérique, qui constitue un public homogène avec un modèle de menace défini. Cette notion de modèle de menace est cruciale, puisque l'autodéfense numérique n'a pas les mêmes enjeux pour chacun·e, les risques encourus sont très différents, ça peut aller du vol des données bancaires, de surveillance, de risque de prison voire de mort.

Nous organisons aussi une permanence bibliothèque, des projections/débats et des ateliers plus théoriques autour des infrastructures du numérique, puisque cette compréhension technique permet de saisir les localisations du pouvoir numérique. Nous menons bénévolement ces actions et n'avons pas de financement. Nous fonctionnons avec une politique du prix libre pour les ateliers et les éditions, notamment pour financer l'achat de clés USB. Parfois, et lorsque des structures très en place demandent des ateliers, on leur demande une contribution, ce qui permet de financer des ateliers pour d'autres structures avec moins de moyens.

~ Des exemples de problèmes / questions récurrentes avec lesquelles les gens viennent aux permanences ?

Dans les ateliers, on a essentiellement des gens qui sont déjà sensibilisés à la question de la surveillance. On fait aussi beaucoup de maintenance, de résolution de

problèmes techniques, mais aussi des problèmes plus spécifiques. Par exemple, on a eu récemment le cas d'une personne issue d'une association qui a "perdu" son téléphone dans une manifestation. Le téléphone n'était pas chiffré, ce qui implique un accès potentiel aux données de l'association. D'un autre côté, on a aussi des personnes qui viennent pour des soucis de confidentialité, par exemple spécifiquement pour dégoogliser leurs téléphones. En fait le système d'exploitation Android est open source et principalement développé/exploité par Google. Quand on achète un téléphone neuf, on a par défaut la version Android de Google à laquelle sont ajoutées des surcouches d'interfaces et d'applications producteur (exemple : Samsung), des applications de Google et parfois d'autres intégrées par le revendeur (exemple : Orange).

Dans ce type de cas, on va essayer d'installer une version d'Android qui n'a pas ces liens avec Google, ce qui parfois est compliqué en fonction de la notoriété du téléphone. Plus un téléphone est connu ou vendu, plus il y a de chance d'arriver facilement à le dégoogliser (puisque plus de personnes ont pu travailler dessus et essayer). La plupart des personnes qui assistent aux ateliers viennent avant d'avoir des problèmes, avec peu de connaissances techniques numériques, mais une conscience du capitalisme de surveillance, de la surveillance policière, des GAFA etc. Encore une fois, ces différentes surveillances n'ont pas les mêmes enjeux et constituent différents modèles de menace.

~ Qu'est-ce qui fait obstacle au développement d'une conscience numérique ?

Ce qui bloque, c'est l'absence de mise en débat de cette surveillance, à laquelle j'ajoute un frein qui vient d'une appréhension de la technique. D'un autre côté, ce qui fait obstacle au développement d'une conscience numérique se situe dans l'argument "je n'ai rien à cacher". C'est cette indifférence individualiste qui constitue en fait un privilège, privilège qui peut facilement se perdre.

~ Est-ce que vous avez eu des réponses des institutions publiques au(x) projet(s) Technopolice ?

Non, à part quelques organes politiques qui essaient de se positionner pour faire bonne image, qui tentent une récupération politique. Du côté administratif, aussi, la plupart de nos demandes CADA sont restées sans réponse. En fait, il est difficile de voir des choses bouger au niveau public, les lignes politiques ne bougeront pas : le numérique est un outil pour conserver le pouvoir. C'est du côté des gens que tout se joue, il s'agit de leur faire prendre conscience des enjeux du numérique.

~ Avez-vous des références culturelles qui peuvent aider à saisir les enjeux de la gouvernance numérique ?

Spontanément, je pense à *Black Mirror*, qui a éveillé les consciences d'un large public sur pas mal de thématiques liées au numérique. En général, la science-fiction et les fictions d'anticipation qui se placent du côté de la dystopie touchent les consciences, mais construisent aussi largement les imaginaires des dominants. La BD *Verax* est super accessible pour comprendre la citation de la NSA/CIA *we kill people based on metadata*. Les romans *the circle* et *the every* de Dave Eggers sur la vie telle que conçue par Google & Amazon. Le catalogue de la bibliothèque Technopolice est dispo ici : <https://inventaire.io/users/technopolicebxl/inventory>

~ Quels outils n'arrivez-vous pas à remplacer ?

Il y a toujours une alternative, sauf peut-être pour des logiciels très précis, un logiciel d'architecture par exemple, ou bien les outils administratifs (lecteur de carte d'identité). À part ça, tout est plutôt une question d'habitude, pour les outils artistiques, c'est un formatage dès l'école aux logiciels propriétaires. Certaines écoles font l'effort d'utiliser et d'enseigner sur des logiciels libres (comme l'ERG par exemple). Je fais souvent l'analogie entre les plats préparés surgelés et les logiciels propriétaires : un plat tout préparé, c'est facile, mais on ne sait pas trop ce qu'il y a dedans. Opter pour le libre ça serait comme faire sa cuisine soi-même avec des ingrédients du jardin.

~ C'est quoi la première étape pour se dégafamiser ?

C'est d'abord savoir ce que sont les GAFA, se rendre compte de leur ampleur et du contrôle de ces grandes firmes, mais aussi de leur rôle premier. Par exemple, si l'on sait que Google est une régie publicitaire, c'est beaucoup plus simple de se rendre compte de ce qu'ils font. L'étape d'après serait donc de chercher des alternatives pour échapper à ce contrôle, et comment généraliser ces alternatives à divers domaines.

~ En conclusion..

Ces dominations numériques, cette surveillance permanente est un choix politique. Elle nous est imposée sans aucune concertation, ni débat, comme si tout cela était la marche forcée du monde. Si certaines technologies de contrôle sont largement installées (et qu'il sera difficile de faire machine arrière), d'autres sont encore naissantes (comme la reconnaissance faciale par exemple) et il est encore possible de s'y opposer. Il est nécessaire de comprendre les enjeux, de concentrer les forces, et surtout de s'organiser collectivement : construisons le monde dont nous avons envie !

Permanence d'autodéfense numérique

[Retranscription hautement subjective d'une permanence d'autodéfense numérique menée par Technopolice]

Le collectif belge Technopolice mène tous les premiers lundis du mois des ateliers d'autodéfense numérique dans les locaux d'une boulangerie. Nous (Vinciane, Théo, Laurent, Marion) y avons participé, et avons saisi des clés, des pistes pour parer aux attaques du capitalisme de surveillance sur le plan numérique. Cette retranscription est un survol des pratiques d'autodéfense numérique, qui sont disponibles en détail dans le *Guide d'Autodéfense Numérique* sur le site technopolice.be.

" De nos jours, les ordinateurs, Internet et le téléphone portable tendent à prendre de plus en plus de place dans nos vies. Le numérique semble souvent très pratique : c'est rapide, on peut parler avec plein de gens très loin, on peut avoir toute son histoire en photos, on peut écrire facilement des textes bien mis en page... mais ça n'a pas que des avantages ; ou en tout cas, ça n'en a pas seulement pour nous, mais aussi pour d'autres personnes qu'on n'a pas forcément envie d'aider. Il est en effet bien plus facile d'écouter discrètement des conversations par le biais des téléphones portables que dans une rue bruyante, ou de trouver les informations que l'on veut sur un disque dur plutôt que dans une étagère débordante de papiers. De plus, énormément de nos informations personnelles finissent par se retrouver publiées quelque part, que ce soit par nous-mêmes ou par d'autres personnes, que ce soit parce qu'on nous y incite — c'est un peu le fond de commerce du web 2.0 —, parce que les technologies laissent des traces, ou simplement parce qu'on ne fait pas attention. " *Guide d'Autodéfense numérique* (6e édition), Les revers de la mémoire numérique, <https://guide.boum.org/pourquoi-ce-guide.html>.

Dégoogliser son smartphone :

Dégoogliser un smartphone, libérer son téléphone des GAFAM est un processus qui comporte différentes échelles et différentes étapes. Il peut s'agir par exemple d'un changement d'applications de type email ou navigateur par leurs équivalents libres, mais aussi, et c'est la partie la plus délicate, un changement d'OS

(système d'exploitation du téléphone). Si cette étape est complexe, c'est qu'une erreur sur le modèle/sous-modèle du téléphone mènerait à l'installation d'un OS libre mais non adéquat, qui pourrait empêcher l'OS de fonctionner à nouveau.

Au vu du nombre de modèles de téléphones disponible aujourd'hui ; les développeurs sont plus éparpillés et il n'y a pas tant de smartphones compatibles avec des OS libres (ou pas suffisamment de documentation pour être sûr de ce que l'on fait). Il est alors recommandé de consulter la liste des téléphones compatibles avant d'en changer, disponible sur le site de Technopolice, où d'aller consulter les membres du collectif lors de leurs ateliers. Puisqu'on ne vous invite pas à changer de téléphone si le vôtre fonctionne encore, une des alternatives est aussi de désactiver certaines surcouches de surveillance en plus des applications ; pour cela, les membres du collectif utilisent un programme qui indique à quoi sert chaque paquet, et quel risque existe si on le désactive. Le principal risque étant que certaines applications cessent de fonctionner, mais il est toujours possible de réactiver ces paquets en cas de problème.

TAILS :

L'anonymat en ligne est une illusion. En réalité, on laisse constamment des traces sur les dispositifs numériques qu'on utilise. La seule manière de se battre contre les systèmes de surveillance est d'en augmenter le coût. Tails est un système d'exploitation alternatif. Il est principalement utilisé par des lanceurs d'alertes, des activistes, des journalistes, des militantes et autres personnes ayant un modèle de menace nécessitant une protection avancée de leurs données et de leur identité.

C'est l'acronyme de The Amnesic Incognito Live System (Le système incognito amnésique direct). À la différence de Windows ou MacOS, ce système est préconfiguré pour se réinitialiser complètement entre chaque utilisation et ne garde en mémoire aucune information. Il est possible d'installer Tails sur une clé USB et en branchant celle-ci à un ordinateur, l'OS de la machine est permuté vers ce système. On peut donc alterner entre un OS classique et Tails en fonction des besoins de protection. En cas de perte de l'ordinateur, de vol ou de contrôle par la police, une fois la clé USB contenant Tails éjectée, plus aucune trace des dernières actions et connexions n'est laissée.

Ce système, basé sur la version Debian de Linux, est programmé pour utiliser le réseau Tor, permettant de contourner la censure, de rajouter de la complexité de surveillance. Pour faire court, Tor permet d'anonymiser la source d'une session de navigation Web ou de messagerie instantanée. L'utilisation de Tails et de Tor

donne donc plusieurs couches de protection. Il est tout de même important de préciser que la connexion au réseau Tor est condamnable dans certains pays comme en Iran ou en Chine.

En résumé, il existe plein d'autres actions possibles pour échapper à la surveillance ; le paramétrage de son navigateur, choisir le bon système de mail, chiffrer ses appareils, etc. Tout ceci dépend aussi de l'utilisation que l'on fait de ces outils, et de notre modèle de menace ; mais avec des conseils avisés chacun choisit son pain, avec les ingrédients qui lui conviennent.

