Les nouveaux Léviathans IV. La surveillance qui vient

Dans ce quatrième numéro de la série Nouveaux Léviathans, nous allons voir dans quelle mesure le modèle économique a développé son besoin vital de la captation des données relatives à la vie privée. De fait, nous vivons dans le même scénario dystopique depuis une cinquantaine d'années. Nous verrons comment les critiques de l'économie de la surveillance sont redondantes depuis tout ce temps et que, au-delà des craintes, le temps est à l'action d'urgence.

Note : voici le quatrième volet de la série des Nouveaux (et anciens) Léviathans, initiée en 2016, par **Christophe Masutti**, alias Framatophe. Pour retrouver les articles précédents, une liste vous est présentée à la fin de celui-ci.

Aujourd'hui

Avons-nous vraiment besoin des utopies et des dystopies pour anticiper les rêves et les cauchemars des technologies appliquées aux comportements humains ? Sempiternellement rabâchés, le *Meilleur de mondes* et *1984* sont sans doute les romans les plus vendus parmi les best-sellers des dernières années. Il existe un effet pervers des utopies et des dystopies, lorsqu'on les emploie pour justifier des arguments sur ce que devrait être ou non la société : tout argument qui les emploie afin de prescrire ce qui devrait être se trouve à un moment ou à un autre face au mur du réel sans possibilité de justifier un mécanisme crédible qui causerait le basculement social vers la fiction libératrice ou la fiction contraignante. C'est la raison pour laquelle l'île de Thomas More se trouve partout et nulle part, elle est utopique, en aucun lieu. Utopie et dystopie sont des propositions d'expérience et n'ont en soi aucune vocation à prouver ou prédire quoi que ce soit bien qu'elles partent presque toujours de l'expérience commune et dont tout l'intérêt, en particulier en littérature, figure dans le troublant cheminement des faits, plus ou moins perceptible, du réel vers l'imaginaire.

Pourtant, lorsqu'on se penche sur le phénomène de l'exploitation des données personnelles à grande échelle par des firmes à la puissance financière inégalable, c'est la dystopie qui vient à l'esprit. Bien souvent, au gré des articles journalistiques pointant du doigt les dernières frasques des GAFAM dans le

domaine de la protection des données personnelles, les discussions vont bon train : « ils savent tout de nous », « nous ne sommes plus libres », « c'est Georges Orwell », « on nous prépare le meilleur des mondes ». En somme, c'est l'angoisse pendant quelques minutes, juste le temps de vérifier une nouvelle fois si l'application Google de notre smartphone a bien enregistré l'adresse du rendez-vous noté la veille dans l'agenda.

Un petit coup d'angoisse ? allez… que diriez-vous si vos activités sur les réseaux sociaux, les sites d'information et les sites commerciaux étaient surveillées et quantifiées de telle manière qu'un système de notation et de récompense pouvait vous permettre d'accéder à certains droits, à des prêts bancaires, à des autorisations officielles, au logement, à des libertés de circulation, etc. Pas besoin de science-fiction. Ainsi que le rapportait *Wired* en octobre 2017[1], la Chine a déjà tout prévu d'ici 2020, c'est-à-dire demain. Il s'agit, dans le contexte d'un Internet déjà ultra-surveillé et non-neutre, d'établir un système de crédit social en utilisant les *big data* sur des millions de citoyens et effectuer un traitement qui permettra de catégoriser les individus, quels que soient les risques : risques d'erreurs, risques de piratage, crédibilité des indicateurs, atteinte à la liberté d'expression, etc.

Évidemment les géants chinois du numérique comme Alibaba et sa filiale de crédit sont déjà sur le coup. Mais il y a deux choses troublantes dans cette histoire. La première c'est que le crédit social existe déjà et partout : depuis des années on évalue en ligne les restaurants et les hôtels sans se priver de critiquer les tenanciers et il existe toute une économie de la notation dans l'hôtellerie et la restauration, des applications terrifiantes comme Peeple[2] existent depuis 2015, les banques tiennent depuis longtemps des listes de créanciers, les fournisseurs d'énergie tiennent à jour les historiques des mauvais payeurs, etc. Ce que va faire la Chine, c'est le rêve des firmes, c'est la possibilité à une gigantesque échelle et dans un cadre maîtrisé (un Internet non-neutre) de centraliser des millions de gigabits de données personnelles et la possibilité de recouper ces informations auparavant éparses pour en tirer des profils sur lesquels baser des décisions.

Le second élément troublant, c'est que le gouvernement chinois n'aurait jamais eu cette idée si la technologie n'était pas déjà à l'œuvre et éprouvée par des grandes firmes. Le fait est que pour traiter autant d'informations par des

algorithmes complexes, il faut : de grandes banques de données, beaucoup d'argent pour investir dans des serveurs et dans des compétences, et espérer un retour sur investissement de telle sorte que plus vos secteurs d'activités sont variés plus vous pouvez inférer des profils et plus votre marketing est efficace. Il est important aujourd'hui pour des monopoles mondialisés de savoir combien vous avez de chance d'acheter à trois jours d'intervalle une tondeuse à gazon et un canard en mousse. Le profilage de la clientèle (et des utilisateurs en général) est devenu l'élément central du marché à tel point que notre économie est devenue une économie de la surveillance, repoussant toujours plus loin les limites de l'analyse de nos vies privées.

La dystopie est en marche, et si nous pensons bien souvent au cauchemar orwellien lorsque nous apprenons l'existence de projets comme celui du gouvernement chinois, c'est parce que nous n'avons pas tous les éléments en main pour en comprendre le cheminement. Nous anticipons la dystopie mais trop souvent, nous n'avons pas les moyens de déconstruire ses mécanismes. Pourtant, il devient de plus en plus facile de montrer ces mécanismes sans faire appel à l'imaginaire : toutes les conditions sont remplies pour n'avoir besoin de tracer que quelques scénarios alternatifs et peu différents les uns des autres. Le traitement et l'analyse de nos vies privées provient d'un besoin, celui de maximiser les profits dans une économie qui favorise l'émergence des monopoles et la centralisation de l'information. Cela se retrouve à tous les niveaux de l'économie, à commencer par l'activité principale des géants du Net : le démarchage publicitaire. Comprendre ces modèles économiques revient aussi à comprendre les enjeux de l'économie de la surveillance.

Données personnelles : le commerce en a besoin

Dans le petit monde des études en commerce et marketing, Frederick Reichheld fait figure de référence. Son nom et ses publications dont au moins deux *best sellers*, ne sont pas vraiment connus du grand public, en revanche la plupart des stratégies marketing des vingt dernières années sont fondées, inspirées et même modélisées à partir de son approche théorique de la relation entre la firme et le client. Sa principale clé de lecture est une notion, celle de la *fidélité* du client. D'un point de vue opérationnel cette notion est déclinée en un concept, celui de la valeur vie client (*customer lifetime value*) qui se mesure à l'aune de profits réalisés durant le temps de cette relation entre le client et la firme. Pour Reichheld, la principale activité du marketing consiste à optimiser cette valeur vie client. Cette optimisation s'oppose à une conception rétrograde (et qui n'a jamais vraiment existé, en fait[3]) de la « simple » relation marchande.

En effet, pour bien mener les affaires, la relation avec le client ne doit pas seulement être une série de transactions marchandes, avec plus ou moins de satisfaction à la clé. Cette manière de concevoir les modèles économiques, qui repose uniquement sur l'idée qu'un client satisfait est un client fidèle, a son propre biais : on se contente de donner de la satisfaction. Dès lors, on se place

d’un point de vue concurrentiel sur une conception du capitalisme marchand déjà ancienne. Le modèle de la concurrence « non faussée » est une conception nostalgique (fantasmée) d’une relation entre firme et client qui repose sur la rationalité de ce dernier et la capacité des firmes à produire des biens en réponse à des besoins plus ou moins satisfaits. Dès lors la décision du client, son libre arbitre, serait la variable juste d’une économie auto-régulée (la main invisible) et la croissance économique reposerait sur une dynamique de concurrence et d’innovation, en somme, la promesse du « progrès ».

Évidemment, cela ne fonctionne pas ainsi. Il est bien plus rentable pour une entreprise de fidéliser ses clients que d’en chercher de nouveaux. Prospecter coûte cher alors qu’il est possible de jouer sur des variables à partir de l’existant, tout particulièrement lorsqu’on exerce un monopole (et on comprend ainsi pourquoi les monopoles s’accommodent très bien entre eux en se partageant des secteurs) :

1. on peut résumer la conception de Reichheld à partir de son premier *best seller*, *The Loyalty Effect* (1996) : avoir des clients fidèles, des employés fidèles et des propriétaires loyaux. Il n’y a pas de *main invisible* : tout repose sur *a)* le rapport entre hausse de la rétention des clients / hausse des dépenses, *b)* l’insensibilité aux prix rendue possible par la fidélisation (un client fidèle, ayant dépassé le stade du risque de défection, est capable de dépenser davantage pour des raisons qui n’ont rien à voir avec la valeur marchande), *c)* la diminution des coûts de maintenance (fidélisation des employés et adhésion au *story telling*), *d)* la hausse des rendements et des bénéfices. En la matière la firme Apple rassemble tous ces éléments à la limite de la caricature.
2. Reichheld est aussi le créateur d’un instrument d’évaluation de la fidélisation : le NPS (*Net Promoter Score*). Il consiste essentiellement à catégoriser les clients, entre promoteurs, détracteurs ou passifs. Son autre best-seller *The Ultimate Question 2.0: How Net Promoter Companies Thrive in a Customer-Driven World* déploie les applications possibles du contrôle de la qualité des relations client qui devient dès lors la principale stratégie de la firme d’où découlent toutes les autres stratégies (en particulier les choix d’innovation). Ainsi il cite dans son ouvrage les plus gros scores NPS détenus par des firmes comme Apple, Amazon et Costco.

Il ne faut pas sous-estimer la valeur opérationnelle du NPS. Notamment parce qu'il permet de justifier les choix stratégiques. Dans *The Ultimate Question 2.0* Reichheld fait référence à une étude de Bain & Co. qui montre que pour une banque, la valeur vie client d'un promoteur (au sens NPS) est estimée en moyenne à 9 500 dollars. Ce modèle aujourd'hui est une illustration de l'importance de la surveillance et du rôle prépondérant de l'analyse de données. En effet, plus la catégorisation des clients est fine, plus il est possible de déterminer les leviers de fidélisation. Cela passe évidemment par un système de surveillance à de multiples niveaux, à la fois internes et externes :

- surveiller des opérations de l'organisation pour les rendre plus agiles et surveiller des employés pour augmenter la qualité des relations client,
- rassembler le plus de données possibles sur les comportements des clients et les possibilités de déterminer leurs choix à l'avance.

Savoir si cette approche du marketing est née d'un nouveau contexte économique ou si au contraire ce sont les approches de la valeur vie client qui ont configuré l'économie d'aujourd'hui, c'est se heurter à l'éternel problème de l'œuf et de la poule. Toujours est-il que les stratégies de croissance et de rentabilité de l'économie reposent sur l'acquisition et l'exploitation des données personnelles de manière à manipuler les processus de décision des individus (ou plutôt des groupes d'individus) de manière à orienter les comportements et fixer des prix non en rapport avec la valeur des biens mais en rapport avec ce que les consommateurs (ou même les acheteurs en général car tout ne se réduit pas à la question des seuls biens de consommation et des services) sont à même de pouvoir supporter selon la catégorie à laquelle ils appartiennent.

Le fait de catégoriser ainsi les comportements et les influencer, comme nous l'avons vu dans les épisodes précédents de la série Léviathans, est une marque stratégique de ce que Shoshana Zuboff a appelé le *capitalisme de surveillance*[4]. Les entreprises ont aujourd'hui un besoin vital de rassembler les données personnelles dans des silos de données toujours plus immenses et d'exploiter ces *big data* de manière à optimiser leurs modèles économiques. Ainsi, du point de vue des individus, c'est le quotidien qui est scruté et analysé de telle manière que, il y a à peine une dizaine d'années, nous étions à mille lieues de penser l'extrême granularité des données qui cartographient et catégorisent nos comportements. Tel est l'objet du récent rapport publié par Cracked Lab Corporate surveillance in

everyday life[5] qui montre à quel point tous les aspect du quotidien font l'objet d'une surveillance à une échelle quasi-industrielle (on peut citer les activités de l'entreprise Acxiom), faisant des données personnelles un marché dont la matière première est traitée sans aucun consentement des individus. En effet, tout le savoir-faire repose essentiellement sur le recoupement statistique et la possibilité de catégoriser des milliards d'utilisateurs de manière à produire des représentations sociales dont les caractéristiques ne reflètent pas la réalité mais les comportements futurs. Ainsi par exemple les secteurs bancaires et des assurances sont particulièrement friands des possibilités offertes par le pistage numérique et l'analyse de solvabilité.

Cette surveillance a été caractérisée déjà en 1988 par le chercheur en systèmes d'information Roger Clarke[6] :

- dans la mesure où il s'agit d'automatiser, par des algorithmes, le traitement des informations personnelles dans un réseau regroupant plusieurs sources, et d'en inférer du sens, on peut la qualifier de « dataveillance », c'est à dire « l'utilisation systématique de systèmes de traitement de données à caractère personnel dans l'enquête ou le suivi des actions ou des communications d'une ou de plusieurs personnes » ;
- l'un des attributs fondamentaux de cette *dataveillance* est que les intentions et les mécanismes sont cachés aux sujets qui font l'objet de la surveillance.

En effet, l'accès des sujets à leurs données personnelles et leurs traitements doit rester quasiment impossible car après un temps très court de captation et de rétention, l'effet de recoupement fait croître de manière exponentielle la somme d'information sur les sujets et les résultats, qu'ils soient erronés ou non, sont imbriqués dans le profilage et la catégorisation de groupes d'individus. Plus le monopole a des secteurs d'activité différents, plus les comportements des mêmes sujets vont pouvoir être quantifiés et analysés à des fins prédictives. C'est pourquoi la dépendance des firmes à ces informations est capitale ; pour citer Clarke en 2017[7] :

> *« L'économie de la surveillance numérique est cette combinaison d'institutions, de relations institutionnelles et de processus qui permet aux entreprises d'exploiter les données issues de la surveillance du comportement électronique*

des personnes et dont les sociétés de marketing deviennent rapidement dépendantes. »

Le principal biais que produit cette économie de la surveillance (pour S. Zuboff, c'est de capitalisme de surveillance qu'il s'agit puisqu'elle intègre une relation d'interdépendance entre centralisation des données et centralisation des capitaux) est qu'elle n'a plus rien d'une démarche descriptive mais devient prédictive par effet de prescription.

Elle n'est plus descriptive (mais l'a-t-elle jamais été ?) parce qu'elle ne cherche pas à comprendre les comportements économiques en fonction d'un contexte, mais elle cherche à anticiper les comportements en maximisant les indices comportementaux. On ne part plus d'un environnement économique pour comprendre comment le consommateur évolue dedans, on part de l'individu pour l'assigner à un environnement économique sur mesure dans l'intérêt de la firme.

Ainsi, comme l'a montré une étude de Propublica en 2016[8], Facebook dispose d'un panel de pas moins de 52 000 indicateurs de profilage individuels pour en établir une classification générale. Cette quantification ne permet plus seulement, comme dans une approche statistique classique, de déterminer par exemple si telle catégorie d'individus est susceptible d'acheter une voiture. Elle permet de déterminer, de la manière la plus intime possible, quelle valeur économique une firme peut accorder à un panel d'individus au détriment des autres, leur valeur vie client.

Tout l'enjeu consiste à savoir comment influencer ces facteurs et c'est en cela que l'exploitation des données passe d'une dimension prédictive à une dimension prescriptive. Pour prendre encore l'exemple de Facebook, cette firme a breveté un système capable de déterminer la solvabilité bancaire des individus en fonction de la solvabilité moyenne de leur réseau de contacts[9]. L'important ici, n'est pas vraiment d'aider les banques à diminuer les risques d'insolvabilité de leurs clients, car elles savent très bien le faire toutes seules et avec les mêmes procédés d'analyse en *big data*. En fait, il s'agit d'influencer les stratégies personnelles des individus par le seul effet panoptique[10] : si les individus savent qu'ils sont surveillés, toute la stratégie individuelle consistera à choisir ses amis Facebook en fonction de leur capacité à maximiser les chances d'accéder à un prêt bancaire (et cela peut fonctionner pour bien d'autres objectifs). L'intérêt de

Facebook n’est pas d’aider les banques, ni de vendre une expertise en statistique (ce n’est pas le métier de Facebook) mais de normaliser les comportements dans l’intérêt économique et augmenter la valeur vie client potentielle de ses utilisateurs : si vous avez des problèmes d’argent, Facebook n’est pas fait pour vous. Dès lors il suffit ensuite de revendre des profils sur-mesure à des banques. On se retrouve typiquement dans un épisode d’anticipation de la série Black Mirror (Chute libre)[11].

La fiction, l’anticipation, la dystopie… finalement, c’est-ce pas un biais que de toujours analyser sous cet angle l’économie de la surveillance et le rôle des algorithmes dans notre quotidien ? Tout se passe en quelque sorte comme si nous découvrions un nouveau modèle économique, celui dont nous venons de montrer que les préceptes sont déjà anciens, et comme si nous appréhendions seulement aujourd’hui les enjeux de la captation et l’exploitation des données personnelles. Au risque de décevoir tous ceux qui pensent que questionner la confiance envers les GAFAM est une activité d’avant-garde, la démarche a été initiée dès les prémices de la révolution informatique.

La vie privée à l'époque des pattes d'eph.

Face au constat selon lequel nous vivons dans un environnement où la surveillance fait loi, de nombreux ouvrages, articles de presse et autres témoignages ont sonné l'alarme. En décembre 2017, ce fut le soi-disant repentir de Chamath Palihapitya, ancien vice-président de Facebook, qui affirmait avoir contribué à créer « des outils qui déchirent le tissu social »[12]. Il ressort de cette lecture qu'après plusieurs décennies de centralisation et d'exploitation des données personnelles par des acteurs économiques ou institutionnels, nous n'avons pas fini d'être surpris par les transformations sociales qu'impliquent les *big data*. Là où, effectivement, nous pouvons accorder un tant soit peu de de crédit à C. Palihapitya, c'est dans le fait que l'extraction et l'exploitation des données personnelles implique une économie de la surveillance qui modèle la société sur son modèle économique. Et dans ce modèle, l'exercice de certains droits (comme le droit à la vie privée) passe d'un état absolu (un droit de l'homme) à un état relatif (au contexte économique).

Comme cela devient une habitude dans cette série des Léviathans, nous pouvons effectuer un rapide retour dans le temps et dans l'espace. Situons-nous à la veille des années 1970, aux États-Unis, plus exactement dans la période charnière qui vit la production en masse des ordinateurs *mainframe* (du type IBM 360), à destination non plus des grands laboratoires de recherche et de l'aéronautique, mais vers les entreprises des secteurs de la banque, des assurances et aussi vers les institutions gouvernementales. L'objectif premier de tels investissements (encore bien coûteux à cette époque) était le traitement des données personnelles des citoyens ou des clients.

Comme bien des fois en histoire, il existe des périodes assez courtes où l'on peut comprendre les événements non pas parce qu'ils se produisent suivant un enchaînement logique et linéaire, mais parce qu'ils surviennent de manière quasi-simultanée comme des fruits de l'esprit du temps. Ainsi nous avons d'un côté l'émergence d'une industrie de la donnée personnelle, et, de l'autre l'apparition de nombreuses publications portant sur les enjeux de la vie privée. D'aucuns

pourraient penser que, après la publication en 1949 du grand roman de G. Orwell, *1984*, la dystopie orwellienne pouvait devenir la clé de lecture privilégiée de l'*informationnalisation* (pour reprendre le terme de S. Zuboff) de la société américaine dans les années 1960-1970. Ce fut effectivement le cas… plus exactement, si les références à Orwell sont assez courantes dans la littérature de l'époque[13], il y avait deux lectures possibles de la vie privée dans une société aussi bouleversée que celle de l'Amérique des années 1960. La première questionnait la hiérarchie entre vie privée et vie publique. La seconde focalisait sur le traitement des données informatiques. Pour mieux comprendre l'état d'esprit de cette période, il faut parcourir quelques références.

Vie privée vs vie publique

Deux best-sellers parus en été 1964 effectuent un travail introspectif sur la société américaine et son rapport à la vie privée. Le premier, écrit par Myron Brenton, s'intitule *The privacy invaders*[14]. Brenton est un ancien détective privé qui dresse un inventaire des techniques de surveillance à l'encontre des citoyens et du droit. Le second livre, écrit par Vance Packard, connut un succès international. Il s'intitule *The naked Society*[15], traduit en français un an plus tard sous le titre *Une société sans défense*. V. Packard est alors universitaire, chercheur en sociologie et économie. Il est connu pour avoir surtout travaillé sur la société de consommation et le marketing et dénoncé, dans un autre ouvrage (*La persuasion clandestine*[16]), les abus des publicitaires en matière de manipulation mentale. Dans *The naked Society* comme dans *The privacy invaders* les mêmes thèmes sont déployés à propos des dispositifs de surveillance, entre les techniques d'enquêtes des banques sur leurs clients débiteurs, les écoutes téléphoniques, la surveillance audio et vidéo des employés sur les chaînes de montage, en somme toutes les stratégies privées ou publiques d'espionnage des individus et d'abus en tout genre qui sont autant d'atteintes à la vie privée. Il faut dire que la société américaine des années 1960 a vu aussi bien arriver sur le marché des biens de consommation le téléphone et la voiture à crédit mais aussi l'électronique et la miniaturisation croissante des dispositifs utiles dans ce genre d'activité. Or, les questions que soulignent Brenton et Packard, à travers de nombreux exemples, ne sont pas tant celles, plus ou moins spectaculaires, de la mise en œuvre, mais celles liées au droit des individus face à des puissances en recherche de données sur la vie privée extorquées aux sujets mêmes. En somme,

ce que découvrent les lecteurs de ces ouvrages, c'est que la vie privée est une notion malléable, dans la réalité comme en droit, et qu'une bonne part de cette malléabilité est relative aux technologies et au médias. Packard ira légèrement plus loin sur l'aspect tragique de la société américaine en focalisant plus explicitement sur le respect de la vie privée dans le contexte des médias et de la presse à sensation et dans les contradictions apparente entre le droit à l'information, le droit à la vie privée et le Sixième Amendement. De là, il tire une sonnette d'alarme en se référant à Georges Orwell, et dénonçant l'effet panoptique obtenu par l'accessibilité des instruments de surveillance, la généralisation de leur emploi dans le quotidien, y compris pour les besoins du marketing, et leur impact culturel.

En réalité, si ces ouvrages connurent un grand succès, c'est parce que leur approche de la vie privée reposait sur un questionnement des pratiques à partir de la morale et du droit, c'est-à-dire sur ce que, dans une société, on est prêt à admettre ou non au sujet de l'intimité vue comme une part structurelle des relations sociales. Qu'est-ce qui relève de ma vie privée et qu'est-ce qui relève de la vie publique ? Que puis-je exposer sans crainte selon mes convictions, ma position sociale, la classe à laquelle j'appartiens, etc. Quelle est la légitimité de la surveillance des employés dans une usine, d'un couple dans une chambre d'hôtel, d'une star du show-biz dans sa villa ?

Il reste que cette approche manqua la grande révolution informatique naissante et son rapport à la vie privée non plus conçue comme l'image et l'estime de soi, mais comme un ensemble d'informations quantifiables à grande échelle et dont l'analyse peut devenir le mobile de décisions qui impactent la société en entier[17]. La révolution informatique relègue finalement la légitimité de la surveillance au second plan car la surveillance est alors conçue de manière non plus intentionnelle mais comme une série de faits : les données fournies par les sujets, auparavant dans un contexte fermé comme celui de la banque locale, finirent par se retrouver centralisées et croisées au gré des consortiums utilisant l'informatique pour traiter les données des clients. Le même schéma se retrouva pour ce qui concerne les institutions publiques dans le contexte fédéral américain.

Vie privée vs ordinateurs

Une autre approche commença alors à faire son apparition dans la sphère universitaire. Elle intervient dans la seconde moitié des années 1960. Il s'agissait de se pencher sur la gouvernance des rapports entre la vie privée et l'administration des données personnelles. Suivant au plus près les nouvelles pratiques des grands acteurs économiques et gouvernementaux, les universitaires étudièrent les enjeux de la numérisation des données personnelles avec en arrière-plan les préoccupations juridiques, comme celle de V. Packard, qui faisaient l'objet des réflexions de la décennie qui se terminait. Si, avec la société de consommation venait tout un lot de dangers sur la vie privée, cette dernière devrait être protégée, mais il fallait encore savoir sur quels plans agir. Le début des années 1970, en guise de résultat de ce *brainstorming* général, marquèrent alors une nouvelle ère de la *privacy* à l'Américaine à l'âge de l'informatisation et du réseautage des données personnelles. Il s'agissait de comprendre qu'un changement majeur était en train de s'effectuer avec les grands ordinateurs en réseau et qu'il fallait formaliser dans le droit les garde-fou les plus pertinents : on passait d'un monde où la vie privée pouvait faire l'objet d'une intrusion par des acteurs séparés, recueillant des informations pour leur propre compte en fonction d'objectifs différents, à un monde où les données éparses étaient désormais centralisées, avec des machines capables de traiter les informations de manière rapide et automatisée, capables d'inférer des informations sans le consentement des sujets à partir d'informations que ces derniers avaient données volontairement dans des contextes très différents.

La liste des publications de ce domaine serait bien longue. Par exemple, la Rand Corporation publia une longue liste bibliographique annotée au sujet des données personnelles informatisées. Cette liste regroupe près de 300 publications entre 1965 et 1967 sur le sujet[18].

Des auteurs universitaires firent école. On peut citer :

- Alan F. Westin : *Privacy and freedom* (1967), *Civil Liberties and Computerized Data Systems* (1971), *Databanks in a Free Society: Computers, Record Keeping and Privacy* (1972)[19] ;
- James B. Rule : *Private lives and public surveillance: social control in the computer age* (1974)[20] ;

- Arthur R. Miller : *The assault on privacy. Computers, Data Banks and Dossier* (1971)[21] ;
- Malcolm Warner et Mike Stone, *The Data Bank Society : Organizations, Computers and Social Freedom* (1970)[22].

Toutes ces publications ont ceci en commun qu'elles procédèrent en deux étapes. La première consistait à dresser un tableau synthétique de la société américaine face à la captation des informations personnelles. Quatre termes peuvent résumer les enjeux du traitement des informations : *1)* la légitimité de la captation des informations, *2)* la permanence des données et leurs modes de rétention, *3)* la transférabilité (entre différentes organisations), *4)* la combinaison ou le recoupement de ces données et les informations ainsi inférées[23].

La seconde étape consistait à choisir ce qui, dans cette « société du dossier (*dossier society*) » comme l'appelait Arthur R. Miller, devait faire l'objet de réformes. Deux fronts venaient en effet de s'ouvrir : l'État et les firmes.

Le premier, évident, était celui que la dystopie orwellienne pointait avec empressement : l'État de surveillance. Pour beaucoup de ces analystes, en effet, le fédéralisme américain et la multiplicité des agences gouvernementales pompaient allègrement la *privacy* des honnêtes citoyens et s'équipaient d'ordinateurs à temps partagé justement pour rendre interopérables les systèmes de traitement d'information à (trop) grande échelle. Un rapide coup d'œil sur les références citées, montre que, effectivement, la plupart des conclusions focalisaient sur le besoin d'adapter le droit aux impératifs constitutionnels américains. Tels sont par exemple les arguments de A. F. Westin pour lequel l'informatisation des données privées dans les différentes autorités administratives devait faire l'objet non d'un recul, mais de nouvelles règles portant sur la sécurité, l'accès des citoyens à leurs propres données et la pertinence des recoupements (comme par exemple l'utilisation restreinte du numéro de sécurité sociale). En guise de synthèse, le rapport de l'U.S. Department of health, Education and Welfare livré en 1973[24] (et où l'on retrouve Arthur R. Miller parmi les auteurs) repris ces éléments au titre de ses recommandations. Il prépara ainsi le Privacy Act de 1974, qui vise notamment à prévenir l'utilisation abusive de documents fédéraux et garantir l'accès des individus aux données enregistrées les concernant.

Le second front, tout aussi évident mais moins accessible car protégé par le droit de propriété, était celui de la récolte de données par les firmes, et en particulier les banques. L'un des auteurs les plus connus, Arthur R. Miller dans *The assault on privacy*, fit la synthèse des deux fronts en focalisant sur le fait que l'informatisation des données personnelles, par les agences gouvernementales comme par les firmes, est une forme de surveillance et donc un exercice du pouvoir. Se poser la question de leur légitimité renvoie effectivement à des secteurs différents du droit, mais c'est pour lui le traitement informatique (il utilise le terme « cybernétique ») qui est un instrument de surveillance par essence. Et cet instrument est orwellien :

> *« Il y a à peine dix ans, on aurait pu considérer avec suffisance Le meilleur des mondes de Huxley ou 1984 de Orwell comme des ouvrages de science-fiction excessifs qui ne nous concerneraient pas et encore moins ce pays. Mais les révélations publiques répandues au cours des dernières années au sujet des nouvelles formes de pratiques d'information ont fait s'envoler ce manteau réconfortant mais illusoire. »*

Pourtant, un an avant la publication de Miller fut voté le Fair Credit Reporting Act, portant sur les obligations déclaratives des banques. Elle fut aussi l'une des premières lois sur la protection des données personnelles, permettant de protéger les individus, en particulier dans le secteur bancaire, contre la tenue de bases de données secrètes, la possibilité pour les individus d'accéder aux données et de les contester, et la limitation dans le temps de la rétention des informations.

Cependant, pour Miller, le Fair Credit Reporting Act est bien la preuve que la bureaucratie informatisée et le réseautage des données personnelles impliquent deux pertes de contrôle de la part de l'individu et pour lesquelles la régulation par le droit n'est qu'un pis-aller (pp. 25-38). On peut de même, en s'autorisant quelque anachronisme, s'apercevoir à quel point les deux types de perte de contrôles qu'il pointe nous sont éminemment contemporains.

- *The individual loss of control over personal information* : dans un contexte où les données sont mises en réseau et recoupées, dès lors qu'une information est traitée par informatique, le sujet et l'opérateur n'ont plus le contrôle sur les usages qui pourront en être faits. Sont en jeu la sécurité et l'intégrité des données (que faire en cas d'espionnage ? que

faire en cas de fuite non maîtrisée des données vers d'autres opérateurs : doit-on exiger que les opérateurs en informent les individus ?).

- *The individual loss of control over the accuracy of his informational profil* : la centralisation des données permet de regrouper de multiples aspects de la vie administrative et sociale de la personne, et de recouper toutes ces données pour en inférer des profils. Dans la mesure où nous assistons à une concentration des firmes par rachats successifs et l'émergence de monopoles (Miller prend toujours l'exemple des banques), qu'arrive-t-il si certaines données sont erronées ou si certains recoupements mettent en danger le droit à la vie privée : par exemple le rapport entre les données de santé, l'identité des individus et les crédits bancaires.

Et Miller de conclure (p. 79) :

> *« Ainsi, l'informatisation, le réseautage et la réduction de la concurrence ne manqueront pas de pousser l'industrie de l'information sur le crédit encore plus profondément dans le marasme du problème de la protection de la vie privée. »*

Les échos du passé

La lutte pour la préservation de la vie privée dans une société numérisée passe par une identification des stratégies intentionnelles de la surveillance et par l'analyse des procédés d'extraction, rétention et traitement des données. La loi est-elle une réponse ? Oui, mais elle est loin de suffire. La littérature nord-américaine dont nous venons de discuter montre que l'économie de la surveillance dans le contexte du traitement informatisé des données personnelles est née il y a plus de 50 ans. Et dès le début il fut démontré, dans un pays où les droits individuels sont culturellement associés à l'organisation de l'État fédéral (la Déclaration des Droits), non seulement que la *privacy* changeait de nature (elle s'étend au traitement informatique des informations fournies et aux données inférées) mais aussi qu'un équilibre s'établissait entre le degré de sanctuarisation de la vie privée et les impératifs régaliens et économiques qui réclament une industrialisation de la surveillance.

Puisque l'intimité numérique n'est pas absolue mais le résultat d'un juste équilibre entre le droit et les pratiques, tout les jeux post-révolution informatique après les années 1960 consistèrent en une lutte perpétuelle entre défense et atteinte à la vie privée. C'est ce que montre Daniel J. Solove dans « A Brief History of Information Privacy Law »[25] en dressant un inventaire chronologique des différentes réponses de la loi américaine face aux changements technologiques et leurs répercussions sur la vie privée.

Il reste néanmoins que la dimension industrielle de l'économie de la surveillance a atteint en 2001 un point de basculement à l'échelle mondiale avec le Patriot Act[26] dans le contexte de la lutte contre le terrorisme. À partir de là, les principaux acteurs de cette économie ont vu une demande croissante de la part des États pour récolter des données au-delà des limites strictes de la loi sous couvert des dispositions propres à la sûreté nationale et au secret défense. Pour rester sur l'exemple américain, Thomas Rabino écrit à ce sujet[27] :

> *« Alors que le Privacy Act de 1974 interdit aux agences fédérales de constituer des banques de données sur les citoyens américains, ces mêmes agences fédérales en font désormais l'acquisition auprès de sociétés qui, à l'instar de ChoicePoint, se sont spécialisées dans le stockage d'informations diverses.*

> *Depuis 2001, le FBI et d'autres agences fédérales ont conclu, dans la plus totale discrétion, de fructueux contrats avec ChoicePoint pour l'achat des renseignements amassés par cette entreprise d'un nouveau genre. En 2005, le budget des États-Unis consacrait plus de 30 millions de dollars à ce type d'activité. »*

Dans un contexte plus récent, on peut affirmer que même si le risque terroriste est toujours agité comme un épouvantail pour justifier des atteintes toujours plus fortes à l'encontre de la vie privée, les intérêts économiques et la pression des lobbies ne peuvent plus se cacher derrière la Raison d'État. Si bien que plusieurs pays se mettent maintenant au diapason de l'avancement technologique et des impératifs de croissance économique justifiant par eux-mêmes des pratiques iniques. Ce fut le cas par exemple du gouvernement de Donald Trump qui, en mars 2017 et à la plus grande joie du lobby des fournisseurs d'accès, abroge une loi héritée du gouvernement précédent et qui exigeait que les FAI obtiennent sous conditions la permission de partager des renseignements personnels – y compris les données de localisation[28].

Encore en mars 2017, c'est la secrétaire d'État à l'Intérieur Britannique Amber Rudd qui juge publiquement « inacceptable » le chiffrement des communications de bout en bout et demande aux fournisseurs de messagerie de créer discrètement des *backdoors*, c'est à dire renoncer au chiffrement de bout en bout sans le dire aux utilisateurs[29]. Indépendamment du caractère moralement discutable de cette injonction, on peut mesurer l'impact du message sur les entreprises comme Google, Facebook et consors : il existe des décideurs politiques capables de demander à ce qu'un fournisseur de services propose à ses utilisateurs un faux chiffrement, c'est-à-dire que le droit à la vie privée soit non seulement bafoué mais, de surcroît, que le mensonge exercé par les acteurs privés soit couvert par les acteurs publics, et donc par la loi.

Comme le montre Shoshana Zuboff, le capitalisme de surveillance est aussi une idéologie, celle qui instaure une hiérarchie entre les intérêts économiques et le droit. Le droit peut donc être une arme de lutte pour la sauvegarde de la vie privée dans l'économie de la surveillance, mais il ne saurait suffire dans la mesure où il n'y pas de loyauté entre les acteurs économiques et les sujets et parfois même encore moins entre les décideurs publics et les citoyens.

Dans ce contexte où la confiance n'est pas de mise, les portes sont restées ouvertes depuis les années 1970 pour créer l'industrie des *big data* dont le carburant principal est notre intimité, notre quotidienneté. C'est parce qu'il est désormais possible de repousser toujours un peu plus loin les limites de la captation des données personnelles que des théories économique prônent la fidélisation des clients et la prédiction de leurs comportements comme seuls points d'appui des investissements et de l'innovation. C'est vrai dans le marketing, c'est vrai dans les services et l'innovation numériques. Et tout naturellement c'est vrai dans la vie politique, comme le montre par exemple l'affaire des *dark posts* durant la campagne présidentielle de D. Trump : la possibilité de contrôler l'audience et d'influencer une campagne présidentielle via les réseaux sociaux comme Facebook est désormais démontrée.

Tant que ce modèle économique existera, aucune confiance ne sera possible. La confiance est même absente des pratiques elles-mêmes, en particulier dans le domaine du traitement algorithmique des informations. En septembre 2017, la chercheuse Zeynep Tufekci, lors d'une conférence TED[30], reprenait exactement les questions d'Arthur R. Miller dans *The assault on privacy*, soit 46 ans après. Miller prenait comme étude de cas le stockage d'information bancaire sur les clients débiteurs, et Tufekci prend les cas des réservation de vols aériens en ligne et du streaming vidéo. Dans les deux réflexions, le constat est le même : le traitement informatique de nos données personnelles implique que nous (les sujets et les opérateurs eux-mêmes) perdions le contrôle sur ces données :

> *« Le problème, c'est que nous ne comprenons plus vraiment comment fonctionnent ces algorithmes complexes. Nous ne comprenons pas comment ils font cette catégorisation. Ce sont d'énormes matrices, des milliers de lignes et colonnes, peut-être même des millions, et ni les programmeurs, ni quiconque les regardant, même avec toutes les données, ne comprend plus comment ça opère exactement, pas plus que vous ne sauriez ce que je pense en ce moment si l'on vous montrait une coupe transversale de mon cerveau. C'est comme si nous ne programmions plus, nous élevons une intelligence que nous ne comprenons pas vraiment. »*

Z. Tufekci montre même que les algorithmes de traitement sont en mesure de fournir des conclusions (qui permettent par exemple d'inciter les utilisateurs à visualiser des vidéos sélectionnées d'après leur profil et leur historique) mais que

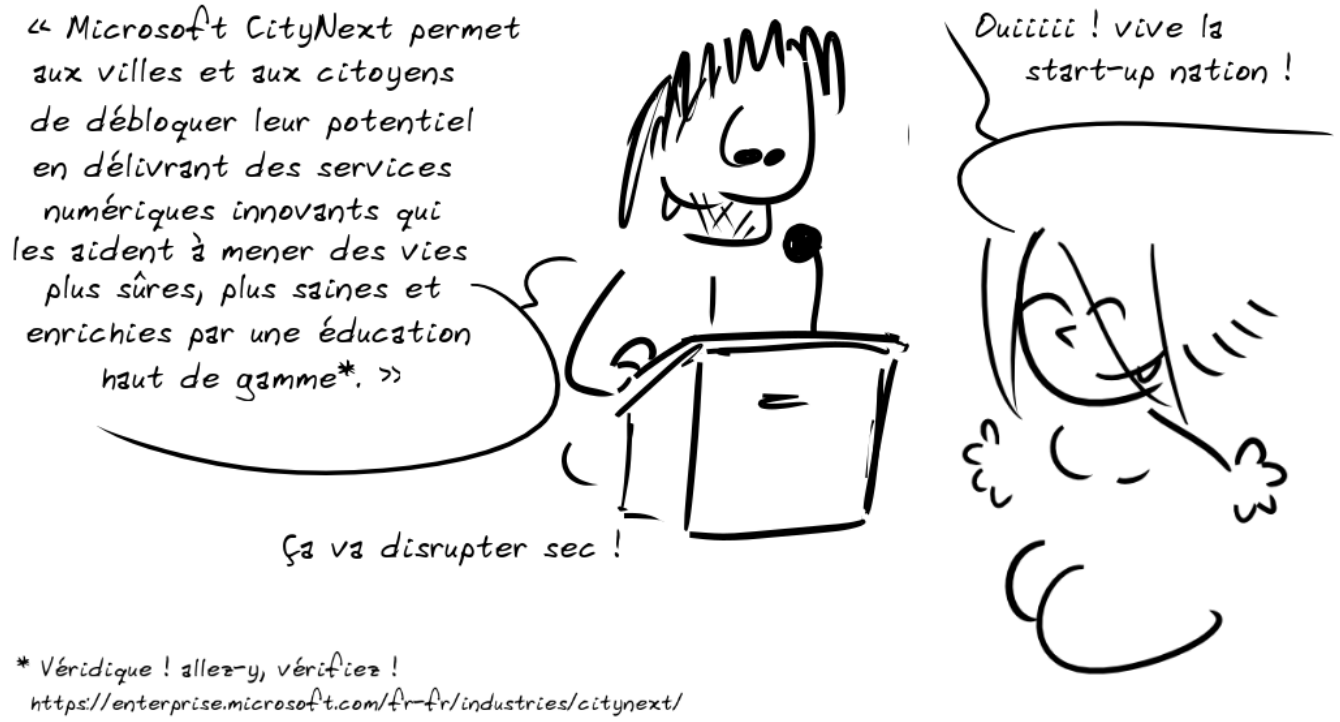
ces conclusions ont ceci de particulier qu'elle modélisent le comportement humain de manière à l'influencer dans l'intérêt du fournisseur. D'après Z. Tufekci : « L'algorithme a déterminé que si vous pouvez pousser les gens à penser que vous pouvez leur montrer quelque chose de plus extrême (nda : des vidéos racistes dans l'exemple cité), ils ont plus de chances de rester sur le site à regarder vidéo sur vidéo, descendant dans le terrier du lapin pendant que Google leur sert des pubs. »

Ajoutons de même que les technologies de *deep learning*, financées par millions par les GAFAM, se prêtent particulièrement bien au jeu du traitement automatisé en cela qu'elle permettent, grâce à l'extrême croissance du nombre de données, de procéder par apprentissage. Cela permet à Facebook de structurer la grande majorité des données des utilisateurs qui, auparavant, n'était pas complètement exploitable[31]. Par exemple, sur les milliers de photos de chatons partagées par les utilisateurs, on peut soit se contenter de constater une redondance et ne pas les analyser davantage, soit apprendre à y reconnaître d'autres informations, comme par exemple l'apparition, en arrière-plan, d'un texte, d'une marque de produit, etc. Il en est de même pour la reconnaissance faciale, qui a surtout pour objectif de faire concorder les identités des personnes avec toutes les informations que l'on peut inférer à partir de l'image et du texte.

Si les techniques statistiques ont le plus souvent comme objectif de contrôler les comportements à l'échelle du groupe, c'est parce que le seul fait de catégoriser automatiquement les individus consiste à considérer que leurs données personnelles en constituent l'essence. L'économie de la surveillance démontre ainsi qu'il n'y a nul besoin de connaître une personne pour en prédire le comportement, et qu'il n'y a pas besoin de connaître chaque individu d'un groupe en particulier pour le catégoriser et prédire le comportement du groupe, il suffit de laisser faire les algorithmes : le tout est d'être en mesure de classer les sujets dans les bonnes catégories et même faire en sorte qu'ils y entrent tout à fait. Cela a pour effet de coincer littéralement les utilisateurs des services « capteurs de données » dans des *bulles de filtres* où les informations auxquelles ils ont accès leur sont personnalisées selon des profils calculés[32]. Si vous partagez une photo de votre chat devant votre cafetière, et que dernièrement vous avez visité des sites marchands, vous aurez de grandes chance pour vos futures annonces vous proposent la marque que vous possédez déjà et exercent, par effet de répétition, une pression si forte que c'est cette marque que vous finirez par acheter. Ce qui

fonctionne pour le marketing peut très bien fonctionner pour d'autres objectifs, même politiques.

En somme tous les déterminants d'une société soumise au capitalisme de surveillance, apparus dès les années 1970, structurent le monde numérique d'aujourd'hui sans que les lois ne puissent jouer de rôle pleinement régulateur. L'usage caché et déloyal des *big data*, le trafic de données entre organisations, la dégradation des droits individuels (à commencer par la liberté d'expression et le droit à la vie privée), tous ces éléments ont permis à des monopoles d'imposer un modèle d'affaire et affaiblir l'État-nation. Combien de temps continuerons-nous à l'accepter ?



Sortir du marasme

En 2016, à la fin de son article synthétique sur le capitalisme de surveillance[33], Shoshana Zuboff exprime personnellement un point de vue selon lequel la réponse ne peut pas être uniquement technologique :

> *« (…) les faits bruts du capitalisme de surveillance suscitent nécessairement mon indignation parce qu'ils rabaissent la dignité humaine. L'avenir de cette*

question dépendra des savants et journalistes indignés attirés par ce projet de frontière, des élus et des décideurs indignés qui comprennent que leur autorité provient des valeurs fondamentales des communautés démocratiques, et des citoyens indignés qui agissent en sachant que l'efficacité sans l'autonomie n'est pas efficace, la conformité induite par la dépendance n'est pas un contrat social et être libéré de l'incertitude n'est pas la liberté. »

L'incertitude au sujet des dérives du capitalisme de surveillance n'existe pas. Personne ne peut affirmer aujourd'hui qu'avec l'avènement des *big data* dans les stratégies économiques, on pouvait ignorer que leur usage déloyal était non seulement possible mais aussi que c'est bien cette direction qui fut choisie d'emblée dans l'intérêt des monopoles et en vertu de la centralisation des informations et des capitaux. Depuis les années 1970, plusieurs concepts ont cherché à exprimer la même chose. Pour n'en citer que quelques-uns : computocracie (M. Warner et M. Stone, 1970), société du dossier (Arthur R. Miller, 1971), surveillance de masse (J. Rule, 1973), dataveillance (R. Clarke, 1988), capitalisme de surveillance (Zuboff, 2015)… tous cherchent à démontrer que la surveillance des comportements par l'usage des données personnelles implique en retour la recherche collective de points de rupture avec le modèle économique et de gouvernance qui s'impose de manière déloyale. Cette recherche peut s'exprimer par le besoin d'une régulation démocratiquement décidée et avec des outils juridiques. Elle peut s'exprimer aussi autrement, de manière violente ou pacifiste, militante et/ou contre-culturelle.

Plusieurs individus, groupes et organisation se sont déjà manifestés dans l'histoire à ce propos. Les formes d'expression et d'action ont été diverses :

- institutionnelles : les premières formes d'action pour garantir le droit à la vie privée ont consisté à établir des rapports collectifs préparatoires à des grandes lois, comme le rapport *Records, computers and the rights of citizens*, de 1973, cité plus haut ;
- individualistes, antisociales et violentes : bien que s'inscrivant dans un contexte plus large de refus technologique, l'affaire Theodore Kaczynski (alias Unabomber) de 1978 à 1995 est un bon exemple d'orientation malheureuse que pourraient prendre quelques individus isolés trouvant des justifications dans un contexte paranoïaque ;
- collectives – activistes – légitimistes : c'est le temps des manifestes

cypherpunk des années 1990[34], ou plus récemment le mouvement Anonymous, auxquels on peut ajouter des collectifs « événementiels », comme le Jam Echelon Day ;
- Associatives, organisées : on peut citer le mouvement pour le logiciel libre et la Free Software Foundation, l'Electronic Frontier Foundation, La Quadrature du Net, ou bien encore certaines branches d'activité d'organisation plus générales comme la Ligue des Droits de l'Homme, Reporter Sans Frontière, etc.

Les limites de l'attente démocratique sont néanmoins déjà connues. La société ne peut réagir de manière légale, par revendication interposée, qu'à partir du moment où l'exigence de transparence est remplie. Lorsqu'elle ne l'est pas, au pire les citoyens les plus actifs sont taxés de complotistes, au mieux apparaissent de manière épisodique des alertes, à l'image des révélations d'Edward Snowden, mais dont la fréquence est si rare malgré un impact psychologique certain, que la situation a tendance à s'enraciner dans un *statu quo* d'où sortent généralement vainqueurs ceux dont la capacité de lobbying est la plus forte.

À cela s'ajoute une difficulté technique due à l'extrême complexité des systèmes de surveillance à l'œuvre aujourd'hui, avec des algorithmes dont nous maîtrisons de moins en moins les processus de calcul (cf. Z. Tufekci). À ce propos on peut citer Roger Clarke[35] :

> *« Dans une large mesure, la transparence a déjà été perdue, en partie du fait de la numérisation, et en partie à cause de l'application non pas des approches procédurales et d'outils de développement des logiciels algorithmiques du XX^{e} siècle, mais à cause de logiciels de dernière génération dont la raison d'être est obscure ou à laquelle la notion de raison d'être n'est même pas applicable. »*

Une autre option pourrait consister à mettre en œuvre un modèle alternatif qui permette de sortir du marasme économique dans lequel nous sommes visiblement coincés. Sans en faire l'article, le projet Contributopia de Framasoft cherche à participer, à sa mesure, à un processus collectif de réappropriation d'Internet et, partant:

- montrer que le code est un bien public et que la transparence, grâce aux principes du logiciel libre (l'ouverture du code), permet de proposer aux

individus un choix éclairé, à l'encontre de l'obscurantisme de la dataveillance ;
- promouvoir des apprentissages à contre-courant des pratiques de captation des vies privées et vers des usages basés sur le partage (du code, de la connaissance) entre les utilisateurs ;
- rendre les utilisateurs autonomes et en même temps contributeurs à un réseau collectif qui les amènera naturellement, par l'attention croissante portée aux pratiques des monopoles, à refuser ces pratiques, y compris de manière active en utilisant des solutions de chiffrement, par exemple.

Mais Contributopia de Framasoft ne concerne que quelques aspects des stratégies de sortie du capitalisme de surveillance. Par exemple, pour pouvoir œuvrer dans cet esprit, une politique rigide en faveur de la neutralité du réseau Internet doit être menée. Les entreprises et les institutions publiques doivent être aussi parmi les premières concernées, car il en va de leur autonomie numérique, que cela soit pour de simples questions économiques (ne pas dépendre de la bonne volonté d'un monopole et de la logique des brevets) mais aussi pour des questions de sécurité. Enfin, le passage du risque pour la vie privée au risque de manipulation sociale étant avéré, toutes les structures militantes en faveur de la démocratie et les droits de l'homme doivent urgemment porter leur attention sur le traitement des données personnelles. Le cas de la britannique Amber Rudd est loin d'être isolé : la plupart des gouvernements collaborent aujourd'hui avec les principaux monopoles de l'économie numérique et, donc, contribuent activement à l'émergence d'une société de la surveillance. Aujourd'hui, le droit à la vie privée, au chiffrement des communications, au secret des correspondances sont des droits à protéger coûte que coûte sans avoir à choisir entre la liberté et les épouvantails (ou les sirènes) agités par les communicants.

Pour aller plus loin :

- La série d'articles sur le framablog
    - Les nouveaux Léviathans Ia
    - Les nouveaux Léviathans Ib
    - Les nouveaux Léviathans IIa
    - Les nouveaux Léviathans IIb
    - Les nouveaux Léviathans III

        - Les nouveaux Léviathans IV
        - Les Nouveaux Léviathans V
        - Les anciens Léviathans I
        - Les anciens Léviathans II
- La série d’article au complet (fichier .epub)