

# Dans les eaux troubles du numérique

27 avril 2020

par Thomas Michel, membre de ZIN TV

Premier lieu commun : Internet est entré dans les mœurs. Consulter ses mails, partager des fichiers, obtenir une information en ligne font aujourd'hui - pour une écrasante majorité d'entre nous - partie des gestes du quotidien. Deuxième lieu commun : Internet ouvre un monde de possibilités. Échanger avec un ami vivant à l'autre bout du monde, s'informer en ligne, gérer son compte bancaire sans sortir de chez soi, faire ses courses sans sortir de chez soi, rencontrer l'âme sœur sans sortir de chez soi, télétravailler malgré le confinement... Génial, non ? Toutefois, depuis ses débuts, ce réseau de réseaux s'est développé en parallèle et avec des techniques de contrôle, de surveillance et de répression, dont les conséquences sont de plus en plus visibles aujourd'hui. Internet ou le plus formidable outil de contrôle que l'être humain n'ait jamais mis au point ?

Même s'il se veut libre, démocratique, transparent, depuis les années nonante, le World Wide Web s'est progressivement vu accaparé par les entreprises de services technologiques (très majoritairement nord-américaines). Répondre aux questions : « Qui détient les données des utilisateurs ? Comment sont-elles utilisées ? À quelles fins ? » suffit à comprendre la transformation qu'a subi le réseau mondial. Loin des ambitions « libres » des débuts (Free software), permettant le contrôle et le partage des programmes et des données par l'utilisateur, le culte du secret industriel et la propriété des brevets se sont peu à peu imposés, selon la logique libertarienne de la Silicon Valley, et ce, parallèlement à l'avènement des sociétés de contrôle. Que dire des formidables possibilités que propose la toile, alors qu'une écrasante majorité des communications d'aujourd'hui passent par Internet, lorsqu'un gouvernement choisit de déconnecter sa population du réseau mondial pour mieux contenir une révolte ? Pour pister des personnes infectées par un virus ? Pour surveiller des opposants politiques ? Pour filtrer des résultats de recherche et influencer l'opinion ?

Ainsi, l'utilisation d'Internet est tout sauf anodine. Elle nous expose à la surveillance, possiblement à la répression, sans parler de son aspect rentable. C'est connu : *si c'est gratuit, c'est que vous êtes le produit*. Autrement dit, la gratuité

n'est pas la liberté. D'autant que les métadonnées sont « l'or du 21ème siècle » : la monétisation des données personnelles a rendu en une petite dizaine d'années les GAFAM (Google, Amazon, Facebook, Apple, Microsoft) et autres BAXT (Baidu, Alibaba, Tencent et Xiaomi) plus hégémoniques, riches et influentes que les compagnies pétrolières les plus prospères. Sans oublier leurs petits, les NATU (Netflix, Airbnb, Tesla et Uber), qui vivent eux aussi des métadonnées que l'on sème... Qui dit gratuit, dit maximum de profit. Aujourd'hui, la concentration du capital passe essentiellement par le biais des nouvelles technologies. Et, cela va sans dire, les algorithmes de nos applications servent les intérêts de ceux qui les programment. Comme nous en a averti le philosophe Louis Althusser : à partir d'une technique, on détermine une idéologie...

## **Des données sur les données**

D'autant que les choses vont vite. Bien plus vite que nos habitudes. Selon certains médias spécialisés dans le numérique, Google aurait réussi à la rentrée 2019 le premier calcul quantique impossible à réaliser avec un ordinateur traditionnel. Vu comme un progrès majeur pour l'industrie et la recherche, ces ordinateurs (quantum computing) se révèlent être de formidables outils de surveillance de masse. En effet, ces machines d'un nouveau genre et d'une rapidité inégalable rendent immédiatement caduques les algorithmes de chiffrement, même les plus récents (ce que n'a pas tardé à confirmer la National Security Agency après l'annonce de Google). Aussi, permettront-elles à l'intelligence artificielle d'expertiser le réel pour en déterminer/définir les tendances majeures (les futures « vérités » ?), et rendront possible, notamment grâce à la cinquième génération des standards de télécommunication (la « 5G »), le stockage et l'analyse en temps réel d'extraordinaires quantités de métadonnées, voire le contrôle de larges territoires, de populations entières... ? Selon la constante de Gordon Earle Moore, cofondateur de l'entreprise nord-américaine Intel et premier fabricant mondial de microprocesseurs, la complexité et les possibilités de calculs de nos machines doublent chaque dix-huit mois... Autrement dit, les techniques de surveillance ont de beaux jours devant elles.

Heureusement, nombreux sont les gouvernements qui le rappellent durant cette période de confinement où l'utilisation des moyens de communication numérique explose, le traitement de nos métadonnées ne sera pratiqué que lorsque cela

sera « *nécessaire pour des motifs d'intérêt public* » notamment dans le domaine de la santé publique. Sauf peut-être en République de Chine, à Taïwan, où les autorités locales et les opérateurs de télécoms, pour contenir la propagation du virus, ont introduit un système de clôture électronique qui alerte la police lorsque les personnes mises en quarantaine sortent de chez elles, ce qui leur coûte de lourdes amendes. Sauf peut-être en Corée du Sud, où les autorités envoient des alertes par SMS aux gens qui ont pu être en contact avec une personne atteinte du coronavirus, en précisant l'âge et le sexe de l'individu concerné. Sauf peut-être en Israël, où le gouvernement de Benjamin Netanyahu (dont le procès pour corruption a été reporté en raison du Covid-19) vient d'autoriser les services secrets à collecter, sans autorisation préalable de la justice, les données de géolocalisation des personnes infectées et de celles les ayant croisées durant les deux semaines précédentes. Sauf peut-être en Pologne, où depuis la mi-mars les citoyens placés en quarantaine doivent télécharger une application pour smartphone, les obligeant à se géolocaliser à l'aide de selfies, afin de répondre aux demandes périodiques d'auto-identification du gouvernement. Sans parler du cas de la Hongrie, où le Premier Ministre Viktor Orbán s'arroge progressivement les pleins pouvoirs sous couvert de menace terroriste biologique. Sans parler de la Russie, où, à Moscou notamment, le maire de la ville prévoit la mise en place d'un système de contrôle dit « intelligent », qui autorisera ou non les citoyens à quitter leur domicile en fonction de leur état de santé. Sans parler du gouvernement nord-américain qui travaille – de concert avec Facebook et Google (dont les systèmes d'exploitation sont les plus utilisés à travers la planète) – à un suivi des données de géolocalisation des individus afin de cartographier les zones de concentration de cas de coronavirus...

« Mais » me direz-vous (parce qu'il y a toujours un mais) : ce sont là des pays forts lointains, qui, pour la plupart, sont connus de longue date pour leurs pratiques douteuses, voire anti-démocratiques. Pourtant, en Europe, l'Italie, le Royaume-Uni, l'Autriche, l'Allemagne travaillent avec leurs opérateurs de télécommunication nationaux à la création de cartes thermiques virtuelles retraçant les déplacements des populations, et ce, bien entendu, grâce à des métadonnées *anonymisées*. En France, grâce à la technologie Bluetooth, l'application « StopCovid », utilisable sur la base du *volontariat*, devrait permettre aux utilisateurs de savoir s'ils ont été en contact avec des personnes contaminées. Sans compter que le géant national Orange (leader ou second opérateur dans les pays européens dans

lesquels il est implanté) travaille à la mise au point d'une application de traçage numérique pour lutter contre le coronavirus. En Belgique enfin, les ministres des Télécommunications et de la Santé Publique ont annoncé à la mi-mars la création d'un groupe de travail « Data Against Corona » qui prévoit d'utiliser les données de géolocalisations de nos téléphones (prochainement requis à des fins de contrôle?) pour lutter contre la propagation du virus. Aussi, le port d'Anvers teste actuellement un bracelet *intelligent* émettant un signal lorsque son porteur ne respecte pas la distance sociale de sécurité...

### **Si c'est efficace, il faut s'en servir**

En Allemagne, la chancelière Angela Merkel, parlant de la surveillance numérique, a déclaré que « *si cela s'avère être un moyen efficace pour suivre la propagation du virus* », elle serait « *bien sûr prête à l'utiliser* ». En effet, un nombre croissant de pays est en mesure de reconstituer les déplacements de ses habitants – présentement, ceux des personnes contaminées par le Covid-19 – via l'analyse des métadonnées de leurs smartphones, de leurs transactions bancaires, des images de vidéo-surveillance... Si ce n'est pas déjà le cas, qu'advierait-il si les autorités, se familiarisant avec ce pouvoir démiurgique, commençaient à l'apprécier ? Le Covid-19 pourrait-il conduire à une surveillance étatique étendue et durable, qui demeurerait une fois la crise sanitaire passée ? Les périodes de « crise » ont toujours suscité des prises de conscience... et des « stratégies du choc », théorisées par Naomi Klein, essayiste canadienne, dans un livre du même nom (*La Stratégie du choc : la montée d'un capitalisme du désastre*). Ou comme le dit limpiment Edward Snowden, ancien employé de la CIA et sous-traitant de la NSA, ayant révélé les détails de plusieurs programmes de surveillance de masse nord-américains et britanniques : « *L'urgence a tendance à se pérenniser. [...] On a vu ce genre de choses se produire dans plusieurs pays. Ce n'est pas l'apanage d'un en particulier* ».

Notre civilisation est une civilisation de moyens. Progressivement, le progrès technique s'est affranchi de ses liens à l'éthique au profit du seul critère de la recherche de la plus grande efficacité. Le mantra selon lequel : « *Ce n'est pas l'outil qui est mauvais, c'est l'usage que l'on en fait* » peut faire sens lorsqu'on parle d'un couteau, mais est aujourd'hui rendu caduc par les nouvelles technologies et leur complexité grandissante. La technique, en tant que recherche du moyen le plus

efficace à court terme « s'indépendantise » des réflexions sur les comportements à adopter pour rendre le monde humainement habitable (je parle ici du fameux principe de précaution qui pose la question du prix de notre puissance). Autrement dit, si une technique est efficace, elle sera utilisée un jour ou l'autre (comme semble le dire plus haut Angela Merkel), quid des conséquences immorales/injustes qu'elle pourrait avoir sur le long terme.

Allons-nous vers des villes surveillées par des drones comme on peut le voir dans certaines capitales européennes ? Si oui, faudra-t-il éliminer les goélands qui s'attaquent à ces machines volantes cherchant à protéger leurs nids ? Si non, faudra-t-il pucer ces mêmes goélands afin de les « traquer » et de leur empêcher l'accès à certaines zones (réservées aux drones de la police) ? Concernant la situation immédiate, le développement de telles applications (du même genre que StopCovid) ayant un coût, ne vaudrait-il pas mieux investir dans des solutions plus efficaces, comme la production de masques et le dépistage de la population ? Et si ce type d'application venait à être adopté par une large partie de la population, cela inciterait-t-il nos gouvernements à l'imposer à l'ensemble des populations ? Et une fois l'application largement déployée, sera-t-il possible de lui ajouter des fonctions coercitives afin de trier les gens comme on trie les malades à sauver de ceux à sacrifier ? Enfin, dans le plus dystopique des futurs, nos métadonnées seront-elles utilisées pour sélectionner les fauteurs de trouble, les localiser, puis les mettre « hors d'état de nuire », par drone et par frappes dites « chirurgicales », comme le fait l'armée étasunienne dans certains pays du Moyen-Orient ?

## **Survivance générale**

Nombreuses sont les associations défendant les libertés fondamentales dans l'environnement numérique (bien que très axée sur la France, la Quadrature du Net en fait partie) à dénoncer les usages policiers des nouvelles technologies appliquées à la surveillance, notamment pendant cette période de coronavirus. Entre autres, la reconnaissance faciale ou le croisement des métadonnées sont en constante augmentation en Europe. La surveillance étatique, mise en place en notre nom ou au nom d'une « guerre » contre un virus se montre de plus en plus arbitraire et massive. Parce que la sécurité totale n'existe pas, seule la surveillance totale peut endiguer l'accident ; le syllogisme : « *la liberté, c'est la sécurité ; la sécurité, c'est la surveillance ; donc la liberté, c'est la surveillance* » ayant joué un

rôle important dans l'érosion progressive de nos droits... Bien avant le Covid-19, lors des manifestations des gilets jaunes en France, les policiers ont eu recours à plusieurs reprises à l'identification automatique des téléphones mobiles de certains groupes de manifestants.

En Belgique, la loi concernant la collecte et la conservation des données dans le secteur des communications électroniques passée en 2016 oblige les sociétés de télécommunication à fournir au gouvernement belge, à sa demande, des informations sur leurs clients et permet au pouvoir judiciaire et aux services de police belges d'accéder aux métadonnées pendant des enquêtes criminelles, et ce, sans autorisation judiciaire. Légitimement, ces mêmes associations luttant contre la surveillance en ligne y voient les prémices d'une légalisation du fichage généralisé. Ce que cette période de confinement fera passer pour normal ?

Lorsqu'à la vidéo-surveillance, à l'interception des communications électroniques, aux suivis des paiements/retraits bancaires, aux collectes des données de connexion d'un ordinateur, aux récupérations des métadonnées des téléphones mobiles s'ajoute l'utilisation de marqueurs chimiques – appelés « PMC » pour *produits chimiques marquants* (également utilisés lors des manifestations des gilets jaunes) –, quel espace reste-il pour les « libertés fondamentales » ? Quel espace pour la contestation (pendant et hors période de confinement) ? Plus sophistiquées que les flash-balls et les lances à eau des forces de l'ordre, ces technologies de surveillance de masse permettent d'identifier efficacement et rapidement des personnes contaminées (autant que des agitateurs ou agitateuses politiques), afin de leur interdire de se déplacer (de manifester, de s'opposer) ? Et puisque les arrestations préventives sont déjà pratiquées, ces outils serviront-ils à l'avenir, comme dans la nouvelle de science-fiction de Phillip K. Dick *The Minority Report* à condamner la « pré-action » ? Serait-ce le « pré-crime » (qui durant le Covid-19 revient à sortir de chez soi) qui sera maintenant traqué ? Si une bonne police est une police invisible, pour ainsi dire indolore (ce que permettent les nouvelles technologies), quel avenir pour les luttes sociales ?

### **Pour un Internet décentralisé et émancipateur**

Quoi qu'en disent nos représentants, toutes ces mesures ne se résument pas à la seule lutte contre le terrorisme ou contre la propagation d'un virus. Elles

peuvent s'appliquer à tout un chacun (suspecté ou non, infecté ou non ?) dès lors que la mise en place d'une surveillance personnalisée est supposée révéler des informations utiles à endiguer l'épidémie ou à la défense des intérêts nationaux. Ainsi, on ne s'étonnera guère, par ricochets, de voir des services de police détourner la législation pour surveiller un citoyen à la suite d'une infraction mineure : ne pas respecter la distance de sécurité (social distancing), l'achat à titre individuel de cannabis, ou après l'organisation d'une manifestation en soutien aux personnes sans papiers en période de confinement. Bien entendu, la répression des mouvements sociaux ne date pas d'aujourd'hui. En outre, depuis les attentats de mars 2016 à Bruxelles, l'arsenal législatif et policier servant à étouffer les luttes sociales n'a cessé de se renforcer. S'ajoute à cela la censure des contenus dits « subversifs » en ligne, notamment sur Youtube ou les réseaux sociaux. Que nous réserve l'après-confinement ?

La surveillance en ligne est une violation des libertés fondamentales, Covid-19 ou pas Covid-19. Comme l'a souvent répété Edward Snowden, dire que l'on se moque du droit à la vie privée parce que l'on a « rien à cacher » revient à se foutre de la liberté de la presse parce que l'on a rien à écrire. Le danger vient autant de ce que l'on ignore que de ce que l'on tient pour certain et qui ne l'est pas. Avant les révélations de l'ancien sous-traitant de la NSA, les représentants de l'agence avaient toujours déclaré ne collecter qu'accidentellement des informations sur les citoyens étasuniens. Enfin, comme l'écrivait Aaron Swartz, hacktiviste nord-américain, dans son *Guerilla Open Access Manifesto* : « *L'information, c'est le pouvoir. Mais comme pour tout pouvoir, il y a ceux qui veulent le garder pour eux* ». Nous devons lutter contre la surveillance de masse autant que possible, en favorisant le libre accès à l'information, en se prémunissant contre le fichage généralisé et en favorisant les outils numériques libres – libres pour combien de temps encore ? –.

En somme, peut-être devrions-nous nous rappeler de ces policiers en civil, aux visages couverts, qui durant une manifestation ou une interpellation retirent leurs brassards et leurs numéros de matricule pour ne pas être identifiables... Peut-être devrions-nous nous méfier de nos objets connectés autant que l'on se méfie du coronavirus, qui même s'ils nous rapprochent et nous permettent de nous organiser, de partager des idées (surtout durant le confinement), nous pistent et nous enferment dans un profile type. Ou tout au moins, devrions-nous

apprendre à mieux/moins les utiliser afin de pouvoir décider de ce qu'ils disent de nous. Bien que la meilleure option pour contrer la surveillance globale soit de ne pas communiquer numériquement – nous faudra-t-il en revenir au pigeon voyageur ? – les outils numériques d'anonymisation, libres et open-source, sont un premier pas vers la maîtrise de nos objets connectés ; surtout en période de pandémie.

### **Matière à penser (en guise de conclusion)**

Cela va sans dire, à l'aune du progrès technologique, la condition humaine a radicalement changé. Il se pourrait que ce « progrès » – dont la progression n'est pas vue comme bénéfique par l'ensemble des habitants du globe : les nuisances liées aux nouvelles technologies étant délocalisées – il semblerait donc que ce « progrès » soit un des événements les plus bouleversants de notre époque pour ce qui est de la nature ou de la liberté humaine. Dès lors, le numérique et la société s'influencent mutuellement. Les nouvelles technologies et les algorithmes qui les font fonctionner ne sont plus de simples intermédiaires, comme pouvait l'être une lettre postale, un fax (ou même un pigeon voyageur), elles deviennent progressivement notre environnement, une manière de percevoir le monde qui nous entoure. De plus, si l'automatisation – qui remplace l'intervention humaine par une machine et/ou un logiciel informatique – réduit la pénibilité du travail, souvent, elle le supprime en même temps (ce qui engendre du chômage). En d'autres termes, le progrès technique n'est pas toujours synonyme de progrès social. Petit à petit, l'être humain s'adapte aux applications qui le guident et l'informent en temps réel et se met à penser par elles – pour ne plus pouvoir penser sans elles ?

Au vu des nouvelles technologies utilisées par nos gouvernements pour faire la guerre (contre des concepts ou des virus), pour mater un mouvement social d'ampleur ou pour donner la mort, ces technologies, autant qu'elles libèrent, pourraient-elles devenir, dans un avenir proche, une des principales menaces qui pèsent sur nos libertés ? Plus encore si l'on se base sur les rapports des (très nombreux) scientifiques du *rapport Meadow*, du GIEC, de l'ONU... qui prévoient un dérèglement climatique violent dans les années à venir, menant à un possible « effondrement » et donc à de nouveaux confinements ou au contraire à des soulèvements massifs et sans précédent ?

L'être humain (celui des pays riches en tête) serait-il devenu l'instrument de ses



instruments ? Croyant se servir de la technique, ce pourrait être finalement lui qui la sert ? Une chose semble se profiler : ce que Jacques Ellul appelle le « phénomène technique » ou *la préoccupation de notre temps de rechercher en toutes choses la méthode la plus efficace s'affranchira volontiers de toute éthique, de tous principes moraux* – le pistage en temps réel et la guerre par les drones en sont des exemples frappants –, au profit de la plus froide, de la plus implacable des efficacités. Ne voit-on pas cette recherche de méthodes rationnelles, efficaces, s'étendre progressivement à l'ensemble des activités humaines ? La question n'est plus qui maîtrise quoi, mais quoi maîtrise qui ?

Thomas Michel, membre du collectif ZIN TV

#### Liens sur Internet de l'article :

<https://zintv.org/dans-les-eaux-troubles-du-numerique/>

#### Sources :

-<https://www.lecho.be/dossiers/coronavirus/en-chine-une-grande-muraille-electronique-pour-controler-les-citoyens/10220089.html>  
-<https://www.lecho.be/dossiers/coronavirus/en-chine-une-grande-muraille-electronique-pour-controler-les-citoyens/10220089.html>  
-[https://www.rtf.be/info/monde/detail\\_israel-l-ouverture-du-proces-de-netanyahu-reportee-pour-cause-de-coronavirus?id=10458075](https://www.rtf.be/info/monde/detail_israel-l-ouverture-du-proces-de-netanyahu-reportee-pour-cause-de-coronavirus?id=10458075)  
-<https://www.lefigaro.fr/secteur/high-tech/les-polonais-en-quarantaine-doivent-se-prendre-en-selfie-pour-prouver-qu-ils-sont-chez-eux-20200324>  
-[https://www.rtf.be/info/monde/detail\\_coronavirus-en-hongrie-viktor-orban-en-route-vers-des-pouvoirs-quasi-illimites?id=10470242](https://www.rtf.be/info/monde/detail_coronavirus-en-hongrie-viktor-orban-en-route-vers-des-pouvoirs-quasi-illimites?id=10470242)  
-<https://siecdigital.fr/2020/04/04/moscou-lance-une-application-de-surveillance-pour-suivre-ses-citoyens-lors-du-confinement/>  
-[https://www.rtf.be/info/medias/detail\\_etats-unis-une-carte-du-virus-basee-sur-des-donnees-fournies-par-facebook-et-google?id=10485812](https://www.rtf.be/info/medias/detail_etats-unis-une-carte-du-virus-basee-sur-des-donnees-fournies-par-facebook-et-google?id=10485812)  
-<https://www.france24.com/fr/20200424-stopcovid-une-application-de-tra%C3%A7age-du-covid-19-qui-fait-d%C3%A9bat>  
-[https://www.rtf.be/info/societe/detail\\_des-donnees-contre-le-corona-votre-telephone-peut-lutter-contre-le-virus?id=10463580](https://www.rtf.be/info/societe/detail_des-donnees-contre-le-corona-votre-telephone-peut-lutter-contre-le-virus?id=10463580)  
-<https://www.lesoir.be/296147/article/2020-04-22/un-bracelet-intelligent-aidant-respecter-la-distance-sociale-teste-au-port>  
-<https://www.lenouvelliste.ca/actualites/monde/lallemagne-mise-sur-les-portables-et-le-bluetooth-contre-lepidemie-781bb94c289d731e46f2926bca39552b>  
-[https://www.lemonde.fr/la-foire-du-drone/article/2019/06/26/les-goelands-defient-les-drones-de-la-police-parisienne\\_5481791\\_5037916.html](https://www.lemonde.fr/la-foire-du-drone/article/2019/06/26/les-goelands-defient-les-drones-de-la-police-parisienne_5481791_5037916.html)  
-<https://abcnews.go.com/blogs/headlines/2014/05/ex-nsa-chief-we-kill-people-based-on-metadata>  
-[https://www.ejustice.just.fgov.be/cgi\\_loi/change\\_lg.pl?language=fr&la=F&table\\_name=loi&cn=2016052903](https://www.ejustice.just.fgov.be/cgi_loi/change_lg.pl?language=fr&la=F&table_name=loi&cn=2016052903)  
-<https://www.nouvelobs.com/societe/20190319.OBS2026/gilets-jaunes-on-en-sait-un-peu-plus-sur-les-marqueurs-chimiques-anticasseurs.html>  
-<https://plus.lesoir.be/213809/article/2019-03-22/comment-les-attentats-du-22-mars-ont-change-la-justice>  
-<https://zintv.org/outil/guerilla-open-access-manifesto/>