Tristan Nitot (dir.), Nina Cercy

Numérique : reprendre le contrôle

Framasoft est un réseau d'éducation populaire, issu du monde éducatif, consacré principalement au logiciel libre. Il s'organise en trois axes sur un mode collaboratif : promotion, diffusion et développement de logiciels libres, enrichissement de la culture libre et offre de services libres en ligne.

Pour plus d'informations sur Framasoft, consultez `http://www.framasoft.org`.

Se démarquant de l'édition classique, les Framabooks sont dits « livres libres » parce qu'ils sont placés sous une licence qui permet au lecteur de disposer des mêmes libertés qu'un utilisateur de logiciels libres. Les Framabooks s'inscrivent dans cette culture des biens communs qui favorise la création, le partage, la diffusion et l'appropriation collective de la connaissance.

Pour plus d'informations sur le projet Framabook, consultez `http://framabook.org`.

ISBN : 979-10-92674-13-2
Prix : 8 euros
Dépôt légal : novembre 2016
Mise en page avec LaTeX

Note — Ce livre a été rédigé dans le cadre du Paris Open Source Summit 2016, par Nina Cercy sous la direction de Tristan Nitot pour le compte de Cozy Cloud. Tristan et Nina remercient chaleureusement toutes les personnes ayant participé à l'élaboration de ce livre, les interviewé-e-s ainsi que les relecteur-trice-s et les membres bénévoles du comité éditorial Framabook (Framasoft), coordonné par Christophe Masutti.

Avant-propos

La donnée, enjeu majeur du numérique

Dire que la donnée est le pétrole du XXI^{e} siècle est déjà un lieu commun. Que ce soit pour nous aider à prendre de meilleures décisions, pour mieux prendre soin de notre santé, pour nous self-quantifier ou nous proposer des publicités ciblées, les acteurs de la donnée personnelle sont de plus en plus nombreux.

Il n'y aurait rien à redire si la gestion des données personnelles – et par extension, de notre vie privée – ne se faisait pas au détriment des individus. Les acteurs de la donnée personnelle, aussi connus sous le terme de GAFAM (Google, Apple, Facebook, Amazon, Microsoft) représentent aujourd'hui les plus grosses capitalisations boursières mondiales. Ils occupent une place prépondérante dans la vie des internautes : Facebook annonce 800 millions d'utilisateurs de Messenger et 900 millions de WhatsApp, Google occupe 90% de parts de marché dans le domaine des moteurs de recherche et Gmail revendiquait, en 2015, 900 millions de comptes différents, loin devant Microsoft, qui en annonçait 475 millions.

Des services comme Facebook et Google réclament d'énormes infrastructures, et proposent pourtant leurs services gratuitement aux internautes. Ou presque. Comme on l'entend souvent sur Internet : quand c'est gratuit, c'est vous le produit, et c'est effectivement en collectant des données personnelles, en profilant et en proposant de la publicité ciblée à leurs utilisateurs que se financent des services comme Google et Facebook, totalement incontournables dans le paysage numérique contemporain. Un acteur

comme Apple, en revanche, va suivre un modèle très différent : vendre cher des appareils très performants et intuitifs, mais qui ne se synchroniseront qu'entre eux, ce qui incite les utilisateurs à investir dans tout le parc (smartphone, ordinateur, montre connectée…) pour profiter de services optimaux, quitte à s'enfermer dans une cage dorée. Ces entreprises n'ont qu'un seul point commun : nous remettons à chacune d'entre elles une partie de notre autonomie numérique. Nous acceptons cette forte dépendance, et les quatre ou cinq acteurs les plus influents du Net contrôlent de fait une immense part du paysage numérique actuel.

Données personnelles : histoire d'une dépossession

Nous donnons de plein gré plus de renseignements à Facebook que nous n'en fournirions au cours d'un interrogatoire. L'analyse de nos données Google ou de nos données Apple trace un portrait plus fidèle de nous que ce que pourrait faire notre meilleur ami. Ces acteurs agrègent la quasi totalité de notre vie privée en ligne, la stockent sur leurs serveurs, et exploitent les informations à leur bénéfice : jamais nous n'avons produit autant de données, et jamais nous n'avons eu aussi peu de maîtrise sur elles. Disséminées sur les serveurs de quelques acteurs centraux, elles sont exploitées, analysées, monétisées pour des régies publicitaires et alimentent un marketing ciblé toujours plus présent et efficace. Cette situation pose plusieurs problèmes :

— nos données sont hébergées dans des silos qui ne communiquent pas entre eux, et ne souhaitent pas le faire. Impossible dans ces conditions de combiner et centraliser nos données personnelles à notre propre bénéfice ;

— la concentration des données personnelles des individus (courriels, centres d'intérêt, orientations politiques, amis, photos…) dans quelques grands silos centralisés rend possible économiquement une surveillance de masse à l'échelle étatique ;

— en utilisant les services des GAFAM, nous nous plions – plus ou moins explicitement – à leurs conditions d'utilisation.

> Les données qui transitent par leurs services (Drive, Messagerie Facebook, Instagram…) leur appartiennent de droit. Nous nous plions également à leurs règles : compte arbitrairement suspendu, changement d'interface qui pourrait poser problème aux personnes en situation de handicap…

Quand Tim Berners-Lee conçoit ce qui va devenir le Web, il insiste sur sa nature décentralisée comme élément fondamental à sa structure. Et si les moyens technologiques et économiques de l'époque n'ont pas permis cette décentralisation totale, il n'est pas trop tard pour reprendre le contrôle aujourd'hui. Les alternatives techniques existent, la philosophie portée par le logiciel libre est garante des piliers sur lesquels appuyer une économie de confiance : fiabilité, indépendance, interopérabilité. Les données que produit un individu lui appartiennent en droit. Mais elles sont entreposées dans d'immenses silos, difficiles à exporter et à récupérer, et changer de solution relève quasiment de l'impossible. La souveraineté et l'autonomie numériques des individus ne sont pas des combats gagnés d'avance : il nous appartient de penser un Internet différent, libre et décentralisé. Nous en avons aujourd'hui les moyens !

Souveraineté et autonomie numériques

Présenter les différents enjeux liés à la souveraineté sur nos données et à l'autonomie numérique, voilà l'ambition de ce livre. Nous avons interrogé différents acteurs du paysage numérique actuel. Ils nous ont parlé de ce qui les mobilise et de l'Internet qu'ils voudraient voir exister demain.

L'objectif : tracer un parcours clair et compréhensible au sein des problématiques de souveraineté et d'autonomie, en donnant la parole à des intervenants et intervenantes de tous les horizons. Nous les remercions du fond du cœur pour leurs contributions de grande qualité, sans lesquelles ce livre n'existerait pas.

— Nina CERCY

Logiciel libre et autonomie numérique

Cela a commencé tout simplement par une imprimante qui fonctionne mal dans une université américaine : en 1984, un certain Richard Stallman voulait résoudre un bug ennuyeux dans le logiciel qui pilotait ladite imprimante, mais le fournisseur a refusé, arguant du fait que le logiciel était « propriétaire », c'est à dire non modifiable par tous. Ainsi, Richard Stallman a pris conscience que celui qui détient le contrôle du code informatique détient aussi le pouvoir sur les utilisateurs de logiciel. Il lança alors le mouvement dit du « logiciel libre », qui est surtout un mouvement pour que chacun soit libre dans son utilisation de l'informatique.

Trente-deux ans plus tard, en 2016, les choses ont bien changé, et l'informatique a envahi nos vies. D'une certaine manière, le logiciel libre a gagné sa bataille contre le logiciel propriétaire : l'essentiel de l'infrastructure de l'Internet tourne grâce à des logiciels libres. Les principaux navigateurs du Web sont aussi des logiciels libres. Le leader des smartphones, Android, repose sur une base de logiciels libres, dont le noyau Linux. De même Linux (ou plutôt GNU/Linux) fait tourner la majorité des plus gros ordinateurs du monde. Aujourd'hui, nombre de *start-ups* se montent à moindre coût et plus rapidement que jamais grâce à leur utilisation de logiciels libres souvent gratuits.

Pourtant le combat pour le logiciel libre, qui vise à donner à chacun le contrôle de ses outils informatiques, est loin d'être gagné. En effet, quand Richard Stallman a commencé son combat, c'était le début de l'ère de la micro-informatique, et l'idée d'avoir un ordinateur personnel pour tous relevait encore du fantasme. Aujourd'hui, au moins en Occident, nous utilisons presque tous trois types d'ordinateurs : un ordinateur personnel (PC, Personal Computer), un smartphone et un *cloud*, un ordinateur dans les nuages, qui nous offre des services tels qu'un *webmail*, un agenda, un réseau social, une application de cartographie, le stockage de nos fichiers, nos photos, la musique que nous écoutons, les vidéos que nous regardons.

Ce *cloud* est, pour Richard Stallman, un cauchemar. En effet, le *cloud*, c'est l'ordinateur de quelqu'un d'autre, qui fait tourner du logiciel sur lequel nous n'avons pas le contrôle. Pire, il contient la plupart de nos données. En termes de contrôle, de souveraineté, l'ère du *cloud* est une formidable régression par rapport à l'idéal d'un PC équipé de logiciels libres.

Imaginons un instant que Google, Facebook, ou des services comme Dropbox, Spotify et Evernote ferment mon compte, ou votre compte. Nous voilà enfermés en dehors de nos vies numériques. Nous perdons l'accès à nos mails, nos contacts, nos fichiers, nos amis, nos photos… Ce scénario démontre bien à quel point nous sommes peu souverains, comment nous avons peu de contrôle sur notre vie numérique.

La promesse initiale du logiciel libre, c'est de rendre de l'autonomie aux individus. C'est Richard Stallman qui se rend compte que le logiciel propriétaire est en train de prendre peu à peu le contrôle de nos ordinateurs, et qui veut empêcher cela. Il définit le logiciel libre comme un logiciel qui respecte un ensemble de libertés, afin d'éviter qu'on perde le contrôle de notre matériel. Et il avait raison : depuis qu'il a donné cette définition en 1984, les ordinateurs sont devenus omniprésents dans nos vies.

Je ne crois pas qu'il faille se résigner pour autant. Certes, notre souveraineté numérique individuelle est sévèrement remise en cause. Mais des pistes existent pour reprendre le contrôle. Des

hacktivistes, des développeurs de logiciel, des penseurs, des régulateurs se sont penchés sur le problème. Nous sommes allés à leur rencontre pour faire le point sur ce sujet. Les échanges ont été passionnants. J'espère que vous aurez autant de plaisir à lire ce livre que nous en avons eu à le rédiger.

Librement,

— Tristan NITOT

1

Données personnelles et nouveaux usages

Reprendre le contrôle sur ses données, oui, mais pour quoi faire ?

Les internautes ont de nombreuses raisons d'être inquiets de la collecte de données personnelles effectuée par les grands acteurs numériques contemporains. Mais au-delà de l'inquiétude, récupérer ses données personnelles est aussi une chance formidable de voir émerger de nouveaux usages ! Reprenons depuis le début : une donnée personnelle, qu'est-ce que c'est ?

« Données personnelles » : voilà une expression qui est à la fois très parlante (nous avons tous une idée de données personnelles nous concernant) et très vague. Il existe des informations à notre sujet qui sont des données à caractère personnel : lorsque je partage ma date de naissance sur Facebook, je partage une donnée à caractère personnel, qui donne des informations à mon sujet et peut éventuellement permettre de m'identifier. Je choisis de partager cette donnée : le fait qu'elle soit publique ne me dérange pas, et elle permet par exemple à mes amis de me souhaiter un joyeux anniversaire lorsque Facebook les informe que mon anniversaire a lieu ce jour-là. Lorsque je fournis mes préférences à un site de ren-

contres, je fournis là encore des données à caractère personnel. Cela ne me dérange pas qu'elles soient rendues publiques dans le cadre de ce site, mais je n'ai pas forcément envie que mon employeur connaisse mon orientation sexuelle et mes préférences. Enfin, nous produisons aussi tous les jours des données personnelles sans y penser : ma position sur Google Maps est tracée toute la journée par défaut. Mon iWatch compte mon nombre de pas, mon temps de sommeil. Mon compteur électrique, tout simplement, enregistre la consommation d'électricité chez moi.

Qu'est-ce qui est fait aujourd'hui de mes données personnelles ?

Des données personnelles que nous fournissons volontairement, nous savons globalement comment elles sont utilisées : si je fournis des préférences à un site de rencontres, il va les utiliser pour me faire rencontrer des personnes qui me correspondent *a priori*. La transaction est claire : je paie un abonnement et, en échange, j'obtiens un service qui se nourrit de mes données personnelles. Mais que se passe-t-il quand je ne paie rien ? Si on traite du modèle de la gratuité au chapitre sur les modèles d'affaires, il est bon de rappeler ici que nos données personnelles, volontaires et involontaires, sont utilisées pour établir un profil qui permettra de nous présenter de la publicité ciblée. On ne sait pas exactement ce qui est collecté (mais la plus grande quantité possible), on ne sait pas comment sont traitées ces informations, ni ce qu'on en déduit sur nous. L'objectif : nous offrir le meilleur service possible et nous garder dans l'écosystème.

Mais alors, pourquoi se les ré-approprier ?

Si les raisons de s'inquiéter sont nombreuses, se ré-approprier ses données est d'abord une immense chance ! Nos données sont stockées chez les acteurs qui les récupèrent : impossible de demander à Facebook de communiquer avec Google pour améliorer ses services, interdiction à ma banque de récupérer en direct

ma consommation électrique (et heureusement !) pour provisionner la somme d'argent correspondante en direct. Mais si je récupère toutes ces données, rien ne m'empêche d'en faire ce que je veux tant que c'est moi qui le décide. Ces données m'appartiennent. Être souverain sur elles, c'est gagner en autonomie. Avec les capacités de traitement qui émergent aujourd'hui, ne pas dépendre d'un acteur ou d'un autre, c'est gagner en liberté de faire absolument ce qu'on souhaite de sa vie numérique.

Et concrètement ?

Concrètement, cette position est proche du courant du *self-data*, représenté notamment par la FING (Fondation Internet Nouvelle Génération) en France. Le *self-data*, c'est considérer que si les données personnelles ont une valeur pour les entreprises, elles en ont sans doute une pour nous. Et en rapatriant toutes nos données chez nous, on peut espérer en tirer des choses plus intéressantes qu'en laissant les entreprises unilatéralement collecter ce qu'elles peuvent. C'est une nouvelle façon d'interagir avec les entreprises : choisir ce qu'on partage, comment on le partage, et dans quel but. Nous nous sommes entretenus avec Daniel Kaplan, président de la FING, qui nous parle d'autonomie numérique et du projet MesInfos.

DANIEL KAPLAN

Co-fondateur et délégué général de la FING (Fondation Internet Nouvelle Génération) depuis 2000. Il participe au Conseil National du Numérique depuis 2013.

À la recherche de l'autonomie perdue

— L'expression « données personnelles » est aujourd'hui utilisée partout et par tout le monde : quel sens lui donnez-vous ?

— Il existe une définition juridique de ce que sont les données personnelles, qui désigne en substance toutes les données qui ont un lien, direct ou indirect, avec votre identité. Ces données sont la plupart du temps produites ou capturées à votre propos au cours des différents actes de la vie. D'autre part, si on les utilise et qu'on les croise, elles permettent également de savoir des choses sur vous quand on en a besoin, pour des raisons plus ou moins licites. Elles permettent aussi de vous identifier au sein d'une masse de personnes.

Ces données peuvent avoir un lien direct ou indirect avec vous : un identifiant ou des informations qui permettent de constater facilement qu'elles ont trait à vous, même si elles ne sont pas clairement reliées à votre identité. Pour la FING (Fondation Internet Nouvelle Génération), cette définition est évidemment légitime, mais nous essayons aussi de réfléchir en termes d'autonomie et de capabilité. Les données personnelles sont les données qui ont trait à vous et qui peuvent avoir une utilité, soit directement pour vous, soit pour une organisation – et il est évidemment nécessaire que ce soit encadré dans ce contexte.

— Comment expliquez-vous l'engouement actuel que l'on observe pour ces données personnelles ?

— L'engouement n'est pas actuel, mais s'inscrit dans un mouvement sur le long terme, qui a plusieurs décennies. Cela fait même tellement longtemps que cet intérêt existe que la première grande loi sur l'informatique en France est une loi sur les données personnelles ! Au départ, elle interdisait aux organismes publics les croisements intempestifs de fichiers grâce auxquels différentes administrations croiseraient leurs données pour trouver par exemple les fraudeurs au fisc, ou bien attribuer ou ne plus attribuer des droits. C'est une évolution qui est complètement consubstantielle à la numérisation progressive de différents processus administratifs, économiques, commerciaux et sociaux. À partir du moment où la relation avec un client passe très largement par un système informatique, l'entreprise possède forcément des données relatives à ce client. Des données d'identification, d'abord, et surtout un très grand nombre de données qui ont trait à la relation qu'elle a avec lui : les contrats que vous avez avec le client, leur fonctionnement, les transactions, les achats, etc.

Très vite, les grands services publics s'informatisent et, à peu près en même temps, débute ce qu'on appelle le marketing *one-to-one*. Le marketing *one-to-one* naît lorsqu'on commence à considérer que nous sommes entrés dans une période d'industrialisation de la relation-client au travers de l'informatisation. La question : comment peut-on recréer les conditions d'une relation personnalisée, qui n'est pas seulement la relation avec un être abstrait ou une série de contrats mais avec une personne qui a ses attentes, son histoire, sa personnalité, et ce alors qu'on est dans une relation de masse médiée par un système d'information ? Mon commerçant de proximité, par exemple, me connaît non seulement comme la personne qui aime acheter tel ou tel produit, mais aussi comme une personne qui parfois vient avec ses enfants ou sa compagne, qui aime bien faire la fête, qui est habillée de telle et telle façon. Éventuellement, il peut me reconnaître, me proposer la même chose que d'habitude, me donner des conseils. Est-ce que l'entreprise pour-

rait apprendre à proposer le même service à partir de l'historique de sa relation ? Ainsi, on commence à chercher et recouper l'information pour construire des profils cohérents : ce sont les débuts de la segmentation.

Aujourd'hui on est bien au-delà de ça parce qu'on a plus d'informations et une bien meilleure capacité de traitement, mais on reste dans le même mouvement : essayer de mieux comprendre les individus, clients ou prospects pour créer une relation plus riche, leur vendre plus de produits ou des produits plus chers. À l'époque, l'objectif était double : fidélisation et densification de la relation. Pour densifier la relation, il fallait être en rapport avec une personne, et pas seulement une série de contrats et d'opérations. Or, la seule manière de faire des propositions pertinentes pour un système informatique, c'est de cumuler l'information. Finalement, le *Big Data* n'est qu'un moment où nous avons passé un certain nombre de seuils dans cette problématique de collecte de données. Mais l'intérêt pour les données personnelles est ancien, il a bientôt 40 ans et les questions sont présentes depuis que l'informatique s'est immiscée dans la relation avec les clients, les usagers, les administrés, les salariés…

Le moment *Big Data*, c'est l'explosion de la quantité de données produites au sein de la société de l'information, notamment parce que les utilisateurs commencent à produire eux-mêmes de la donnée. On publie des choses sur Facebook, YouTube, Twitter, on se met en relation avec ses amis, on contribue à des débats, on confie ses documents à Google ou à d'autres, et on engendre des volumes de données considérables. On obtient une série de données comportementales qui n'ont rien à voir avec le fait d'avoir un contrat avec telle ou telle entreprise, mais tout à voir avec le fait qu'on a laissé des dispositifs capturer des données à partir de pratiques en ligne, de mobilité physique, pour nourrir un certain nombre de services. Petit à petit, on arrive à des volumes considérables et on développe en même temps des moyens de traiter ce volume de données disparates. La technique est assez ancienne, finalement, mais l'évolution des outils informatiques permet de le faire sur des bases de données beaucoup plus importantes, à des coûts raisonnables et

presque instantanément quand il s'agit de faire du *retargeting* sur le web. Ce sont des passages de seuil dans un mouvement ancien dont la base est toujours la même : est-ce que l'on peut proposer à un système informatique d'être en charge d'une partie importante de la relation avec des clients ou des prospects et de prendre les décisions les moins idiotes possibles ?

La seule différence entre hier et aujourd'hui, c'est le passage de seuils. Entre le moment où seules quelques personnes très riches avaient une automobile et celui où on a refait intégralement le paysage urbain autour de l'automobile, on sent bien qu'un seuil a été franchi. Aujourd'hui, le traitement des données personnelles connaît effectivement une nouveauté : une grande partie de la collecte n'a plus à voir avec une relation établie, consciente, contractualisée avec les entreprises. Ces données sont la trace d'une activité ou viennent des supports qu'on utilise pour se mettre en relation avec d'autres personnes, pour s'exprimer, ce qui n'est pas du tout la même chose que faire un achat ou un acte administratif. Et les capacités de traitement permettent de tirer des conclusions qui vont très loin, qui rendent cela accessibles à de nombreux acteurs. Les individus sont ainsi de plus en plus environnés de décisions informatiques, qui vont de la micro-décision qui consiste à m'afficher un peu partout sur le web des publicités pour des vélos parce que je suis fan de vélo, à la prédiction comportementale qui voudrait modéliser mes risques de devenir un délinquant.

Une autre différence, c'est le passage du champ politique à l'expérience quotidienne des gens. La question de la collecte des données a longtemps été présente dans le champ politique : aujourd'hui, elle commence à intervenir dans la vie en ligne des individus au point que les pratiques en matière de collecte de données sont vraisemblablement une des causes de la dégradation forte de la confiance accordée aux entreprises et peut-être une des causes de la dégradation assez nette de la fidélité, qui était pourtant l'objectif de départ du marketing *one-to-one*. C'est aussi la première fois que les technologies de protection de la vie privée, comme les *adblockers*, commencent à représenter une part significative des pra-

tiques des internautes, au point d'inquiéter un certain nombre de sites qui vivent de la publicité.

— N'est-ce pas paradoxal de confier tant de données tout en manifestant une vraie perte de confiance envers les entreprises ?

— Ce n'est pas parce qu'on confie des données qu'on fait confiance à ceux à qui on les confie. La confiance vis-à-vis de ces acteurs-là est aujourd'hui très basse, plutôt plus basse que pour les acteurs pré-numériques, mais l'absence de confiance ne veut pas dire qu'on ne traite pas avec les gens. Cela dit, on le fait en partie parce qu'on a le sentiment qu'il n'y a pas d'alternatives. La conséquence, ce n'est pas qu'il ne se passe rien : on a toujours besoin de ces services, mais les gens sont sensibles à de nouvelles propositions et peuvent plus facilement basculer d'une proposition à une autre, pour peu qu'on leur en donne les moyens. C'est plus difficile en ligne parce qu'il y a un vrai effet de réseau : quand vous avez construit tout votre réseau sur Facebook, se dire qu'on va aller voir autre chose – pas forcément pour des problématiques de vie privée mais pour d'autres raisons –, c'est très compliqué. Vous avez déjà un énorme investissement sur la plateforme, qu'il est très difficile de faire bouger. C'est d'ailleurs sur ce genre de cas que les lois sur la portabilité pourraient jouer un rôle, ce qui explique qu'elles soient si fortement combattues par nombre d'acteurs. On est aujourd'hui dans une situation où il y a usage, sans qu'il y ait forcément confiance.

— Comment se développe cette idée qu'on pourrait, en tant qu'individus, récupérer nos données et les exploiter nous-mêmes ? Y a-t-il une prise de conscience à ce sujet ?

— Nous travaillons clairement sur la question de la récupération des données, pour autant je ne suis pas du tout certain qu'on puisse parler de prise de conscience. En dehors de personnes très sensibilisées ou versées dans la technique qui pensent qu'elles

pourraient récupérer leurs données et s'en servir, on ne voit pas encore de mouvement de fond dans les enquêtes sur le sujet. On observe cette tendance chez certaines personnes qui sont plutôt des acteurs de l'Internet sensibles aux valeurs du web originel. On l'observe également dans d'autres domaines militants, comme les associations de patients qui demandent le retour des données personnelles de santé chez le patient, dans l'optique politico-sociale de rééquilibrer le pouvoir médical. Mais même sans parler de tendance de fond, il y a aujourd'hui une disponibilité à entendre ce discours s'il se traduit comme une amélioration de la vie quotidienne. Les gens ne voient pas encore forcément l'intérêt de se réapproprier leurs données, mais ils sont conscients que quelque chose ne va pas, qu'ils utilisent certains services sans être à l'aise, ce qui est problématique pour un développement économique sain.

Pour la majorité des gens, cette capacité à entendre un nouveau discours ne s'exprimera pas sous une forme de revendication du type « je veux me libérer, je veux reprendre le pouvoir ». Tout d'abord, la notion de données reste très abstraite : on voit bien ce qu'on peut savoir de nous, on a une idée assez juste de ce qu'est une donnée personnelle, mais quand on commence à réfléchir aux usages… Moi qui ne suis pas informaticien, est-ce que j'ai envie d'y consacrer du temps, de gérer ces données ? La plupart des gens ont le sentiment que c'est très abstrait, qu'il faut être calé, et que ça va être très compliqué. Ainsi, cette disposition à entendre de nouvelles propositions doit se traduire non pas sous un angle de contrôle mais sous l'angle d'une valeur positive pour les individus.

Cela interroge par ailleurs la notion de *privacy paradox* : les individus sont presque unanimes sur le fait que les plateformes captent trop de données, qu'ils se sentent surveillés, tout en continuant à fournir des données aux grandes plateformes. D'une part, cela indique qu'il n'y a pas beaucoup d'alternatives, d'autre part, c'est un signe fort que ces menaces ne sont pas prioritaires pour eux. Parmi les multiples sujets de votre vie, les multiples possibilités d'allocation de votre temps, de votre attention, vous allez accorder plus d'importance à ce qui vous permet d'accomplir ce qui a du sens pour vous plutôt qu'à vous protéger contre ce qui pourrait

avoir un potentiel impact négatif. Pour caricaturer, on apprend à conduire non pas pour boucler sa ceinture mais pour aller quelque part, et on boucle sa ceinture pour y arriver vivant. La question qui se pose aujourd'hui c'est : est-ce qu'on peut montrer aux gens qu'en leur redonnant l'accès et l'usage de leurs données, ils pourront faire des choses qu'ils ne pouvaient pas faire jusqu'ici ? Est-ce qu'en plus d'être bénéfique à leur vie privée, ça leur facilitera la vie ? Est-ce que ça réduira le taux de sollicitations inutiles ou polluantes, est-ce que ça évitera des décisions néfastes qui se prennent en totale opacité ? De mon point de vue, c'est bien dans ce sens-là que cela va se passer.

C'est pour cela que le terme « souveraineté » me paraît juste politiquement, mais pas adéquat du point de vue des individus. Je pense qu'ils ne se posent pas la question comme ça, à l'exception des militants. Pour ma part, je parle de capabilité : la capacité, pour un individu, dans la société dans laquelle il est, de se fixer ses propres buts et de se mettre en chemin pour les atteindre. L'enjeu, c'est d'être autonome au sens où je peux imaginer ce que, moi, individu, je voudrais accomplir. Autonome ne veut pas dire seul : je suis dans une société, je communique avec autrui, j'ai des possibilités et des contraintes mais à un moment je choisis d'accomplir telle ou telle chose, de mon propre chef. Et j'ai la possibilité de formuler cet objectif parce que j'ai l'espoir de réussir à me donner les moyens d'y arriver. On est ici dans la mise en capacité des individus, dans l'autonomie. Autonomie qui ne signifie pas « laissez-moi tranquille », mais bien plutôt : est-ce que je peux dire moi ce que je cherche ? Ce que je veux ? Ce que j'aime ? Et essayer de l'obtenir ? Est-ce que j'ai les outils et les communautés pour le faire, est-ce que je peux adhérer à des solutions auxquelles j'ai décidé d'adhérer en pleine connaissance de cause ? Au fond, les données personnelles sont aujourd'hui collectées et traitées par d'autres, et la seule possibilité qu'ont les individus, c'est d'avoir plus de contrôle sur ce que ces autres en font. Nous sommes toujours bloqués dans le paradigme qui consiste à éviter une non-valeur plutôt qu'à obtenir une valeur.

Les données pourraient devenir un outil dont les individus peuvent se servir pour mieux se connaître, mieux se projeter dans l'avenir, mieux se situer dans leur environnement, mieux partager avec d'autres – y compris avec des entreprises –, prendre des meilleures décisions et évaluer les résultats de ces décisions. Si ces données sont si utiles pour les entreprises dans un monde numérisé – et on veut bien le croire – il n'y a pas de raison qu'elles ne le soient pas pour les individus. Si on met l'accent sur l'utilité, il peut se passer quelque chose au niveau des individus.

— *Vous êtes porteur du courant du* self-data, *qui encourage la réappropriation des données personnelles par les individus. Comment procédez-vous ? Est-ce que ça fonctionne ?*

— Nous privilégions une approche qui va d'abord dans le sens de la création d'usages et qui essaiera ensuite de faire adhérer les gens. Vraisemblablement, c'est de cette façon que les gens adopteront ce nouveau paradigme, puisque dans la hiérarchie des préoccupations des individus, ce n'est jamais la technique qui arrive en premier.

Ça commence à fonctionner dans toute une série de domaines : le *quantified-self* en est un exemple. Les gens achètent et paient cher des objets dont la fonction est de capturer des données qui les concernent, et d'organiser ces données pour eux. On est ici dans le pur usage : ces données les intéressent parce qu'elles ont du sens vis-à-vis de ce qu'ils font et de ce qu'ils sont. On commence à trouver ainsi nombre d'applications concrètes. Nous avons mis en place le pilote *MesInfos* pour chercher ce genre de nouvelles applications : nous examinons les interactions entre de vrais consommateurs et de vraies enseignes comme la MAIF pour déterminer les usages possibles et tester en conditions réelles.

Il y a des exemples : une entreprise comme *digi.me*, qui agrège les données des individus sur l'ensemble de leurs réseaux sociaux, dit qu'elle a à peu près 300 000 utilisateurs. Le fait de pouvoir retrouver l'historique de leur tweet, de pouvoir naviguer dans le temps, par thème, entre tweets, Facebook, Instagram et autres pré-

sente donc un intérêt pour certaines personnes. Les agrégateurs de comptes bancaires font la même chose dans un domaine très précis, et il y a également une clientèle pour cela. Ces usages-là semblent rencontrer un vrai intérêt, et ils sont permis par la capture de nos propres données personnelles, qu'on fait sortir des grands silos des boîtes avec lesquelles on est en relation. C'est pour cela qu'on commence par réfléchir à la portabilité, à l'importation de données depuis des services que les individus utilisent déjà. Rapatrier ses données depuis les grands silos est la clef pour faire émerger des usages.

2

Sensibiliser : les difficultés de porter un discours sur la souveraineté

Sensibiliser les internautes

Rendre aux individus une autonomie et une souveraineté numériques ne va pas de soi : les solutions techniques peuvent être à disposition, mais encore faut-il que les utilisateurs souhaitent les utiliser ! La sensibilisation des internautes à l'importance de la souveraineté et de l'autonomie numériques est un thème pris en charge par de nombreuses associations sous diverses formes : conférences, ateliers de prise en main d'outils, publication de rapports, sensibilisation des acteurs politiques et des décideurs… Les arguments sont nombreux, connus, la situation a été mille fois traitée et analysée, et pourtant, rien ne semble fondamentalement bouger dans les pratiques quotidiennes des individus. Savoir, c'est bien, agir, c'est mieux ! Pourquoi est-il si difficile de sensibiliser à cette thématique ?

Faire changer les pratiques quotidiennes

Le discours sur la souveraineté numérique est difficile à porter pour plusieurs raisons. Il ne s'agit pas simplement d'expliquer un avis ou une position théorique : il s'agit de faire réfléchir sur des usages tellement quotidiens et tellement automatisés qu'on ne sait pas trop par où commencer l'explication. Le changement n'est pas évident : il ne suffit pas de cliquer sur un bouton pour passer d'un coup à une pratique saine d'Internet. On se heurte facilement aux arguments du « rien à cacher » ou « je m'en fiche », qui ne se déconstruisent pas en une minute. Si on s'attaque au sujet de la surveillance de masse, il est difficile de faire prendre conscience aux individus des effets d'une surveillance presque invisible. Plus généralement, l'habitude, la facilité d'utiliser les services des GAFAM et l'intangibilité des effets négatifs de ce modèle rendent la sensibilisation assez difficile. Le contexte politique n'est pas en reste : défendre le droit à la vie privée dans un contexte de surveillance liée au terrorisme rend parfois le discours difficile à entendre.

L'éducation numérique, un enjeu primordial

Pour faire évoluer les choses, on ne pourra faire l'économie d'une vraie éducation numérique, quels que soient les acteurs qui la prennent en charge. Découvrir Internet et plus généralement l'informatique par le prisme de quelques outils tend à les faire considérer comme les seules possibilités, et à renforcer leur centralité dans le paysage numérique. Une fois habitués, les internautes rencontrent nettement plus de difficultés à envisager un changement de modèle ou d'outils. Nous nous sommes entretenus avec Adrienne Charmet, présidente de La Quadrature du Net, pour en savoir plus.

ADRIENNE CHARMET

Porte-parole et coordinatrice de La Quadrature du Net depuis 2014. Militante des libertés numériques, elle a présidé Wikimedia France et travaille aujourd'hui à la sensibilisation de l'opinion publique française.

Sensibiliser est un sport de combat

— Avec la Quadrature du Net, vous faites un énorme travail de sensibilisation sur le thème du numérique. D'après vous, comment sensibiliser les individus à l'importance d'avoir le contrôle de ses données ou d'en faire ce qu'on veut ? Comment les sensibiliser à l'importance de sortir des silos, à la surveillance des États ?

— Réussir à sensibiliser, c'est vraiment un de nos gros défis : écrire et publier des analyses sur les raisons pour lesquelles on a besoin de maîtriser la conservation des données, les raisons pour lesquelles ce n'est pas bien de les stocker sur les serveurs de grosses sociétés dont le modèle économique est basé sur la publicité ciblée et donc sur la collecte de données personnelles, des analyses sur la surveillance des États, c'est assez simple, finalement. Expliquer le fonctionnement et expliquer pourquoi on a besoin de souveraineté individuelle et collective, expliquer pourquoi on a besoin de l'inscrire dans la loi, on sait très bien le faire. Mais la sensibilisation du grand public reste très difficile. Donc je vais répondre dans l'autre sens : pourquoi est-ce que c'est si difficile de sensibiliser ?

À mon sens, il y a deux raisons : d'une part, quand on parle de données et de surveillance, on parle de choses qu'on ne voit pas en tant qu'individu. Tout se passe sur nos connexions, et le processus est totalement invisible. Si on avait quelqu'un qui nous suivait

dans la rue, on se rendrait compte qu'on est surveillés, mais là on ne s'en rend pas compte parce qu'on est dans le domaine de l'immatériel. D'autre part, si c'est très difficile de sensibiliser le public, c'est aussi parce que les grosses plateformes étaient déjà là lorsque le grand public est arrivé en masse sur Internet, ainsi que le modèle économique basé sur l'exploitation des données personnelles. Le très grand public sur Internet, c'est le milieu des années 2000, et le milieu des années 2000 c'est Youtube, Facebook, Google… Il y a une partie de la population qui a connu Internet avant, mais finalement pas tant de monde que ça. Pour la plupart des gens, la situation actuelle est normale, en fait.

Il y a plein de gens pour qui Internet c'est Google, c'est Facebook ; ils ne vont pas sur Internet mais ils vont sur Google ou sur Facebook. Il faut désapprendre un certain nombre de choses, dont la centralisation, et c'est cela qui est très compliqué.

Le deuxième problème, c'est le double discours des entreprises et des États qui minimise complètement l'impact de la surveillance de masse par la collecte des données personnelles. L'impact que ça peut avoir sur notre vie privée, et par conséquent sur d'autres pans de notre vie, est complètement minimisé. Le fait d'avoir conscience, même de manière très impalpable, que ce qu'on fait, ce qu'on dit, ce qu'on pense sur Internet peut être lu et exploité, c'est rentré dans les mœurs. De toute façon si je n'ai rien à me reprocher, ce n'est pas grave, de toute façon, on ne s'intéresse pas à moi, je suis quelqu'un de trop petit pour intéresser… Du coup, il y a une forme de fatalisme qui se développe. Enfin, vu la manière dont l'Internet s'est concentré en silos de grosses plateformes hypercentralisées, reprendre la main de manière individuelle et collective sur nos données et sur notre vision d'Internet a un coût assez important.

Je pense que c'est pour ça que c'est aussi difficile de sensibiliser le plus grand public, et d'ailleurs on cherche encore la recette magique. Mais pour l'instant, quand on arrive à provoquer une prise de conscience chez les gens à qui on parle de ça, le saut pour sortir de cet écosystème est tellement élevé que finalement les gens ne le font pas. Et comme, en plus, ils ont pris conscience des problèmes,

ils culpabilisent. Donc on se retrouve avec une génération d'angoissés sur Internet. C'est pas génial : c'est bien d'avoir conscience des dangers, mais si on en reste au stade angoissé, on rend juste les gens malheureux.

— Vous qui travaillez régulièrement avec des acteurs étatiques ou au niveau européen, est-ce qu'il y a un blocage de leur côté ? Et si oui, est-ce qu'il y a quand même des instances qui vont dans le bon sens ? La souveraineté numérique au niveau français ou européen, c'est un sujet important aujourd'hui ?

— Alors, il y a deux sujets vraiment différents : la souveraineté à l'échelle individuelle sur ses propres données, et la souveraineté collective. Au niveau individuel, le problème qu'on rencontre aujourd'hui, c'est que la souveraineté individuelle rentre frontalement en conflit avec la sécurité. Quand on parle des libertés, on en parle la plupart du temps à propos des questions de terrorisme et de sécurité nationale. Globalement, nos interlocuteurs viennent du monde de la sécurité – ministère de l'intérieur, ministère de la défense – et là on est effectivement dans une opposition frontale avec eux. Au pire, ils ne reconnaissent pas l'atteinte à la vie privée. Ils ne veulent pas reconnaître le fait que cette atteinte massive à la vie privée par la légalisation de la surveillance est un danger pour la démocratie, parce que ça va à plus ou moins long terme assécher la créativité, la liberté d'expression et la liberté de penser. Au mieux, ils le reconnaissent, mais ils estiment qu'entre liberté et sécurité il vaut mieux choisir la sécurité. Et à partir de là, il n'y a pas de dialogue possible parce qu'ils considèrent que nous ne sommes pas légitimes à défendre ce point de vue face au risque terroriste.

— Quand vous dites « nous », c'est La Quadrature du Net ?

— La Quadrature et les autres associations. Il y a quand même des acteurs avec qui on partage certains points de vue : la CNIL en est un, même si on trouve souvent qu'ils ne vont pas assez loin.

Un certain nombre d'associations, d'ONG aussi. En tant qu'association, je trouve qu'on a assez bien réussi à sensibiliser d'autres acteurs dans le domaine des droits, c'est surtout au niveau étatique qu'il y a un blocage.

Ensuite, sur la souveraineté collective, on est dans un paysage beaucoup plus complexe. Il y a dans l'air un fantasme de souveraineté à la Russe, un fantasme qui fait voter l'existence d'un Haut Commissariat à la souveraineté numérique, un fantasme de système d'exploitation national. C'est complètement contradictoire avec les contrats que l'Éducation Nationale passe avec Microsoft. Il y a également un discours sur les grosses plateformes qui dit : « Google, Facebook et Twitter ne sont pas sympas, en plus ils ne nous aident pas dans la lutte contre le terrorisme ». Et dans le même temps, on leur impose des responsabilités énormes dans la lutte contre le terrorisme, et on leur demande de faire la censure eux-mêmes. On a des acteurs comme l'ANSSI ou ses équivalents au niveau européen qui disent « il est absolument indispensable de sécuriser les communications électroniques, de chiffrer » et des instances politiques ou judiciaires qui répondent « ah mais nous, le chiffrement ça nous empêche de travailler ». Un discours complètement contradictoire où on sent une volonté de se dégager du pouvoir des entreprises américaines, sans être prêts à accepter les conséquences de ce désengagement : promouvoir la sécurisation individuelle et collective de nos données, décentraliser Internet, travailler sur du logiciel libre.

Là-dessus arrivent des discours plus ou moins sincères et désintéressés d'acteurs qui semblent avoir un business derrière les questions de souveraineté et qui font un *lobbying* très actif. Certains promoteurs de la souveraineté numérique, très médiatisés, ont une vision d'Internet sur un mode russe ou chinois, vantant des systèmes d'exploitation ou de protection souverains auprès des décideurs politiques ou des services de défense et de sécurité, parfois à de hauts niveaux d'influence. Préoccupés (à juste titre) par les risques de cyberattaques et d'indépendance, ces acteurs peuvent adhérer à cette vision simpliste, sans comprendre que la souveraineté en mode bouclier est d'une part très nocive, complètement contraire

à l'esprit d'Internet, et d'autre part très fragile parce que la souveraineté ne peut être qu'une souveraineté résiliente, décentralisée, et qu'on a besoin de renforcer chaque maillon plutôt que de faire un bouclier en verre par-dessus.

Nous pensons vraiment que la souveraineté individuelle permet de renforcer chaque individu pour mieux renforcer la souveraineté collective, et qu'elle passe par la décentralisation, le chiffrement et le logiciel libre. Ce sont les trois clefs de la souveraineté numérique.

— Est-ce que l'association est la structure la plus pertinente pour mener une entreprise de sensibilisation ?

— L'avantage des associations, c'est qu'elles peuvent couvrir des champs très différents. Nous sommes face à deux questions : les usages et l'environnement politique. La Quadrature travaille plutôt sur l'environnement politique et législatif. Je pense que la forme associative est bonne, mais elle n'est pas du tout assez massive. Pour nous, la sensibilisation ne peut être efficace que si ce discours sur la souveraineté numérique devient majoritaire, y compris du point de vue des États.

On ne peut pas perpétuellement continuer à se battre contre les États sur ce sujet. Tant qu'ils n'auront pas compris l'intérêt de ce qu'on propose, on va rester dans une forme d'opposition qui est compliquée à défendre. C'est difficile d'avancer dans une période où les gens ont peur en se positionnant contre la politique antiterroriste du gouvernement. Les gens qui nous rejoignent sont souvent dans une posture d'opposition à ce discours sécuritaire, mais il y a sans doute plein de gens qui n'ont pas du tout envie d'être dans une posture d'opposition au gouvernement, et qui pour autant seraient tout à fait capables d'entendre ce qu'on a à dire. Par la force des choses, on se retrouve à avoir un discours complètement opposé au discours public, alors que nous avons les mêmes intérêts.

— Est-ce qu'on est dans la même situation au niveau français et au niveau européen ?

— De plus en plus, malheureusement. Une partie des questions de vie privée a été recouverte par les questions sécuritaires, ce qui n'était pas le cas avant. On a longtemps eu au niveau européen une attention très importante portée à la vie privée. Le règlement sur les données personnelles a été très largement débattu avec des parlementaires européens de tous les groupes. Mais ces derniers temps, la question sécuritaire revient au premier plan. Le parlement européen a fini par voter le PNR sous la pression des attentats de novembre en France.

En revanche, les recours juridiques qu'on a au niveau européen sont très intéressants. La CEDH et la Cour de justice de l'Union Européenne ont une jurisprudence traditionnellement plus favorable à la vie privée et notamment aux questions de données de connexion que la France. Le Conseil d'État en France, qui est l'instance contre laquelle on peut se retourner pour contester des lois, n'est pas du tout favorable à la vie privée. La Cour de Justice de l'Union Européenne est déjà beaucoup plus sensibilisée à l'impact sur les individus d'une collecte massive de données. Il ne faut pas idéaliser l'Europe, mais les parlementaires européens sont un peu moins sous la pression médiatique, et peuvent se permettre de porter des points de vue qui seraient plus difficiles à porter au niveau national.

Il y a également une masse de parlementaires qui viennent de pays dans lesquels les questions de libertés individuelle et collective sont très importantes. Les parlementaires du nord de l'Europe, par exemple, sont très sensibles à ces questions de libertés individuelles, et les pays de l'Est sont très sensibles aux questions de surveillance. On se retrouve parfois avec des députés très à droite, assimilables à l'extrême droite sur de nombreuses questions, mais à qui il ne faut surtout pas parler de surveillance, parce qu'ils ont vécu jusqu'à il y a un peu plus de 20 ans dans des pays où la surveillance était quotidienne et réelle. Les Allemands de l'Est, les Polonais ont bien conscience de l'impact de la surveillance sur

des individus et sur une société. Au parlement européen, ce n'est pas chez les parlementaires français que nous trouvons du soutien, mais chez des Allemands, les Néerlandais, les Suédois, plutôt qu'en Italie ou en Grande-Bretagne.

— Pensez-vous que l'éducation numérique soit centrale dans l'acquisition de la notion de souveraineté numérique ?

— Il y a une vraie mainmise des grandes entreprises sur l'éducation numérique et un gros manque de formation des enseignants. Si la moyenne d'âge des enseignants est entre 35 et 40 ans, ils n'ont jamais été formés aux questions numériques. Cette génération a découvert Internet à la fac. Les enseignants ont appris à donner des cours sans outil informatique. Les enfants sont habitués aux services des grandes entreprises : nos messageries sont chez Google, nos postes de travail sous Windows. Si on a eu du Microsoft au CDI de son école, qu'on a passé son B2I sur Word, qu'on a fait des exposés que sous Powerpoint, on ne connaît aucune autre alternative. La question de l'éducation est fondamentale, et c'est scandaleux de voir des écoles s'équiper d'iPads, de voir l'Éducation Nationale signer des contrats avec Microsoft. Outre le fait que ça coûte très cher, c'est comme si l'Éducation Nationale se mettait en partenariat avec MacDo pour les cantines. Il y a un vrai conditionnement, dès l'enfance, et ce n'est pas bon pour le futur. Un autre problème, c'est qu'on croit que des personnes qui sont nées en même temps que les ordinateurs seraient des *digital natives*. Ce n'est pas vrai. On ne maîtrise pas l'informatique parce qu'on a utilisé un ordinateur très tôt. On maîtrise les outils d'Internet. Aujourd'hui, les enfants de douze ou treize ans que je connais, y compris dans des familles sensibilisées à ce genre d'enjeux, ne comprennent pas quel était l'intérêt d'un ordinateur quand il n'y avait pas Internet. Et tant qu'on n'aura pas résolu ce problème d'éducation très inquiétant, on ne pourra pas résoudre la question de la souveraineté individuelle.

— Mais alors qui doit s'occuper de cette éducation numérique ? Le public, le privé ? Quel autre acteur que l'État ?

— Assez naturellement, on pourrait se dire que c'est à l'État de s'occuper de l'éducation numérique, ou en tout cas de donner l'impulsion. Mais la vraie question est dans la décentralisation : libre ou pas, il ne faut pas qu'il y ait un acteur trop central. Je crains beaucoup les nouveaux silos du libre. La question de la sécurité des données est presque accessoire. Utiliser Signal, ça se fait tout seul. La vraie difficulté, c'est la décentralisation. C'est très difficile de travailler à grande échelle et en décentralisant, dans la mesure où il faut renoncer à avoir un acteur qui gère tout. Si c'est l'État qui fournit un *cloud* personnel, mais qu'il vote une loi qui dit que pour des questions de sécurité nationale, il peut y avoir accès, on n'a pas avancé. L'information est toujours concentrée au même endroit.

Aujourd'hui, l'État peut facilement demander des informations sur nous parce qu'on a concentré nos données chez quelques acteurs. Alors que si le *cloud* est décentralisé, que les données sont chez quinze hébergeurs différents, l'un associatif, l'autre français, un autre européen… La surveillance devient très coûteuse. Décentralisation, et accessibilité des outils : si on n'arrive pas à faire des outils accessibles, on ne touchera pas le grand public, et si on n'est pas dans une lutte permanente contre la centralisation, on reproduira les mêmes problèmes.

Mais il ne faut pas se contenter de faire monter le coût de la surveillance pour la rendre impossible économiquement, il faut aussi lutter contre la surveillance en tant que telle, et contre ce modèle économique qui se base sur l'exploitation des données personnelles. Il ne faut pas laisser les lois être votées sans rien dire, en se disant qu'on va augmenter la résilience des individus. Il faut faire les deux en même temps. C'est cela qui est difficile, mais il ne faut pas renoncer. On ne peut sans doute pas se battre amendement par amendement, mais on peut documenter les lois, continuer à mettre le doigt sur ce qui ne va pas. Si on arrive à augmenter plus rapidement la résilience et les compétences sur la question de la souveraineté des individus, ils pourront contester ces lois plus tard.

3

L'accessibilité, pour un numérique inclusif

Développer un logiciel accessible, c'est développer un logiciel qui prend en compte les divers handicaps qui peuvent affecter une personne. Déficience visuelle ou auditive, dyslexie, ne doivent pas empêcher les personnes affectées d'avoir accès à des contenus numériques. D'autant que ces difficultés sont soumises à des variations liées au contexte : pris dans le métro avec une connexion quasi-inexistante, vous voilà en situation de handicap ! L'accessibilité d'un logiciel est une condition *sine qua non* à la souveraineté numérique des individus. Qu'il y ait des moyens pour reprendre le contrôle sur ses données est une bonne chose, mais si on ne peut ni les utiliser, ni accéder aux données en question, ni les exploiter à son bénéfice, peut-on encore parler d'une souveraineté numérique ?

L'accessibilité, en quoi ça consiste ?

Techniquement, l'accessibilité se décompose en deux parties : des dispositifs d'accès, et des systèmes intégrés aux plateformes et aux langages de développement capables d'améliorer l'accès et de délivrer les contenus aux personnes en situation de handi-

cap ; et des bonnes pratiques de développement s'appuyant sur ceux-ci. Si les premiers sont conçus et développés par des structures qui connaissent le sujet (fabricants de plage de lecture braille par exemple), ou qui s'attachent le talent d'experts du domaine (comme Apple et ses employés travaillant au développement de son lecteur d'écran maison, VoiceOver) et sont déjà utilisés par les concernés, c'est sur les développeurs des solutions utilisées par les utilisateurs finaux que repose la seconde partie. Elle consiste à rendre les logiciels et les produits compatibles avec ces systèmes, dans les aspects matériels ou logiciels de ce qu'on développe. L'accessibilité est un vaste sujet qui comprend une quantité gigantesque de littérature et de documentation, notamment en ce qui concerne le Web : des guides et des ressources sont disponibles, des communautés engagées sont prêtes à accompagner les bonnes volontés sur le sujet, et il existe des standards qui varient en fonction des langages. Le W3C, organisme qui promeut et organise les standards du Web, a écrit un référentiel sur l'accessibilité dès avril 1997 (le WCAG, *Web Content Accessibility Guidelines*). À première vue, tout semble donc couler de source.

Pourtant, l'accessibilité est loin d'être une évidence. Libres ou propriétaires, la plupart des logiciels ne suivent pas aujourd'hui toutes les recommandations d'accessibilité. Par économie, méconnaissance, ou parce que respecter ces recommandations nombreuses s'avère parfois être un casse-tête technique, la négliger est source d'inégalité. Mais le fait que la plupart des développeurs ou concepteurs d'outils numériques ne soient pas directement concernés rend l'automatisation de ces processus plus difficile : il faut régulièrement sensibiliser à l'importance de l'accessibilité pour être sûr qu'elle soit prise en compte. Enfin, l'accessibilité des contenus souffre également de l'évolution très rapide du numérique : un logiciel qui était parfaitement accessible peut considérablement régresser d'une version à l'autre pour peu que ses développeurs n'aient pas eu la formation nécessaire, ou que l'accessibilité ne soit plus une priorité de l'entreprise.

Un souci d'égalité dans un monde de plus en plus numérique

L'accessibilité numérique est un enjeu qui gagne chaque jour en importance. Démarches administratives, courses en ligne, réseaux sociaux, de larges pans de notre vie quotidienne passent par l'intermédiaire de nos appareils électroniques. Quand notre nomadisme numérique nous conduit de surcroît à nous positionner, utilisateurs valides, en situation de handicap (petits écrans, bruit ambiant, absence de réseau), il devient évident que l'effort à fournir pour rendre nos contenus accessibles n'est pas un « luxe » à réserver à une petite portion de la population, mais bien un levier essentiel pour l'accès à nos données personnelles.

ARMONY ALTINIER

Consultante et formatrice en accessibilité numérique. Elle a fondé l'association Liberté 0 qui promeut le numérique libre et ouvert à tous, et aide au développement de projets numériques inclusifs.

Du privilège à la liberté

— Pourquoi l'accessibilité est-elle un enjeu essentiel de l'autonomie numérique des individus ?

— L'accessibilité numérique, c'est permettre à tous les individus d'accéder aux contenus et aux fonctionnalités d'une interface numérique, quels que soient leurs moyens d'y accéder.

Quand on a des problèmes de mobilité, de communication ou de concentration par exemple, le monde physique est semé d'embûches qu'il peut être très difficile de surmonter : des escaliers, des portes trop étroites, des environnements bruyants, des contrastes insuffisants. C'est le quotidien de nombreuses personnes handicapées. Contrairement à des matériaux physiques, le numérique a une nature « fluide » qui permet d'adapter une même interface sous différentes formes afin de répondre aux besoins de la personne qui l'utilise. À cet égard, il apporte des solutions absolument formidables pour l'autonomie des personnes handicapées ! À condition que ce soit accessible…

Aujourd'hui, les frontières entre vie physique et vie numérique s'estompent. Il devient de plus en plus difficile de s'informer, travailler, communiquer, faire ses courses, étudier sans utiliser un ordinateur, une tablette ou un smartphone. Pour les personnes en situation de handicap, cette possibilité ne va pas de soi. Le débat sur le lien entre accessibilité, liberté et souveraineté est à l'origine parti

du logiciel libre, qui est un élément fort de la souveraineté numérique. Richard Stallman définit le logiciel libre par quatre libertés :

1. la liberté d'utilisation,
2. la liberté d'étudier le fonctionnement et d'accéder au code source,
3. la liberté de modifier le logiciel et
4. la liberté de partager ses modifications.

Si on a un handicap et qu'on ne peut pas utiliser un logiciel parce qu'il n'est pas accessible, s'agit-il toujours d'un logiciel libre ?

Cette première question a donné naissance à un mouvement en faveur de l'accessibilité dans le logiciel libre, notamment avec l'association Liberté 0 qui promeut le numérique libre et accessible. Ce mouvement repose sur la constatation suivante : si une liberté n'est pas valable pour tout le monde, ce n'est plus une liberté, c'est un privilège.

Pour une personne handicapée, le numérique est vraiment émancipateur. Quand on est aveugle aujourd'hui, avoir un iPhone facilite vraiment la vie : on peut scanner ses billets de banque pour savoir ce qu'on a comme argent sur soi, on peut prendre une photo du menu du restaurant et en avoir une version audio restituée, on peut utiliser son GPS pour être autonome dans ses déplacements, on peut travailler plus facilement, communiquer sur Internet, et tout cela grâce à l'accessibilité numérique. Les services rendus par le numérique ont été immenses, et ont permis l'inclusion de nombreuses personnes handicapées.

Évidemment, le numérique est utile à tout le monde, à tel point qu'on en devient presque dépendant. On ne se rend pas toujours compte qu'on y laisse une partie de soi-même et de sa capacité à faire les choses seul-e. Et quand on est handicapé-e, on laisse une partie de son autonomie dans une machine, ce qui est dangereux quand on ne maîtrise pas cette machine. Le jour où l'appareil ne prend plus en compte l'accessibilité, où le fabricant décide que l'accessibilité n'est plus importante pour lui, où le logiciel est retiré du marché parce qu'il n'est pas libre… les personnes handicapées

risquent de perdre leurs yeux, leur voix [1], leur travail, leurs moyens de communication.

L'accessibilité est donc un enjeu d'autonomie extrêmement fort et important pour les personnes handicapées.

Le numérique aujourd'hui, s'il ne respecte pas les normes d'accessibilité, empêche de travailler, de communiquer, de faire ses courses, il exclut les personnes handicapées d'une bonne partie des besoins de la vie quotidienne. Et c'est un problème réel : il arrive parfois que, d'une version à l'autre, on observe des régressions. Que ce soit dans le cas de l'iPhone ou dans le cas de Firefox !

C'est d'ailleurs l'un des éléments compliqués avec l'accessibilité numérique : contrairement au bâti par exemple, rien n'est acquis. Certes, c'est beaucoup moins cher et plus facile de prendre l'accessibilité en compte dans le monde numérique, mais c'est aussi plus facile à casser. Le bâti, ça peut être parfois très coûteux, ça peut impliquer de gros travaux, mais une fois qu'on a une rampe ou un ascenseur, c'est là pour de bon et ça ne bougera pas.

Au contraire, le numérique évolue très vite : pour reprendre l'exemple de Firefox, il y en a plusieurs versions par an, et il suffit que le développeur n'y ait pas pensé pour que les développements pour l'accessibilité sautent la fois d'après.

— Le logiciel libre est-il plus propice à intégrer ces normes d'accessibilité ?

— Pas plus qu'ailleurs. Le Libre rencontre une difficulté par rapport à des systèmes centralisés comme ceux que développent Apple. Apple maîtrise tout, du matériel au logiciel. Ils peuvent, s'ils le décident, faire en sorte que tout soit complètement accessible. C'était le cas quand il y avait Steve Jobs : il avait vraiment cette ambition, et les ordinateurs Apple étaient effectivement les plus accessibles. Les plus accessibles, mais les plus fermés. Et c'est parce que ce sont les plus fermés que ce sont les plus accessibles.

1. Voir l'article « La petite fille muette réduite au silence par Apple, les brevets, la loi et la concurrence » sur le Framablog : `https://framablog.org/2012/06/14/silence-maya/`.

Le problème, c'est que ce sont des logiciels propriétaires et commerciaux : maintenant qu'il n'y a plus Steve Jobs, ce n'est plus une priorité et on observe parfois de vraies régressions lors de changement de versions. C'est une forme de prison dorée : tant que ça marche, c'est parfait, mais il n'y a aucun moyen de faire pression ni d'influencer la prise de décision, on ne sait pas qui sont les développeurs ni comment les sensibiliser directement.

Le logiciel libre pose d'autres difficultés : la liberté, l'interopérabilité entre divers systèmes codés de manière très différente, ça rend l'accessibilité difficile à prendre en compte de manière unifiée. Il faut à chaque fois expliquer, sensibiliser, former, mais en général les gens sont plutôt ouverts au sujet. Et on a également des moyens d'agir quand ça ne fonctionne pas. On a résolu un bug de Firefox qui durait depuis des années en allant simplement voir le développeur chez Mozilla. Une semaine plus tard, c'était corrigé, alors que le bug était répertorié depuis très longtemps. Et on ne peut faire ça que dans le Libre, ce qui souligne bien l'importance d'être maître de ses données et de son matériel.

— Comment sensibilise-t-on à l'accessibilité numérique, que ce soit dans le monde du logiciel libre, dans le logiciel propriétaire ?

— Au niveau du logiciel libre, le discours sur les quatre libertés fonctionne bien en général, parce qu'il interroge sur la différence entre liberté et privilège. Les engagements du logiciel libre sur la liberté en font un discours assez facile à porter vers les communautés.

Quant au niveau global, il y a des lois sur l'accessibilité pour les personnes handicapées. La convention internationale relative au droit des personnes handicapées des Nations Unies parle d'accessibilité numérique, avec un système d'obligations que la France a ratifié. En France, la loi du 11 février 2005 parle d'accessibilité numérique dans son article 47. Dans la loi d'Axelle Lemaire pour une République numérique, l'article 44 porte sur une obligation d'accessibilité, avec des sanctions financières, pour rendre les contenus numériques globalement accessibles. C'est très axé sur le Web

parce que l'accessibilité web est un terrain bien connu : on a des normes, on sait faire de l'accessibilité web très facilement. C'est extrêmement bien documenté, le W3C a publié un standard, les WCAG (*Web Content Accessibility Guidelines*) qui est devenu une norme ISO. C'est la référence dans le monde et en Europe en particulier.

En France, il existe le référentiel général d'accessibilité pour les administrations (RGAA) qui est un référentiel de vérification de la conformité à WCAG. Il y a une vraie documentation, des ressources sous licence libre, et ensuite, c'est aux associations de se mobiliser. Elles commencent à le faire, mais elles ont parfois du mal avec le monde numérique en général, ce qui les empêche d'être aussi actives qu'elles devraient l'être.

L'un des problèmes, lorsqu'on parle d'accessibilité numérique, c'est que ça prend vite un tour assez technique. Le sujet peut être assez complexe quand on n'y connaît rien, et il est vrai qu'on ne peut pas leur demander d'être compétents sur tout, mais il faudrait que les associations montent globalement en compétences sur le numérique. Il faudrait se mobiliser sur deux axes à la fois :

1. sensibiliser les associations de handicap au numérique et au logiciel libre, aux questions de souveraineté, à la dépendance dont elles n'ont pas toujours conscience ;
2. sensibiliser les informaticiens à l'accessibilité numérique.

Pour un développeur web, ce n'est pas très compliqué à apprendre, l'accessibilité est le plus souvent incluse dans les bonnes pratiques du langage, ils en font donc parfois sans le savoir comme M. Jourdain faisait de la prose. Il est important de comprendre qu'il ne s'agit pas de développer des technologies pour les personnes handicapées, elles sont déjà équipées de technologies d'assistance. L'enjeu consiste seulement à rendre compatible les logiciels, contenus et interfaces avec ces technologies d'assistance pour qu'ils puissent interagir avec les équipements spécifiques, et il suffit la plupart du temps de respecter les standards du langage.

— Comment mettre en place des bonnes pratiques et à quel niveau doit-on travailler dans les solutions de reprise en main de nos données personnelles ?

— Implémenter de bonnes pratiques, c'est la clé pour que ça fonctionne : on n'a pas toujours besoin de recruter un expert, mais ce qui est vraiment essentiel c'est d'intégrer l'accessibilité dans son organisation.

Techniquement, ce n'est pas très compliqué, mais ça peut obliger à repenser sa façon de travailler et d'interagir avec les autres. Il faut également que ça procède d'une vraie volonté, et qu'on vérifie régulièrement que l'accessibilité est respectée. Ce que je préconise, c'est d'avoir dans l'organisation une volonté de la direction au sens large – ça peut être le board chez la TDF [*The Document Foundation*, fondation qui porte le projet LibreOffice], le conseil d'administration dans une association, le directeur ou la directrice dans une entreprise –, mais il importe qu'il y ait une lettre d'engagement sur ce sujet pour dire explicitement : « c'est une volonté que notre organisation soit accessible, nous devons le prendre en compte, ce n'est pas facultatif ». Ça n'a l'air de rien, mais c'est vraiment important de dire que c'est une priorité.

D'abord, il est plus facile de sensibiliser à une initiative issue d'une décision politique de l'organisation. J'ai déjà travaillé avec des gens du terrain qui étaient bloqués systématiquement soit par le *middle-management*, soit par la direction.

Ce n'est que par une décision stratégique que des actions opérationnelles vont pouvoir être mises en place de façon pérenne dans l'organisation : déblocage des budgets nécessaires pour former les employés par exemple, ou allocation de temps supplémentaire pour développer la partie accessibilité d'un projet. Il est dans tous les cas nécessaire d'avoir une personne référente dans la structure sur le sujet de l'accessibilité numérique.

Le référent ou la référente est une personne qui va faire (ou faire faire) des audits régulièrement, surtout quand ce sont des projets qui évoluent sur le long terme. Il est important de vérifier de temps en temps qu'on n'a pas régressé, parce que c'est ça le vrai danger :

les régressions quand on change de version. Si on a fait un gros travail, il suffit que le développeur ou la développeuse qui a été formé-e soit parti-e et que le nouveau ne sache pas à quoi sert tel ou tel attribut, il l'enlève et voilà, cela ne fonctionne plus. Cela arrive tous les jours, ce n'est pas de la mauvaise volonté de la part des gens, c'est juste qu'ils ne voient pas forcément sur le moment à quoi ça sert.

En résumé, il y a donc trois ingrédients :

— désigner une personne référente pour conserver un lien et sensibiliser aux bonnes pratiques ;
— un engagement de la direction ;
— faire un point régulier sur le niveau de prise en compte de l'accessibilité dans le projet.

Dans le cas de plus petites communautés ou de développements individuels bénévoles, c'est un peu différent. Il ne faut pas tout attendre des autres, il faut s'autoformer, il y a beaucoup de documentation qui existe, donc RTFM quoi :-) Maintenant, avec le portail RGAA [1], il y a des ressources, des guides, des modèles de documents… le tout sous licence libre. C'est aussi une question d'engagement personnel.

1. Voir le *Référentiel Général d'Accessibilité des Administrations*, à l'adresse `http://references.modernisation.gouv.fr/rgaa-accessibilite/`.

4

La souveraineté numérique et l'État

Souveraineté et État de droit

La souveraineté numérique n'est pas seulement un enjeu individuel : elle intéresse également les États souverains, qui maîtrisent le territoire national sans toujours maîtriser le territoire numérique. Documents confidentiels qui transitent par Google, impossibilité d'avoir prise sur les informations stockées à l'étranger sur des serveurs hors de contrôle, loi qui s'applique différemment en fonction du lieu de stockage des informations… Les tentatives d'instaurer un système d'exploitation ou un *cloud* souverains se sont soldées par des échecs, preuve de la difficulté pour l'État français de s'adapter à un monde numérique en plein changement. Preuve également que les réponses à apporter aux questions numériques dépassent probablement les frontières : la France a-t-elle vraiment vocation à gérer seule l'espace numérique français ? N'est-ce pas à l'Europe de faire contrepoids aux géants américains et chinois ?

De nombreux discours étatiques sur le numérique

Le rapport de l'État au numérique n'est ni simple, ni univoque. Entre les différents ministères et secrétariats, entre les différentes agences gouvernementales, il y a négociations et débats récurrents. Le chiffrement, le système d'exploitation souverain, le respect absolu du droit à la vie privée en sont des exemples. Pris entre des impératifs de sécurité, le respect des libertés des citoyens, la nécessité de s'adapter à l'écosystème numérique actuel, les différents acteurs de l'État n'ont pas toujours des positions cohérentes.

Pourtant, la souveraineté numérique n'est pas une option. D'une part, les États ne peuvent pas se permettre de laisser circuler des documents sensibles par le biais de services sur lesquels ils n'ont aucun pouvoir, et ne peuvent pas négliger leur rôle de protecteur des citoyens. D'autre part, les grands acteurs d'Internet commencent à remplacer de manière inquiétante certains services publics (le *Safety Check* de Facebook en est un exemple flagrant : souhaitons-nous laisser à une entreprise la responsabilité de gérer ce type de crises ?). Enfin, peut-on envisager une souveraineté individuelle sans une souveraineté étatique, au moins partielle ? L'État est la structure à laquelle les individus doivent pouvoir s'adresser pour faire respecter leurs droits numériques (droit à l'oubli, droit à la portabilité).

Entendons-nous bien : il ne s'agit pas de remplacer la centralisation des grands acteurs du net par une centralité d'État. Nous ne faisons pas tous aveuglément confiance à l'État, et la majorité d'entre nous n'a sans doute pas envie de lui laisser la mainmise sur ses données personnelles. Cela dit, on peut estimer qu'il est du rôle de l'État d'encourager la souveraineté et l'autonomie numériques des individus, de promouvoir des alternatives, et surtout des alternatives libres et transparentes. On s'inquiéterait à juste titre d'une mainmise de l'État sur le numérique, et elle n'est pas souhaitable. Pour autant, l'État peut avoir un rôle incitatif intéressant et faciliter l'émergence d'alternatives respectueuses de la vie privée des citoyens.

Ce chapitre nous a donné l'occasion de présenter deux points de vue complémentaires d'acteurs gouvernementaux ou proches

de l'État. Tout d'abord, nous nous sommes entretenus avec Isabelle Falque-Pierrotin, présidente de la CNIL et conseillère d'État, qui nous a présenté sa vision du paysage numérique contemporain et de ses perspectives. Nous avons également rencontré Charles Schulz, fondateur de l'*Open Document Foundation*, qui nous a parlé spécifiquement de la souveraineté numérique de l'État.

ISABELLE FALQUE-PIERROTIN

Conseillère d'État et présidente de la CNIL depuis 2011. Elle est également présidente du G29, organisme qui regroupe les autorités de protection des données de l'Union Européenne, depuis 2014.

Remettre les géants au pas

— Comment se pose aujourd'hui la question de la souveraineté numérique face à de grands acteurs comme Google, Apple, Facebook, Amazon ou Microsoft ?

— La question de la souveraineté numérique au regard des données se pose de deux manières. D'une part au niveau micro : c'est-à-dire au niveau de l'individu ; les individus ont le sentiment de perdre une maîtrise individuelle, une forme de souveraineté individuelle sur leurs données face à un écosystème numérique de plus en plus complexe, voire confus pour eux. Toutes les études mettent en évidence cette espèce de malaise, de gêne par rapport à cette perte de maîtrise. D'autre part, la question de la souveraineté numérique se pose aussi sur un plan macro, puisque la géographie actuelle des données est une géographie dans laquelle les données sont principalement collectées en Europe, exportées aux États-Unis et traitées par des acteurs américains, voire des acteurs chinois. En tout cas, peu traitées par des acteurs européens. Il y a donc là aussi une perte de souveraineté collective de l'Europe sur son territoire par rapport à ses propres données. Comment est-ce qu'on résout ce problème-là ? Comment est-ce qu'on se comporte vis-à-vis des grands acteurs de l'Internet, les GAFA, qui illustrent les deux pertes de souveraineté, à la fois individuelle et territoriale ?

Jusqu'à présent, les CNIL étaient relativement handicapées vis-à-vis d'eux, parce que leur offre est largement une boîte noire :

on s'en rend compte lorsqu'on commence à discuter de la politique de vie privée de Google, de Facebook, et qu'on voit bien que ces politiques reposent sur une combinaison de données la plus large possible – on l'a encore vu récemment avec Whatsapp. Cette combinaison de données, justement, illustre la perte de maîtrise par l'individu de ses données, parce que dans le fond, dès qu'un individu rentre dans un écosystème, les données dudit individu sont partagées de façon transversale à l'intérieur de l'écosystème de Facebook, de Google etc. sans qu'on lui demande quoi que ce soit. Ces acteurs nous disaient : « nous on est américains, on est chinois, le droit européen ne nous est pas applicable. » Aujourd'hui, une partie de la négociation consiste à leur faire admettre que, s'ils viennent prester en Europe, ils doivent respecter les règles européennes. Cela implique par exemple de donner la possibilité à l'individu de choisir s'il souhaite ou non combiner ses données. Demain, avec le réglement européen qui a été adopté en mai 2016 et qui sera pleinement applicable en 2018, on entre dans un nouveau cadre juridique européen, une loi européenne commune. L'énorme avantage de ce nouveau cadre, c'est qu'il remet les acteurs européens à égalité de concurrence avec ces acteurs mondiaux, parce qu'il soumet ces acteurs mondiaux au droit européen dès lors qu'ils offrent un produit ou un service à destination d'un Européen. Donc, demain, il ne s'agit plus de savoir si les critères actuels – établissement en Europe, moyens de traitement en Europe, des critères juridiques assez sophistiqués – sont respectés. Dès lors qu'un acteur international, même s'il n'est pas établi en Europe, offre un bien ou un service numérique à destination d'un consommateur ou d'un citoyen européen, le droit européen lui est applicable et on est légitimement en droit de demander à ces acteurs le respect des droits des personnes : consentement, portabilité, etc. On récupère ainsi une souveraineté européenne sur ces grands acteurs mondiaux qui est considérable. Je suis absolument convaincue d'une chose, c'est qu'il n'y aura de souveraineté numérique qu'européenne. Bien sûr, la France peut dire « moi je veux mes données en France » ; je n'y crois qu'à moitié. Je crois qu'il est absolument nécessaire, dans cet univers numérique, que l'Europe puisse

parler d'une seule voix, que ce soit vraiment le continent, le marché européen des 500 millions de consommateurs qui puisse être pris en compte. Le fait de coordonner les régulateurs européens et la possibilité d'avoir un front uni par rapport à ces grands acteurs mondiaux sont absolument décisifs si on veut être crédible.

Le deuxième aspect, c'est la nécessité de redonner à l'individu une capacité de maîtrise individuelle de cet écosystème numérique. Là encore c'est l'orientation du réglement qui met véritablement l'individu au centre du numérique : il lui confère des droits renforcés en termes de consentement, de nouveaux droits, comme le droit à la portabilité. Ce droit à la portabilité est essentiel : il donne la possibilité à l'individu d'être indépendant de la plate-forme auprès de laquelle, normalement, il consomme ses services, et de dire : « je change de fournisseur ; je récupère les données qui sont les miennes sur cette plate-forme et je vais les utiliser ailleurs ». En termes d'autonomie individuelle, c'est très intéressant. Et ce besoin de maîtrise individuelle, ce n'est pas juste une vue de l'esprit. Le droit à l'oubli nous en a donné une belle illustration : à l'issue de la décision du juge européen, il y a 300 000 ou 400 000 Européens qui ont fait des demandes de déréférencement. C'est l'expression du fait que les personnes veulent maîtriser leur vie en ligne, qu'ils veulent pouvoir limiter dans le temps l'effet d'un contenu et donc ciseler leur vie numérique en fonction de leurs propres caractéristiques, de leurs propres objectifs, notamment quand on cherche un travail. Je trouve que c'est intéressant, parce que ça montre bien que cette appétence des individus à maîtriser leur vie numérique est réelle, et le règlement y répond. Et là aussi, je crois qu'on récupère de la souveraineté individuelle, c'est-à-dire de la capacité de choix et d'autonomie au niveau de l'individu.

Donc, que ce soit au niveau collectif ou individuel, le règlement européen est à mon avis une étape absolument décisive de cette réflexion sur la souveraineté numérique. Il permet à l'Europe de remonter dans le train, de prendre sa place dans le numérique, parce qu'il faut bien dire qu'on a quand même un peu perdu pied face aux grands acteurs internationaux. Aujourd'hui on dit « on a un

marché » : c'est bien, mais ça ne suffit pas. Il faut aussi des acteurs, et pour avoir des acteurs, il faut avoir une offre. Avec ce cadre juridique rénové, nos acteurs européens peuvent se battre à égalité de concurrence avec les acteurs mondiaux. Il faut qu'ils se saisissent de ce cadre juridique rénové.

Cette réglementation leur offre un outil de différenciation qui est un outil extrêmement précieux qui correspond justement aux attentes des gens. Les gens ne vont pas se détourner de la société numérique, nous allons tous continuer à utiliser, à consommer ces services. En revanche, il y a une maturité croissante des individus à ce sujet. Configurer l'utilisation de nos services, gérer les paramètres de confidentialité, c'est devenu assez banal. Les profils Facebook sont aujourd'hui largement fermés alors qu'il y a cinq ou six ans, les profils étaient publics, entièrement ouverts ! On voit bien qu'il y a une courbe d'apprentissage et que les gens aujourd'hui sont très heureux de profiter des bénéfices de cette société numérique, mais en fixant eux-mêmes les balises de l'utilisation de leurs données. Le règlement arrive à point nommé, exactement pour faire écho à cela, et au plan plus général, pour remettre les acteurs professionnels à égalité de concurrence avec les acteurs internationaux.

— Pensez-vous qu'il soit souhaitable de mettre en place une éducation numérique commune au niveau européen qui permette aux gens de se saisir de ces questions de souveraineté numérique et pas simplement de subir ces pratiques ?

— Je pense que l'éducation numérique est effectivement un objectif public absolument central. Il faut que nous soyons collectivement capables de passer à l'échelle, c'est-à-dire pouvoir profiter de tous les bienfaits de l'univers numérique mais en même temps d'en maîtriser les éventuels effets négatifs – en tous cas de savoir à quelles conditions on va dans cet univers. À la CNIL, nous avons lancé depuis déjà pas mal de temps un collectif sur l'éducation numérique pour essayer de faire prendre conscience de l'importance de cet enjeu. Jusqu'à une période encore récente, on éduquait

d'abord aux risques et aux dangers du numérique. Alors que ce n'est pas la question centrale ! C'est comme si on apprenait les feux rouges à un enfant sans lui apprendre à se promener dans la rue. Ça n'a pas de sens. Je crois que c'est un univers nouveau avec des codes, des modes de fonctionnement, des potentialités radicalement nouvelles et ça, effectivement, il faut en faire l'apprentissage. Au niveau français, on a lancé il y a quatre ans ce collectif pour l'éducation numérique et il fait tache d'huile. C'est-à-dire qu'au plan international, au sein de la conférence mondiale des autorités de protection des données, la CNIL et le Canada ont animé un groupe de travail depuis trois ans qui est le seul groupe de travail de la conférence mondiale qui soit aussi actif. Et ce que nous avons produit (et qui sera dévoilé à la conférence de Marrakech au mois d'octobre) c'est un référentiel de compétences pour les professeurs. Nous pensons que l'éducation numérique doit entrer dans les programmes scolaires, et pas par la petite porte : il faut que les ministères de l'éducation dans chacun des pays se dotent d'une manière ou d'une autre d'un programme d'éducation à la société numérique. Ce référentiel nous permet de définir de manière très concrète ce qu'il faut que les individus sachent pour être capables d'être des citoyens numériques éclairés. Les compétences sont expliquées d'une façon extrêmement simple. Ce que nous souhaitons, c'est que ce référentiel soit adopté à la conférence de Marrakech et qu'il devienne un référentiel mondial, pour que tous les ministères dans tous les pays puissent s'en servir comme base pour dire à leur propre administration : « Voilà le programme d'éducation numérique que l'on doit faire ». Et ça, c'est fabuleux ! Je crois vraiment que cela nous aidera considérablement. Il s'agit de répondre à des questions très simples du type : « Qu'est ce que je dois comprendre dans la liberté d'expression ? », « Est-ce que je suis capable de configurer mon ordinateur/application pour faire ceci ou cela ». Ça mêle à la fois des concepts et des conseils prosaïques pour interagir les uns avec les autres.

— Comment travaillez-vous avec vos homologues européens ?

— Avec nos homologues européens, nous sommes membres du G29, le réseau des « CNIL » européennes dont j'assure la présidence. Il se réunit tous les deux mois, et il produit régulièrement des recommandations, des *guidelines*, etc. Nous sommes actuellement dans une période très particulière : le G29 doit, en l'espace de 18 mois, être capable de passer de ce règlement européen qui vient d'être adopté, qui est une sorte de monument textuel – plus d'une centaine de pages, d'articles très sophistiqués, pleins de compromis – à un document opérationnel pour mai 2018. Un document opérationnel, cela veut dire « Quelles sont les règles précises de désignation d'un *DPO* (Data Protection Officer) ? Est-ce que le *DPO* européen, c'est celui du *headquarters* ?» Nous devons fournir des réponses à des questions extrêmement concrètes.

Personnellement, j'ai souhaité que ces *guidelines* puissent être produites par les autorités européennes, bien sûr, mais à partir d'un retour de terrain substantiel. Nous avons mis en place un système de *fab-lab* qu'on a lancé au mois de juillet. Avant le mois de juillet, nous avions défini un plan d'action pour 2016 avec des sujets prioritaires, et nous avions fait venir à notre *fab-lab* de juillet des représentants de tous les secteurs économiques concernés et de la société civile pour les faire travailler sur ces sujets. Nous voulions comprendre quelles étaient leurs questions et propositions sur ces priorités et, à partir de là, travailler sur un matériau qui va nous permettre de finaliser les premières *guidelines* pour 2016. Et au fur et à mesure que nous travaillons les différents sujets, nous mettons en place un *fab-lab* qui nous permet de faire de la co-construction multi-acteurs avec les acteurs concernés. C'est très intéressant, parce qu'on est au plus proche du terrain : cela évite que les autorités de protection moulinent dans le vide. C'est d'ailleurs la première fois que les acteurs eux-mêmes se rencontrent de façon aussi précise sur un sujet. Les fédérations professionnelles font du lobbying, la société civile fait du lobbying à sa façon. Mais le fait de les faire travailler ensemble sur le même sujet, et que ce sujet ne soit pas une réflexion générale sur les cadres juridiques euro-

péens mais un ensemble de sujets très précis, est très enrichissant pour tout le monde. Pour vous donner l'exemple du *DPO* : quel doit être son positionnement dans l'entreprise ? Quels doivent être ses pouvoirs ? Ou encore sur le thème de la portabilité, comment voient-ils ce droit ? Les faire travailler ensemble sur les mêmes sujets est très utile et les regards croisés donnent des résultats très intéressants.

— Vous parliez de concertation entre acteurs : vous qui travaillez en étroite collaboration avec l'État, comment est-ce que vous gérez ce contexte assez tendu entre l'ANSSI et la CNIL qui vont défendre le chiffrement et le droit à la vie privée, et le Ministère de l'Intérieur qui ne sera pas du même avis… Est-ce que vous avez l'impression d'être écoutés ?

— Écoutés, oui. Suivis, pas toujours. Bien sûr, nous avons des positionnements et des missions qui ne sont pas les mêmes, et sur les lois renseignement par exemple, nous avons défendu une position qui n'était pas celle du ministère de l'Intérieur, notamment sur la question du contrôle des fichiers alimentés par les nouvelles techniques de collecte que permettaient la loi Renseignement, les *IMSI catchers*, les boîtes noires etc. Les lois récentes sur le renseignement ont donné de nouveaux moyens d'action aux services de renseignements. Ce que nous avons dit, c'est que ces nouveaux moyens d'actions – qui sont en fait de nouvelles données – alimentent les fichiers de renseignement. Et ces fichiers de renseignement ne sont contrôlés par personne. Nous les connaissons au moment de leur création, mais dans des conditions assez imprécises, parce qu'ils bénéficient d'une dérogation et, par conséquent, les documents qu'on reçoit sont très limités. La transparence – et c'est compréhensible – au moment de la création est beaucoup plus réduite par rapport à d'autres fichiers publics. Voilà ce que je dis depuis longtemps déjà aux ministres de l'Intérieur successifs, à la suite des révélations de monsieur Snowden : je pense qu'on entre dans un univers nouveau qui se caractérise par une crise de confiance généralisée de la part des individus vis-à-vis de cette sphère numérique. Par rapport aux pouvoirs publics, la crainte que

nous avons, c'est que cette méfiance s'installe. Et de mon point de vue, il est temps qu'on puisse mettre en place un contrôle de ces fichiers de souveraineté, dans des conditions qui peuvent être *ad hoc* bien entendu. On ne va évidemment pas contrôler les fichiers de la DGSI comme on contrôle un fichier de police. Et nous nous sommes préparés à cette éventualité : nous sommes parfaitement capables à la CNIL de monter un dispositif de contrôle qui soit spécifique et *ad hoc* pour des fichiers de ce type. J'ai dit à Manuel Valls et Bernard Cazeneuve que c'était une garantie démocratique, qu'il était absolument nécessaire de faire cela au moment de la loi Renseignement. On donne plus de pouvoir aux services de renseignement, plus de modalités d'intervention, il faut naturellement qu'il y ait plus de contrôles. C'est un exemple typique de différence de positionnement. Ensuite, des choix politiques sont faits. L'arbitrage nous a été rendu, et ça n'a pas été mis en place. Sur le chiffrement, la position de la CNIL est nuancée : nous nous sommes favorables au chiffrement, et pas seulement parce que cela protège la vie privée, mais parce que le chiffrement est le moyen privilégié d'assurer la sécurité de l'écosystème numérique. Et nous, notre mission, c'est aussi d'assurer la sécurité des données de toutes sortes, et pas seulement des données personnelles. L'univers numérique dans lequel nous évoluons est bâti de bric et de broc : quand vous êtes utilisateur d'une appli, ou consommateur d'un service, il y a en fait une multitude d'autres acteurs derrière qui interagissent les uns avec les autres dans des conditions qui sont assez obscures. Si vous fragilisez un maillon de la chaîne en interdisant le chiffrement, c'est l'ensemble de celle-ci qui est désorganisée et ça peut revenir en boomerang d'une façon totalement non maîtrisée. C'est pourquoi nous pensons que les technologies de chiffrement sont indispensables aujourd'hui, vu la complexité de cet univers numérique.

Ce sujet de la sécurité est central ! L'année passée, une faille de sécurité majeure a été rendue publique presque chaque mois. Nous avons certes une position qui est distincte de celle des pouvoirs publics sur le chiffrement, pour autant je crois que, dans notre position, nous souscrivons à l'objectif d'intérêt général qui est d'as-

surer la sécurité globale des systèmes. La CNIL a un statut très particulier : nous sommes au sein de l'État, mais nous travaillons aussi avec les acteurs économiques concernés. Entre régulateurs et acteurs économiques, les intérêts sont liés. De fait, la crise de confiance actuelle porte préjudice aux libertés mais aussi considérablement aux acteurs économiques. Si nous ne résolvons pas cette crise, la société numérique va se ralentir. Il est impératif, il est critique qu'acteurs public et privés soient capables de travailler ensemble, de se doter des moyens pour que cet univers numérique continue à se développer et à innover – il apporte de la croissance, des potentialités fabuleuses – mais dans le respect du droit des personnes. On entend parfois des gens opposer innovation et protection des données mais il ne faut pas les opposer. La protection des données est un moyen de construire une innovation qui soit plus durable, parce que comprise, enracinée dans un marché. L'innovation qui fait peur, qui n'est pas comprise, qui méconnaît toutes les libertés, elle ne fonctionne pas. Regardez ce qu'il s'est passé avec les Google Glass. Il y a deux ans, lorsque Google a lancé ses lunettes sans réfléchir à la manière dont ça allait être reçu, ils ont subi un rejet majeur des premières expérimentations parce que les gens étaient paniqués, à raison, de cette intrusion dans leur vie quotidienne.

La CNIL est à un point nodal d'interaction entre acteurs économiques et sociétés civiles, pour construire ensemble cet univers numérique. Inquiétude ou résignation ? Nous observons une très forte augmentation de nos plaintes. L'année dernière, il y en avait eu 6 000, cette année, c'est 8 000. Globalement, on sent que la population française est beaucoup plus vigilante sur le respect de ses droits, la gestion de son e-réputation. Est-ce qu'elle est inquiète, est-ce qu'elle est vigilante, ça je ne saurais pas le dire. En tout cas, nos concitoyens ont de plus en plus conscience que cet univers numérique tourne à partir de leurs données, mais qu'ils ont tout de même des droits sur ces données. J'aurais tendance à distinguer le public et le privé, parce qu'on est un peu à front renversé par rapport à 1978. Vis-à-vis du privé, il y a une volonté d'être bien certain que le banquier ou l'assureur utilisent les données comme ils

doivent les utiliser et qu'encore une fois, c'est bien moi, individu, qui suis aux commandes de tout ça. Pas une inquiétude donc, mais une volonté de maîtrise. Du côté du public, notamment dans le contexte de sécurité nationale, ce qui nous remonte c'est l'idée que c'est légitime, que si on n'a rien à cacher après tout, c'est normal qu'on se défende contre le terrorisme.

— Est-ce que vous pensez qu'il y a des initiatives à favoriser en plus de l'éducation numérique ?

De notre point de vue, la protection des données est un atout concurrentiel. Ce n'est pas simplement une contrainte qui est imposée par l'État, c'est aussi un argument vis-à-vis des consommateurs pour les inciter à choisir un produit, parce que leurs données seront respectées, parce que la relation de confiance qu'ils vont nouer sera de meilleure qualité, parce qu'ils seront mieux traités. Et ça a énormément de prix : les données sont un élément clef pour garder son client. Ce positionnement commence à faire école, et au niveau des start-ups – dans l'Internet des objets par exemple –, on sent bien que l'utilisation des données personnelles comme argument de vente commence à monter en puissance. Notre posture, c'est d'inciter à des offres alternatives, des offres qui soient plus frugales sur les données, qui fassent de la *privacy by design*, qui proposent un service différent. Dire « les données sont un élément de la confiance et on peut les traiter différemment des GAFAM », c'est prêcher dans le désert si vous n'avez personne qui offre un service de cette nature. Il est donc très important que se matérialisent des offres de ce type. Et effectivement, il faut que les pouvoirs publics puissent inciter ou au moins promouvoir des offres de cette nature. Dans le projet de loi sur la République numérique, on a aussi introduit une responsabilité d'assurer la promotion des technologies de chiffrement. La réponse est donc bien entendu juridique, mais aussi technique et commerciale. Si l'on veut piloter l'univers numérique d'une façon à la fois dynamique et respectueuse des données, il faut mobiliser les différents outils qui s'offrent à nous. Ce n'est pas simplement la réglementation qui changera la donne :

la réglementation offre un cadre, une opportunité dont les acteurs doivent se saisir et qui doit les encourager à développer des produits différents : européens, *privacy by design*. Aujourd'hui, il y a tout ce qu'il faut pour que ces fleurs-là éclosent.

— La dernière mission de la CNIL : anticiper. Comment percevez-vous les perspectives de changement à moyen terme ?

Je trouve les offres alternatives encore modestes. Le temps presse, et si on veut avoir des champions européens c'est maintenant qu'il faut se lancer, pas dans cinq ans. Je pense qu'il ne faut pas tarder.

CHARLES SCHULZ

Co-fondateur et ancien président de *The Document Foundation*, qui coordonne le projet LibreOffice.

Réguler pour mieux régner

— Qu'est-ce que la souveraineté numérique des individus implique pour l'État ?

— La souveraineté des individus ne peut être totalement distincte de la souveraineté d'un État. La souveraineté d'un individu ou des individus par rapport à l'État dans lequel ils vivent existe, mais de manière différente. Un État peut, et doit, entretenir une armée, une force de police, des infrastructures de base. S'il ne le fait pas, il n'existe pas vraiment en tant que tel, ou pour mieux dire, il n'est pas souverain. La souveraineté d'un individu, à partir de ce constat veut dire deux choses : un individu reste maître et en contrôle de son devenir, responsable et libre de ses choix. Il est aussi capable de transférer une partie de sa souveraineté à un État. Si un ou des individus sont souverains sans un État, on s'aperçoit bien vite qu'ils doivent s'organiser pour se défendre, subsister, survivre. Autrement dit, l'organisation implique une délégation, un partage de la souveraineté. Il n'est pas certain d'ailleurs qu'un être humain puisse survivre absolument *ex nihilo* : c'est un délire rousseauiste, et il ne sert qu'à bâtir des pensées politiques reposant sur une hypothèse de départ fausse.

Il existe une tradition européenne, qui n'est pas forcément la tradition française, qui privilégie l'analyse des rapports fondamentaux entre l'État et l'individu. Cette analyse tente de dépasser le cadre du droit ou des droits, de la forme de gouvernement, de la

culture, de la religion, etc. Quelle est la thèse issue de cette tradition ? Un État peut exiger l'obéissance ou du moins la conformité avec les normes édictées (encore une fois, la question n'est pas de connaître la forme de gouvernement) à partir du moment où il a les moyens effectifs de protéger l'individu. Cela se vérifie au travers des âges et des régimes. Le paysan peut à tout moment entrer derrière les lourdes murailles du château en cas d'invasion, de guerre ou de brigandages. Mais il doit à son seigneur des corvées, des impôts en nature ou en monnaie, et il lui doit l'hommage. Mais si le seigneur n'a pas de château, s'il ne peut même pas lui fournir des armes et envoyer une troupe de ses gens pour le défendre, alors en réalité le lien de dépendance féodal n'est que théorique, quand il n'est pas automatiquement juridiquement rompu.

Dans un État moderne, l'individu paye ses impôts, il se plie aux lois, démocratiquement votées ou pas, et en retour, il bénéficie d'infrastructures, de la police, de l'armée, de l'hôpital. Si aucun de ces services n'existe, il y a fort à parier que l'individu n'a personne à qui payer ses impôts ; mais il devra au minimum s'acquitter d'une somme pour sa protection physique à un chef de guerre local.

Cette tradition issue de penseurs du droit germanique a le mérite de mettre en lumière ce point de rencontre entre la souveraineté de l'individu et celle de l'État. Il s'agit donc d'une relation d'interdépendance, quelle que soit la souveraineté réelle des individus. Cette interdépendance se vérifie aussi dans le champ numérique.

Sur le plan numérique, ces principes se traduisent à la fois par le besoin de l'État d'exercer les prérogatives qui lui sont propres (la loi existe aussi sur Internet, la confiance est nécessaire au commerce, la liberté d'expression doit être garantie…) mais aussi par la capacité de l'État à aider ses citoyens à accéder au numérique. L'État peut en effet financer les infrastructures réseau à l'échelle de son territoire, et il fixe aussi le cadre juridique approprié pour les échanges sur Internet.

On peut également souhaiter que l'État puisse permettre à ses citoyens et à ses entreprises d'aller plus loin, en facilitant l'accès à des outils ou en définissant un cadre normatif favorable au dé-

veloppement d'un réseau qui facilite l'éducation, les échanges, la culture, le commerce…

En réalité, il est assez facile de voir que bien des missions classiques de l'État ont une traduction numérique. La difficulté est que le numérique est un champ immatériel – réel mais immatériel – ce qui rend leur application parfois complexe et délicate, voire improductive dans certains cas.

— Que penser d'une souveraineté numérique nationale ?

— La souveraineté numérique nationale est de prime abord la déclinaison de la souveraineté nationale au domaine numérique. Cela semble simple, voire simpliste. Ça ne l'est pas. Il existe une grille de lecture qui oppose la souveraineté numérique nationale à celle des individus. Nous y reviendrons mais il est important de comprendre qu'en réalité l'un ne va pas sans l'autre, et en définitive il ne peut exister de souveraineté numérique personnelle sans celle de l'État dans lequel on vit.

Concrètement, la souveraineté numérique nationale se décline sur plusieurs axes :

— la capacité d'un État à pouvoir contrôler ses moyens de défense sur le plan numérique : si un État se repose sur un fournisseur basé à l'étranger, ou sur un fournisseur ayant des technologies capables de déchiffrer ses communications les plus sensibles, les plus secrètes, on ne peut pas dire qu'il soit réellement souverain numériquement ;
— la capacité d'un État à stocker et faire opérer un certain nombres de services numériques dans une zone qu'il contrôle : cela peut être le territoire national, mais cela peut aussi signifier la capacité de pouvoir archiver et rapatrier un certain nombre de données sans être espionné ou empêché ;
— la capacité d'un État à opérer des solutions de défense numérique (de cyber-défense) qu'il contrôle et en lesquelles il a confiance : cela implique l'existence d'un écosystème de confiance, un écosystème national d'acteurs (entreprises, communautés du Libre, solutions, projets, experts, etc.).

> Cela implique aussi l'existence de partisans, d'entreprises, d'individus qui « jouent le jeu » : en cas de crise, de guerre, de cyberattaque comme en temps « normal », l'assentiment des citoyens à se défendre collectivement, au travers de l'État mais aussi en relais et soutien de celui-ci.

Il faut remarquer que ces axes n'ont de sens que si les citoyens sur lequel l'État repose ont accès à des technologies, des produits et des services qui leur permettent d'exercer au moins dans une certaine mesure leur propre souveraineté numérique. Des services numériques qui ne garantissent pas le respect de la vie privée, de la réversibilité et de la portabilité ne permettent pas une souveraineté numérique individuelle effective. En ce sens, l'État doit encourager les services, les logiciels et les écosystèmes qui donnent aux individus la capacité de rester et d'accroître leur souveraineté numérique.

— Souveraineté des individus, souveraineté nationale, en opposition ou en complémentarité ?

— La souveraineté nationale et celle des individus est distincte, mais aucune n'est exhaustive, en ce sens qu'aucune ne pourrait exister sans l'autre. Cela étant posé, il existe des cas où les deux souverainetés entrent en conflit. C'est le cas par exemple d'individus qui ne se soumettent pas à la loi ; dans cet exemple-ci, certains individus enfreignent les lois en connaissance de cause (criminalité, terrorisme). Dans un autre exemple, l'État souverain n'a pas l'assentiment (explicite, implicite) de la majorité des individus et tente par la contrainte physique, légale, économique, de poursuivre ses objectifs (dictature, guerre civile). Dans ces cas-là il est juste de dire que la souveraineté des individus est en opposition à celle de la souveraineté nationale.

Pour autant, on constate également que les deux situations évoquées plus haut ne sont pas durables : la criminalité n'est pas considérée comme une activité normale et légitime, une situation de guerre civile ou de crise politique grave mettant en jeu la violence (légitime) de l'État de façon continue envers ses citoyens ne l'est

pas non plus. La souveraineté des individus et la souveraineté nationale sont et doivent donc être complémentaires.

Aujourd'hui, un enjeu majeur est la prise en compte des sujets numériques comme sujets intégralement politiques dans le débat public. Du chiffrement à la maîtrise des données en passant par la confiance numérique, ces thèmes sont assez absents des débats « officiels ». Ils gagneraient à monter en importance, au risque cependant de simplifier certaines questions. Précisément parce que les démocraties ne peuvent faire l'impasse sur des sujets ayant des conséquences réelles sur ce qu'elles sont et leur manière de fonctionner. Il ne faut pas oublier le principe politique de base des démocraties comme la France : *le gouvernement du peuple par le peuple*.

5

Souveraineté numérique et modèles d'affaires

« Si c'est gratuit, c'est vous le produit » : voilà une phrase qu'on entend souvent lorsqu'on évoque les grands acteurs d'Internet qui proposent gratuitement leurs services. Facebook et Google en tête, ces acteurs fournissent des services d'une très grande qualité, sans demander de contribution financière à leurs utilisateurs. Pour se financer, ils collectent des données sur ces derniers et les analysent. Ils les monétisent et proposent ensuite des annonces publicitaires ciblées.

Cette gratuité n'est pas anodine. Elle vient au prix d'un traçage constant de vos activités sur Internet, au mépris de votre vie privée. Elle se nourrit de ce que vous avez de plus personnel : votre historique Google raconte, jour après jour, votre vie et vos préoccupations. Vos conversations les plus intimes sur Facebook sont analysées pour mieux cerner vos intérêts. Vos achats, vos goûts, vos déplacements, toutes ces données sont engrangées et servent à construire, touche par touche, votre double virtuel qu'il faudra faire consommer le plus possible, coûte que coûte. La grande majorité des internautes se sent espionnée sur Internet, pourtant Google et Facebook restent pourtant les deux acteurs principaux du paysage numérique contemporain. Comment cela se fait-il ?

Le piège de la gratuité

Dan Ariely, professeur en économie comportementale, a mené plusieurs expériences sur notre perception de la gratuité, qui mènent toutes aux mêmes conclusions : la gratuité est une source de satisfaction irrationnelle pour les individus. L'une de ces expériences est particulièrement parlante : lorsqu'on propose à des individus un très bon chocolat à 15 centimes et un chocolat basique à 1 centime, 73 % des individus choisissent le bon chocolat. Que le chocolat basique devienne gratuit, et 69 % des sujets le choisissent au lieu du bon chocolat. Le gratuit provoque une réaction irrationnelle et perturbe fortement notre capacité à évaluer. En prenant cela en compte, on comprend mieux pourquoi on entend systématiquement critiquer le modèle Google, mais qu'il reste un modèle dominant. Si illusoire soit-elle, la gratuité est un puissant incitateur et fausse la concurrence entre diverses solutions.

Comment en sortir ?

Il est difficile de proposer des solutions qui contrebalancent l'effet de la gratuité, mais on a pu voir une évolution ces dernières années. L'exemple de la musique permet d'établir un parallèle intéressant : l'industrie du disque s'est battue pendant des années contre le téléchargement illégal, sans comprendre que la mutation était plus importante que le simple fait de télécharger des contenus illégalement. Ce que les clients ne supportaient plus, c'était de payer cher pour un CD verrouillé qui ne leur apportait rien de plus que l'objet qu'ils avaient acheté. Aujourd'hui, les gens ont recommencé à payer pour la musique qu'ils écoutent – pas tout, évidemment – parce qu'on leur propose de payer non plus pour un objet, mais pour un service. Un catalogue important mis à leur disposition, la musique qu'ils aiment disponible partout et sur n'importe quel appareil… Ils paient pour un champ de possibilités, non plus pour un objet en particulier.

Il est plus que temps de réfléchir à des modèles d'affaire alternatifs. Nous avons rencontré Fabrice Rochelandet, chercheur à

l'Université Paris 13, pour parler plus en détails du rapport des individus à la monétisation de leur vie privée et des modèles d'affaires alternatifs.

FABRICE ROCHELANDET

Chercheur en Sciences de l'Information et de la Communication à l'Université Paris III. Il s'intéresse aux problématiques de vie privée et aux enjeux de régulation de l'économie numérique.

Déconstruire la gratuité

— Qu'est-ce que vous pensez de cette notion de souveraineté numérique, d'autonomie de l'individu sur ses données personnelles ? Est-ce que vous pensez que c'est un concept qui va se développer à l'avenir, est-ce que c'est une idée qui parle au grand public, qui s'incarne dans des pratiques ?

— Si on examine aujourd'hui la capacité de contrôle des individus sur leurs données, il y a plusieurs thèses. La première, c'est la thèse de l'*empowerment* : on pense qu'il faut essayer de rationaliser la situation en disant : « si on vous donne un contrôle sur vos données, vous serez plus conscients de la valeur de ces données, et vous allez faire plus attention ». En vous donnant un droit de propriété sur une ressource, on va vous rendre plus responsable, et vous allez y faire attention. C'est un discours que je ne trouve pas très convaincant, parce que tous les travaux dans ce domaine montrent que les individus ont une rationalité limitée à ce sujet. C'est normal, on n'essaie jamais de réfléchir à tous les possibles : si vous allez voir votre banquier, il ne va pas vous expliquer tous les placements avec leurs différents taux de risque, vous ne comprendriez pas. Il vous dira : « voilà, il y a le placement petit écureuil, le placement gentille marmotte et le placement renard aventurier… » Il vous donnera donc trois niveaux et vous proposera de choisir votre niveau de placement, plus ou moins prudent.

Ce que je reproche à la théorie de l'*empowerment*, c'est d'affirmer que les gens sont capables de gérer rationnellement leur vie privée et de gérer en continu tous les paramètres qui la concernent. Personnellement, je pense qu'il faut accompagner la souveraineté numérique. Si on donne trop de souveraineté aux individus, on crée un phénomène inverse, ce qu'on appelle une illusion de contrôle en psychologie. À force de donner aux gens des moyens de contrôle sur la manière dont les données sont collectées, leur conservation, les individus finissent par croire qu'ils contrôlent leurs données alors qu'en réalité ils finissent par en divulguer davantage et surtout ne s'intéressent plus à ce qu'elles deviennent, la manière dont elles vont être exploitées. Et ça peut multiplier les risques, ça peut les rendre victimes de cet *empowerment*, de cette mise en capacité. Cela dit, le fait que les individus doivent avoir un certain contrôle sur la manière dont leurs données sont exploitées, c'est une idée essentielle. Mais il ne faut pas trop charger la barque sur les individus, ne pas trop leur faire porter la charge du coût de ce contrôle. Il faut aider les individus, et trouver des solutions pour les accompagner.

— Quelles instances seraient pertinentes pour aider les individus, dans ce cas ? Les États, les associations, les entreprises, les startups ? Est-ce qu'il faut proposer des modèles d'affaires alternatifs ?

— Je pense qu'il faut établir une régulation mixte. À mon avis, il faut que l'impulsion soit contrôlée par des autorités indépendantes. Pas forcément par l'État, mais plutôt par des autorités comme la CNIL à condition qu'elle soit plus indépendante. Aujourd'hui, certains pensent que la CNIL est ringarde, mais ce n'est pas du tout le cas, elle manque en fait cruellement de moyens. Quand on parle avec des gens de la CNIL, ils sont très au courant de tout ce qu'il se passe, mais ils ont des budgets qui limitent leur action. Ce ne sont pas les plus pauvres en Europe : si on regarde l'équivalent de la CNIL Irlandaise, il n'y a qu'une seule personne qui gère les réclamations. J'avais réalisé cela en menant une étude dans laquelle nous avions testé les localisations des sièges sociaux des grandes

firmes d'Internet, et nous avions montré qu'il n'y avait pas qu'une question d'optimisation fiscale dans la localisation. Nous avions mis en place un indice de vie privée, et on voyait par exemple que les cent premières firmes de l'Internet choisissaient leurs sièges sociaux non seulement en fonction des avantages fiscaux mais aussi parce que la protection effective de la vie privée y était plus faible, comme Facebook en Irlande.

En plus de la régulation, il faut également stimuler les initiatives citoyennes et associatives. Je ne pense pas que cela puisse venir des entreprises dont il s'agit en fait de cadrer les comportements plutôt que de stimuler. Mais ça peut venir d'ONG, de forums d'individus, de forums citoyens, d'internautes éclairés sur le devant de la scène et qui se tiennent au courant de la situation, et qui jouent le rôle de lanceurs d'alerte. Ça peut être des internautes qui tiennent des blogs spécialisés, et la société civile a un rôle éminemment important à jouer. Et puis après, il y a des solutions qui peuvent venir du logiciel libre, j'en suis convaincu.

Ce que je défends avec d'autres collègues, c'est qu'il faut repenser l'idée de vie privée. On parle beaucoup de *privacy by design* ces derniers temps. La *privacy by design*, c'est l'idée que le respect de la vie privée doit être inclus dès la conception des outils. Nous sommes très critiques vis-à-vis de cette idée, parce qu'elle est très *top-down*. La *privacy by design* nous dit : on va déterminer vingt principes et on va donner ça aux industriels. Et qu'ils se débrouillent pour l'appliquer.

Mais ce n'est pas du tout une solution miracle : l'économie numérique est fondée aujourd'hui sur une *no-privacy by design*. L'utilité de Facebook n'existe que parce qu'on lui délivre des données personnelles. Si je ne donne pas de données personnelles à Facebook, je n'ai pas de service. C'est comme une rencontre dans un bar : si je veux me mettre en relation avec quelqu'un, il faut que je lui dise un peu ce que je fais et que la personne me dise ce qu'elle fait aussi. À une échelle beaucoup plus importante, c'est la même chose : la donnée personnelle crée le service. Les utilisateurs ont donc plutôt intérêt à divulguer beaucoup de données s'ils veulent obtenir un service personnalisé. Imposer une *privacy by design* à des

acteurs dont les services dépendent des données des utilisateurs de leur service, c'est complètement vain. La *privacy by design* peut aussi créer une illusion de contrôle.

Enfin, et c'est ce qui pose le plus de problème de mon point de vue, la *privacy by design* suppose qu'on sache ce qu'est la vie privée actuellement. Or s'il y a une chose avec laquelle je suis d'accord avec Mark Zuckerberg (le fondateur de Facebook), c'est que la vie privée est une norme sociale qui a évolué. Après, je ne suis pas d'accord avec les conséquences qu'il en tire. Mais on fait effectivement le constat que la vie privée est devenue complètement endogène au fonctionnement de la plupart des services en ligne, au rythme de l'innovation, et à l'appropriation de ces outils par les individus. On redéfinit sans arrêt les frontières de la vie privée. Donc vouloir définir en vingt critères la vie privée et imposer aux entreprises et aux développeurs de logiciel de les suivre en leur disant « voilà, la vie privée c'est ça », c'est complètement aberrant. La vie privée est une notion très moderne qui date du XIX^{e} siècle. Si vous habitez dans un village, vous avez une conception totalement différente de la vie privée que si vous habitez dans une grande métropole, où chacun vit dans l'anonymat. Évidemment, ça change aussi quand on passe au domaine numérique. La *privacy by design* est complètement aux antipodes de la souveraineté numérique des individus : on fait sans les individus, on protège la vie privée sans définir ce que c'est. Et je mets au défi n'importe qui de définir ce que c'est. La capacité de contrôle des données personnelles, c'est un moyen, ce n'est pas une définition.

— On a parfois proposé cette définition de la vie privée : « le droit à être laissé tranquille ? »

— Oui, ça peut être le droit à être laissé tranquille, mais il y a plein de gens qui ne souhaitent pas être laissés tranquilles. La vie privée numérique, c'est une dimension et elle évolue en fonction du contexte dans lequel on est. Quand on est en vacances, on peut avoir envie d'être déconnecté, on a un rapport à la vie privée qui est très différent. Par ailleurs, la vie privée est au milieu d'une

guerre informationnelle, où vous avez d'un côté les grands acteurs du Web, les banques, les assureurs qui font sans arrêt des pas en avant, que ce soit Facebook avec sa paramétrisation, ou Google qui essaie d'en savoir toujours plus sur les individus… et de l'autre côté des individus qui essaient de se protéger mais qui ne sont pas bien armés pour ça.

— *Que faire, alors ?*

— Je pense que la bonne solution est entre la *privacy by design* et la thèse de l'*empowerment*. Nous appelons cela la *privacy by using* : il s'agit d'accompagner les individus, de leur donner des outils qui permettent un certain apprentissage de la vie privée. Cela pourrait consister en un système informatique où l'on ferait apparaître de petites pastilles sur chaque application sur son smartphone. Ces petites pastilles pourraient virer au vert ou au rouge pour vous signaler selon le volume de données exigées ou exploitées par telle ou telle application. Après, c'est vous qui choisissez : vous avez Snapchat, vous avez Instagram mais attention, par rapport à votre profil, celle-ci elle est très très intrusive, vous avez déjà divulgué beaucoup de données dans d'autres applications, si vous utilisez cette application aujourd'hui, vous risquez beaucoup sur votre vie privée. Le plus important c'est d'instiller ces alertes au moment où l'individu est en situation d'usage. Ça n'empêchera pas l'individu d'utiliser la technologie qui est potentiellement dangereuse, mais ça lui donnera du recul sur son utilisation.

Notre vrai problème, c'est cette absence de norme, de définition claire et nette de la vie privée. Quels sont les bons *nudges*, quels sont les bons signaux que l'on veut faire passer ? En fait, on ne sait pas quelles sont les bonnes informations à faire remonter. Il ne faut pas tomber dans les mêmes travers que la *privacy by design*, en tout cas. D'où l'importance de la société civile, des lanceurs d'alerte, des internautes qui sont informés, parce que eux peuvent faire remonter l'information. Ensuite, il faut la traiter, il faut la synthétiser et arriver à faire en sorte que le petit système qui va vous alerter précisément, ou le petit débat qui va avoir lieu, ou la petite pop-up

qui va apparaître, le petit bilan que vous allez recevoir, tous ces éléments conjugués permettent aux internautes de faire leur choix. Et de choisir en fonction de leur usage : « moi je veux pouvoir profiter pleinement de l'Internet et tant pis pour ma vie privée » ou « j'accepte un usage restreint qui protège ma vie privée. »

— Il y a un module Firefox, Ghostery, qui permet de faire plus ou moins ce que vous décrivez. Il empêche une partie du pistage des internautes, mais ça se fait parfois au prix de certaines fonctions (les commentaires ne sont plus affichés, moins d'animations…)

— Oui, mais le problème, c'est que je ne sais pas qui est derrière Ghostery. Il faut de la transparence sur la chaîne de production de l'information. Il faut qu'on sache qui est derrière, qui est le lanceur d'alerte, un peu comme quand on se note les uns les autres sur Wikipedia. La production de l'information, la manière dont elle remonte, il faudrait que ce soit totalement ouvert. À partir de là, on informe les individus et on les informe au moment de leur usage, par des mécanismes qui ne soient pas étatiques, ni ne proviennent des grandes entreprises, mais qui viennent des communautés. Là, il y a peut-être un espoir.

— Est-ce que vous pensez qu'il y a un modèle d'affaires qui peut concurrencer le modèle du tout-gratuit, ou en tout cas de la gratuité perçue ?

— Il y a plusieurs possibilités. Soit on instaure un modèle payant, ce qui est difficile à mettre en place en raison des coûts du changement pour les utilisateurs, soit on amène petit à petit les gens à payer. C'est ce qu'il s'est passé pour le business de la musique : les plateformes ont offert des catalogues ouverts, elles ont mis en place une portabilité de la musique sur les différents appareils, et avec des modèles premium, on fait payer les gens. S'ils veulent rester en mode gratuit, on leur gâche bien leur expérience avec de la publicité pour les amener à payer. Un modèle encore

plus intéressant, c'est celui de Netflix : tout le monde paie, leur algorithme vise des communautés d'individus plutôt que directement des individus, ils ne revendent pas les données et ils les exploitent à bon escient, pour rendre du service. La clef, c'est créer du service, pour que les consommateurs aient un intérêt suffisant à payer. Au début, il faut que ce soit gratuit, sinon c'est un peu difficile de faire adhérer les gens. C'est le modèle freemium, en somme.

Mais il ne faut pas s'illusionner : le modèle dominant est aussi menacé aujourd'hui. Même les géants du web risquent de ne pas pouvoir rester éternellement dans le même modèle. Aujourd'hui, ça fonctionne parce qu'il existe une vraie croyance dans la valeur de la donnée personnelle. Quand on y pense, c'est assez stupéfiant de voir des étudiants fraîchement sortis de leur école, qui créent Snapchat et deviennent milliardaires en deux ou trois ans, alors qu'ils n'ont toujours pas de modèle économique de départ. Ils lèvent des millions et des millions en occupant un terrain qui n'est pas exactement celui de Facebook ni exactement celui d'Instagram. Ils amoncellent des tonnes et des tonnes de données personnelles et, à partir de là, ils arrivent à convaincre les marchés financiers et tous les investisseurs se ruent sur eux parce qu'on ne veut pas louper un tournant, ni continuer à investir dans la vieille économie. Et ce genre de services crée un effet de croyance énorme. Il y a des bulles un peu partout en ce moment.

La gratuité ne fonctionne que parce qu'il y a un compromis entre le consommateur qui donne ses données d'un côté et un acteur qui fournit un service de l'autre, en échange du temps et de l'attention des consommateurs. Finalement, c'est toujours le vieux modèle de la publicité étendu à tout un ensemble diversifié d'activités. Mais même ce modèle ne fonctionne pas pour beaucoup d'acteurs. Google devient à cet égard extrêmement offensif sur le *cloud* parce qu'il voit ses revenus publicitaires se tasser et qu'il se fait dépasser par Facebook pour ce qui est de la publicité en ligne sur l'Internet mobile… Mais dans l'ensemble des écosystèmes que ces opérateurs de plateformes numériques organisent, la gratuité reste un modèle dominant parce que les acteurs financiers y croient, et le jour où ce système s'écroulera, il risque de ne pas rester grand

monde. Même les grands acteurs se repositionnent pour rassurer leurs actionnaires : cette économie de la gratuité est finalement soutenue par une énorme financiarisation.

6

Proposer des alternatives crédibles

L'autonomie, une histoire de libre choix

Être autonome, que ce soit dans le domaine du numérique ou pas, implique de pouvoir choisir entre plusieurs alternatives et de ne pas être en situation de dépendance vis-à-vis d'un acteur ou d'une solution. Si une entreprise propose un service, toute personne qui l'utilise est dépendante du bon vouloir de cette entreprise : qu'elle ferme, ou qu'elle décide simplement de ne plus investir dedans, et son utilisateur n'y pourra rien. Dans le cadre numérique, cela se traduit par une dépendance à un logiciel ou à un service en ligne, et d'autant plus quand ce logiciel ou ce service appartiennent à un écosystème fermé. Si le logiciel cesse d'être disponible, le service disparaît. Pour peu qu'il ait décidé d'utiliser ses propres formats de documents, ces documents ne sont même plus exploitables. Le logiciel libre est la seule alternative qui permette une autonomie numérique : librement modifiable et redistribuable, on peut le modifier pour l'adapter à ses besoins, et le *forker* (continuer à en développer une copie) si l'entreprise cesse de le maintenir pour continuer à l'utiliser.

Le fait de pouvoir examiner le code source est également une garantie forte de confiance : son utilisateur n'est pas dépendant de l'honnêteté de l'entreprise qui produit le logiciel, puisque cette honnêteté est vérifiable.

Les alternatives existantes

Aujourd'hui, il existe de nombreuses alternatives libres et open source aux services les plus populaires. LibreOffice propose des services pour remplacer la Suite Office de Microsoft, Gimp peut remplacer Photoshop… Pour permettre aux internautes d'utiliser des services comparables à ceux fournis par Google, l'association Framasoft a lancé l'initiative Dégooglisons Internet en 2012, qui consistait notamment à fournir des services alternatifs, gratuits et respectueux de la vie privée des utilisateurs. Leur initiative a connu un grand succès, notamment parce qu'elle offrait des services faciles à utiliser et relativement ergonomiques. Mais ils se sont rapidement retrouvés confrontés à deux problèmes : ils n'avaient que les moyens d'une association pour tenir la charge de centaines de milliers d'utilisateurs, et ils finissaient par devenir un nouvel acteur central, ce qui ne rentrait pas dans leur optique de ne pas enfermer les utilisateurs.

Même lorsqu'on propose une solution libre et open source, il ne s'agit pas d'enfermer les utilisateurs en étant la seule alternative possible aux GAFAM : décentraliser, même au niveau du libre, est un effort essentiel.

Le design, prochain défi du logiciel libre

Proposer des alternatives techniques est un premier pas essentiel, sans lequel rien n'est possible. Il s'agit désormais de passer un nouveau seuil : faire en sorte que les utilisateurs de ces alternatives ne soient pas seulement un public déjà sensible aux enjeux du logiciel libre et de la décentralisation, mais des utilisateurs lambdas qui utiliseront ces solutions non pas par dépit, mais par choix, parce qu'elles sont aussi ergonomiques et puissantes que les solutions

proposées par Google ou Microsoft. Pour cela, se concentrer sur le design et l'ergonomie et réfléchir en termes d'expérience utilisateur est un défi majeur posé au logiciel libre. La route est longue, mais la voie est libre !

PIERRE-YVES GOSSET

Délégué général de Framasoft, association d'éducation populaire promouvant le logiciel libre et la culture libre. Militant des libertés numériques, il coordonne la plupart des projets de l'association.

Framasoft, de l'esprit du Libre

— Pourquoi la concentration des données nuit-elle à la souveraineté numérique/l'autonomie numérique des individus ?

— La concentration des données à un seul endroit crée une soumission de l'individu à un tiers. Plus cette concentration est importante, plus la soumission et la dépendance sont grandes. On pourrait faire la même analogie avec le pouvoir. Il ne viendrait à personne l'idée de donner tout le pouvoir du monde à 1, ou même à 10 individus, qui pourraient créer les lois, les modifier, ou appliquer la justice !

On a donc un système de pouvoir mondial plutôt décentralisé : il y a bien sûr des États, mais ceux-ci reposent sur une répartition du pouvoir (par exemple le judiciaire, le législatif et l'exécutif, dans la plupart des sociétés occidentales). Il existe en plus une décentralisation au sein de l'État : État, régions, départements, communes, quartiers, familles, etc. Si on en revient au numérique, notre postulat est simple : l'information – et donc les données – sont du pouvoir !

Une donnée comme votre numéro de sécurité sociale peut déterminer à quelles aides vous avez droit. Une autre donnée peut vous envoyer en prison. De façon plus légère, la reconnaissance faciale sur la photo de vacances d'un ami peut indiquer à votre patron si vous avez préféré la mer ou la montagne.

Partant de ce postulat, j'estime que la délégation de pouvoir que nous accordons aux GAFAM est de plus en plus importante. Et qu'aucun contre-pouvoir réel, y compris celui du logiciel libre, ne semble pouvoir y mettre un terme.

Les photos que l'on télécharge sur Instagram, les documents que l'on crée sur Google Docs, les liens que nous entretenons avec nos « amis » sur Facebook etc. sont autant de « minuscules pouvoirs » que nous donnons à ces entreprises. Petit à petit, octet par octet. Tout au long de la journée. Rien ne prouve à l'avance qu'elles en feront mauvais usage. Mais rien ne prouve le contraire non plus ! Et cela peut même se faire contre leur volonté, dans le cas d'une faille exploitée par des personnes mal intentionnées, ou lorsqu'un gouvernement impose à ces entreprises de fournir des données.

Mais, même sans aller jusqu'à ces cas – qui sont loin d'être extrêmes, puisqu'avérés dans les faits – la soumission des individus aux GAFAM se constate au quotidien : un compte de réseau social fermé arbitrairement, une interface web qui ne prend plus en compte un handicap, l'obligation de se créer un compte Google pour accéder à un contenu, la très forte incitation à être présent sur Facebook pour rester en contact avec nos amis.

Les problématiques qui émergent sont donc celles-ci : faut-il souhaiter une autonomie numérique des individus ? Et pourquoi ? Si l'on est capable de répondre à ces questions plus politiques et éthiques que techniques, alors la démonstration sera faite que la concentration des données est nuisible à cette autonomie.

— Comment sortir de cette centralisation et rendre leur souveraineté/autonomie numérique aux individus ?

— La force des GAFAM est de laisser croire (ou de faire croire) qu'ils sont devenus indispensables, et que cela ne vaut pas la peine d'aller chercher ailleurs, puisqu'ils sont gratuits et extrêmement efficaces. Partant de là, les utilisateurs se disent « Bah, Google ou Microsoft : même combat. Pourquoi irais-je m'embêter à m'autohéberger ou à trouver un prestataire local puisque j'ai déjà ce qui

se fait de mieux techniquement ? » Notre réponse ne doit donc pas seulement être technique.

En ce qui concerne Framasoft, nous avons choisi la stratégie suivante :

D'abord, expliquer

Nous travaillons avec tous les types de publics, et cela nous permet de nous rendre compte de l'ignorance globale de bon nombre de personnes face au numérique. Certes, beaucoup d'usages sont – à peu près – maîtrisés. Mais demandez-leur comment fonctionne Internet et vous vous apercevrez vite qu'ils ne peuvent pas percevoir les enjeux de la concentration des données puisqu'ils n'ont pour la plupart aucune idée de ce qu'il se passe lorsqu'ils uploadent leurs photos de vacances sur Facebook.

Et je pense d'ailleurs sincèrement qu'il s'agit d'une volonté délibérée (sans y voir de complot pour autant !) des GAFAM de laisser le grand public dans cette ignorance. Tout simplement parce que quand on comprend une chose, on peut la *hacker*, détourner ses usages, en inventer de nouveaux etc.

La bonne nouvelle concernant ce point, c'est que l'être humain est fondamentalement curieux. Par conséquent, si on l'accompagne dans la découverte des phénomènes techniques ou financiers d'Internet, la réaction quasi-systématique que nous constatons est… que les gens veulent en savoir plus ! Nous essayons de décrire ces phénomènes de concentration, leurs enjeux, et leurs conséquences (immédiates et potentielles). Ensuite, libre à chacun de faire ce qu'il veut : modifier son comportement et agir, ou estimer que la situation est acceptable pour lui et ses semblables, et qu'elle ne mérite pas l'effort bien réel que nécessite le changement.

Nos moyens pour cela sont dérisoires : un site web (degooglisons-internet.org) et une petite centaine d'interventions face au public par an. Mais au moins, nous faisons notre part.

Ensuite, démontrer

Une fois les enjeux compris, et les réponses à leurs questions obtenues, il n'était pas rare qu'on nous dise « Très bien, je veux agir : vous me proposez quoi comme alternative ? ». Et là, c'était le drame©.

En effet, comment dire à une personne convaincue que la centralisation des données est nuisible qu'elle doit s'installer un serveur de pad (en node.js), un serveur Owncloud (PHP) ou un service type Loomio (dans un conteneur docker) le tout sur un serveur dédié ! Les gens sont curieux, mais bien rares sont ceux techniquement compétents pour ce genre de choses (et on ne peut pas les en blâmer). Si cette première marche est trop haute, il n'y a juste aucune chance qu'ils grimpent tout l'escalier menant à éviter les GAFAM.

La solution que nous avons mise en place était simple dans l'idée, mais complexe en pratique : proposer nous-même ces services à tout un chacun. Nous sommes donc devenus hébergeurs de solutions libres comme Etherpad, Owncloud ou Loomio, que nous avons traduites, mises en valeur, et… ouvertes au public. En les invitant à découvrir des alternatives autrement que sur la capture écran d'un compte github, cela a rendu concret le fait qu'il était possible d'utiliser autre chose que les services des GAFAM.

Nous nous sommes engagés à ouvrir 30 services libres en 3 ans. Après deux ans, nous en sommes à 20, il nous en reste encore donc 10. La route est longue, mais la voie est libre !

Enfin, essaimer

La bonne nouvelle, c'est que le public nous a suivis.

La mauvaise nouvelle, c'est qu'il nous a suivis *en masse* !

Nous savions que nous allions avoir des milliers d'utilisateurs. Voire des dizaines de milliers. Mais nous n'avions pas envisagé d'en avoir des centaines de milliers ! Heureusement, nous avons des compétences en interne qui nous permettent de tenir la charge, mais devenir un point central, un nouveau silo de données – fût-

il libre ! – n'était pas *du tout* l'objectif que nous avions en tête. Nous avons donc accéléré notre phase d'essaimage, l'idée principale étant de « décentraliser Framasoft » en accompagnant l'émergence de nouvelles structures ou mettant en valeur des structures existantes, ayant les mêmes valeurs et objectifs que la nôtre.

— Comment ne pas reproduire de nouveaux silos de services alternatifs aux GAFAM ?

— D'abord, en construisant des milliers de petits silos, tellement petits qu'on ne pourra pas les considérer comme des silos. Ensuite, en donnant à l'utilisateur la possibilité de passer ses données d'un « micro-silo » à l'autre de façon aussi simple que possible.

Pour le second point, nous savons déjà que les solutions libres et interopérables sont l'unique solution. Mais la mise en œuvre simple de processus de migration dépasse aujourd'hui largement le champ de compétence de notre association.

Pour le premier point, c'est l'objectif du projet « CHATONS » (Collectif des Hébergeurs Alternatifs Transparents, Ouverts, Neutres et Solidaires) que Framasoft impulse cet automne.

Ce projet visera à mettre en avant de petites structures proposant des services en lignes libres, respectueux des données, sans publicité, etc. Afin que tout citoyen souhaitant quitter les GAFAM puisse trouver une structure (de préférence autre que Framasoft) pouvant l'accompagner dans cette démarche.

Un aspect essentiel du projet CHATONS est que nous souhaitons qu'il y ait une prise en compte de l'aspect pédagogique des enjeux. Il ne s'agit pas uniquement de proposer des services alternatifs. Les *Chatons* devront s'engager à essayer de réduire l'écart qui se creuse entre les citoyens lambda et les informaticiens. C'est essentiel, afin d'aller dans le sens de l'adage « Si tu donnes un poisson à un homme, il mangera un jour. Si tu lui apprends à pêcher, il mangera toujours. »

Évidemment, il ne s'agit pas de faire de Kevin Dupuis-Morizeau un spécialiste de node.js ! Mais si nous pouvons l'aider à comprendre qu'il y a des humains derrière les services et ser-

veurs qu'il utilise, et qu'on peut même offrir un verre à ces humains pour qu'ils puissent expliquer pourquoi le service était en panne la veille, nous aurons redonné du savoir et du pouvoir, et enfoncé un coin dans la démarche de « délégation de pouvoir » menée par les GAFAM.

On a beaucoup parlé du « comment ? » avec plein de solutions techniques. Nous (libristes), on répète : « c'est pas bien, parce que les gouvernements blablabla, l'espionnage blablabla, etc. »

Mais le fait est que mes parents, eux, ils s'en cognent du gouvernement ou de l'espionnage. Je pense qu'il nous faut construire un discours transversal, multi-disciplinaire (informatique, philosophique, mathématique, sociologique, écologique, etc. et surtout, *surtout*, économique) sur le capitalisme de surveillance.

7

Blockchain et droit à l'oubli

Être souverain et autonome implique de ne pas dépendre d'un acteur qui a le pouvoir de couper l'accès à nos données, fermer notre compte du jour au lendemain sur un réseau social, nous empêcher de récupérer simplement nos documents… Autant de pratiques qui sont aujourd'hui très communes dans l'Internet centralisé que nous connaissons ! Mais depuis quelque temps, une alternative à ces modèles centralisés se popularise : la *blockchain*.

Si on connaît souvent la *blockchain* grâce à la monnaie numérique Bitcoin, le concept d'origine est beaucoup moins spécifique que cela. Expliquer son fonctionnement précis serait trop ardu, intéressons-nous plutôt à ses spécificités et à sa possible utilisation.

La *blockchain* est un réseau ouvert et décentralisé. Tout le monde peut la consulter. Elle vit grâce à l'activité du réseau qui l'héberge. En cas de problème avec une *blockchain*, il n'y a personne à contacter. Personne n'a le pouvoir de modifier seul la *blockchain*, ni d'en supprimer un quelconque élément. Mais son contenu est infalsifiable. Merveilleuse promesse de souveraineté ! Une communauté peut enregistrer des opérations dont elle peut garantir l'authenticité, et sans risque de laisser à une personne le pouvoir de supprimer des éléments ou la tentation de modifier l'historique à son avantage. Moins de centralisation, plus d'indépendance.

Mais la situation n'est pas aussi simple. Avoir une autorité centrale n'est pas une lubie, cela permet d'avoir quelqu'un qui garantit que les membres peuvent avoir confiance les uns dans les autres puisque quelqu'un est là pour régler les conflits et faire respecter les règles. Et si on décentralise la confiance, on décentralise également cette capacité de régler les conflits. Si demain quelqu'un enregistre sur une *blockchain* une information qui me compromet, un contenu illégal ou non libre de droit, personne n'est plus en mesure de le retirer. Pour peu que ce contenu attente à ma vie privée, c'est plutôt une impossibilité de faire respecter la souveraineté numérique des individus qui se profile. Pour illustrer cette problématique, Primavera de Filippi et Michel Reymond analysent la possibilité de faire appliquer le droit à l'oubli [1], élément emblématique de la souveraineté des individus, aux informations contenues dans une *blockchain*.

1. Le droit à l'oubli permet aux citoyens européens de demander aux moteurs de recherche le déréférencement de certaines informations les concernant.

PRIMAVERA DE FILIPPI, MICHEL REYMOND

Primavera de Filippi est chercheuse au CNRS à Paris et à l'université de Harvard. Michel Reymond est actuellement assistant post-doc à la Faculté de Droit de l'Université de Genève.

La blockchain : comment réguler sans autorité

Le 13 mai 2014, la Cour de Justice de l'Union Européenne (CJUE) rendait l'arrêt Google Spain, qui accordait aux citoyens européens le droit de demander l'effacement des résultats de recherches menant à des sites Internet contenant des informations inexactes, inadéquates ou excessives les concernant. Le droit à l'oubli repose sur le droit à la protection de la vie privée : il postule que les personnes physiques n'ont pas à rendre indéfiniment des comptes sur les événements honteux ou désagréables auxquels ils ont été associés dans un lointain passé. De façon plus large, on pourrait décrire le droit à l'oubli comme une tentative de conciliation entre, d'une part, le besoin humain d'être réhabilité ou pardonné, et, d'autre part, le rôle d'Internet en tant que registre numérique de l'histoire (Leta Jones, 2016)

Cette opposition est d'autant plus forte depuis l'apparition de nouvelles bases de données décentralisées, connues sous le nom de *blockchains*, soit la technologie utilisée par le réseau Bitcoin. Dans la mesure où la blockchain est inaltérable et résistante à la censure et à la modification par conception, elle entre en conflit direct avec le droit à l'oubli. [1] La présente contribution cherche à analyser les défis posés par ces technologies émergentes vis-à-vis du droit à l'ou-

1. Le présent article traite du droit à l'oubli tel qu'il est défini par la loi européenne, et plus précisément par la *Directive 95/46/EC du Parlement européen et du concile* du 24 octobre 1995 sur la protection des individus quant à la gestion de leurs données personnelles et de la libre circulation de ces données. Les variations légales

bli. Nous présenterons d'abord le droit à l'oubli (I) et la blockchain (II), nous analyserons ensuite si le droit à l'oubli a titre à s'appliquer à la blockchain (III) et, si tel est le cas, nous examinerons plus en avant si et comment les obligations afférant au droit à l'oubli peuvent être exécutées sur la blockchain (IV).

Définitions

Le droit à l'oubli

Le droit à l'oubli est une obligation de droit communautaire de la protection des données, imposée aux moteurs de recherche. Il permet aux citoyens européens de demander le retrait de résultats de recherches liés à leur nom et qui mèneraient à des sites Internet contenant des informations « inexactes, inadéquates ou excessives », et qui ainsi porteraient atteinte à leur vie privée. Le droit à l'oubli a été déduit par la CJUE du droit Européen de la protection des données, et notamment de la *Directive 95/46/CE*, dans l'arrêt Google Spain, en mai 2014. À l'issue de celui-ci, un ressortissant espagnol a pu amener le moteur de recherche Google à retirer un lien, apparaissant suite à une recherche portant son nom, vers une notice originellement publiée en 1998 et archivée sur le site d'un journal espagnol ; celle-ci portait sur sa participation à une vente aux enchères dans le but de recouvrer ses dettes de sécurité sociale (CJUE, 2014). L'obligation concerne tous les moteurs de recherche, mais la position hégémonique de Google sur ce marché en a fait le principal destinataire. La société a par conséquent mis en place un processus décisionnel interne pour le déréférencement et a reçu jusqu'à présent environ 500 000 requêtes, conduisant au retrait d'environ 1 500 000 résultats au total [1].

Il faut noter que le droit à l'oubli ne s'applique qu'aux liens fournis par un moteur de recherche non-spécifique à la suite de

de ce concept dans les lois nationales de certains États membres (Leta Jones, 2016) ne seront pas prises en compte ici.

1. Voir Google Inc. (28 août 2016). *Requêtes européennes de déréférencement liées à la vie privée*. Tiré de `https://www.google.com/transparencyreport/removals/europeprivacy/`.

la recherche du nom d'une personne (CJE, 2014, at par. 96). *A contrario*, il n'affecte pas directement l'intégrité du contenu référencé, comme par exemple le site web d'un journal, un article ou un billet émis sur un blog ; il n'a pas non plus vocation à s'appliquer aux résultats obtenus en cherchant des mots-clefs autres que nom et prénom. Ainsi, le droit à l'oubli est conceptuellement plus proche d'un droit limité au déréférencement plutôt qu'à un droit d'être oublié au sens littéral [1]. Et même s'il n'est pas exclu que ce droit puisse éventuellement s'appliquer au-delà des simples moteurs de recherche généralistes, et donc s'étendre à d'autre types d'intermédiaires informationnels, une telle extension nécessite que ces intermédiaires incarnent un danger similaire pour la vie privée des individus. Par exemple, cela sera le cas lorsqu'ils permettent à leur utilisateurs, lors d'une recherche portant sur un nom, d'obtenir un « aperçu structuré » leur permettant d'établir un profil plus ou moins détaillé de la personne concernée (CJUE, 2014, at pars. 37, 80 ; Article 29 DPWP, 2014, at par. 17-18).

La blockchain

Une blockchain est une base de données décentralisée qui possède quelques caractéristiques spécifiques. En premier lieu, une blockchain fonctionne comme un réseau décentralisé en pair-à-pair, qui n'est ni possédé ni contrôlé par une autorité centrale. Chaque pair du réseau possède une copie de la blockchain, et il contribue avec ses capacités de calculs à la sécurité et au maintien des opérations du réseau. En second lieu, une blockchain est une base de données à laquelle on ne peut que faire des ajouts : la seule possibilité est d'ajouter de l'information, dans l'ordre chronologique ; il est impossible de modifier ou supprimer une information une fois qu'elle est enregistrée. Enfin, une blockchain est un registre certifié [2], qui repose sur la cryptographie pour assurer que

1. La dénomination « Droit à l'oubli » est trompeuse. Une alternative appropriée serait « Droit au déréférencement ». Dans un souci de simplicité, nous utiliserons tout de même le premier.

2. Dans la mesure où une blockchain permet uniquement d'ajouter de l'information, les données ne peuvent être ni modifiées ni supprimées par qui que ce soit. On peut ainsi utiliser une blockchain pour certifier l'intégrité d'un ensemble de données

toutes les données enregistrées sont cohérentes, et ont été validées par la majorité des nœuds du réseau (Nakamoto, 2008).

Les avantages de cette technologie sont évidents, notamment sur la question de l'intégrité des données et de leur certification. Puisque personne ne peut modifier l'information stockée dans une blockchain *a posteriori*, la blockchain peut prouver qu'un document spécifique a existé, ou qu'un événement est arrivé à un moment *t* (Lemieux, 2016).

En revanche, la blockchain soulève de nombreuses inquiétudes, en majorité liées à l'inaltérabilité de l'information contenue (Vogel, 2015). La technologie fonctionne de telle manière qu'il serait impossible de supprimer du contenu illicite ou inadéquat s'il venait à être stocké dans une blockchain sans une action coordonnée de la majorité des nœuds individuels. Et dans la mesure où elles peuvent contenir des informations inadéquates, non pertinentes ou excessives, les blockchains pourraient également devenir un défi posé au droit à l'oubli. Puisqu'aucun acteur central n'est là pour contrôler le réseau, personne ne peut être tenu responsable de l'application du droit à l'oubli dans la blockchain (Umeh, 2016)

Les interactions entre la blockchain et le droit à l'oubli

L'application du droit à l'oubli à la blockchain Bitcoin

En partant des éléments expliqués ci-dessus, il pourrait être intéressant de se questionner sur l'éventuelle application du droit à l'oubli à la blockchain Bitcoin. Si, par hypothèse, un individu avait opéré une transaction gênante dans le passé, comme une inscription à un site du type Ashley Madison, pourrait-il légitimement demander la suppression de cette transaction du registre Bitcoin ?

Puisque le droit à l'oubli ne s'applique présentement qu'aux moteurs de recherche généralistes, le premier réflexe est de répondre par un « non » catégorique. On peut néanmoins se deman-

stockées à l'intérieur. De plus, toutes les données enregistrées dans une blockchain doivent être signées par la clef privée de la personne qui les ajoute. Ainsi, même si l'identité de cette personne n'est pas connue, on peut tout de même s'appuyer sur la blockchain pour certifier la source des informations contenues.

der dans quelle mesure le droit à l'oubli pourrait être étendu à la blockchain Bitcoin par analogie, la possibilité d'une telle extension n'étant, on le rappelle, non exclue d'emblée si l'intermédiaire informationnel porte un danger suffisant pour la vie privée des individus, et notamment par la diffusion d'un profil public lorsqu'on entre le nom d'une personne. Ce dernier élément de l'argument sous-tend cependant que l'exercice du droit à l'oubli exige un élément de publicité et d'accessibilité au public : c'est d'ailleurs pourquoi les moteurs de recherche ont l'obligation de prévenir à l'affichage de certains résultats mais ne sont pas pour autant amenés à retirer les liens correspondants de leur index ni à empêcher leur diffusion lors de l'emploi d'autres mots-clés que des noms (Reymond, 2016, at 41-43). Par conséquent, une personne ne devrait pas pouvoir l'invoquer pour demander la suppression d'un lien non public contenu dans une base de données en ligne ; le droit à l'oubli ne peut donc pas être invoqué pour faire supprimer certaines informations disponibles sur Internet : il ne sert qu'à protéger les citoyens de la perspective d'être indéfiniment liés à des contenus faciles à trouver sur Internet, comme dans le cas où un employeur taperait le nom de ses recrues potentielles au moment de l'embauche (Rustad & Kulevska, 2016, at 365-366).

Sur deux aspects, la blockchain Bitcoin ne répond pas à ces exigences. Premièrement, dans la mesure où le réseau Bitcoin met en relation des pseudonymes, l'information liée à la transaction notée dans le registre décentralisé ne permet pas l'identification des utilisateurs du réseau, et ne donne aucune information sur le contexte général de l'échange (De Filippi, 2016). Les individus qui font des échanges en Bitcoin ne sont désignés dans la blockchain qu'à travers leur adresse Bitcoin, un identifiant global sous forme d'une chaîne de caractères de ce type : 37WctrDb1G1orXhJ8vgx7zS2WCuSuBk6EQ. Aucune autre information n'est disponible, ni sur leur identité hors ligne, ni sur la nature de leur transaction. Ainsi, les informations stockées dans la blockchain Bitcoin ne pose pas d'effet visible sur la vie privée des personnes qu'elle répertorie, ou en tout cas dans aucune mesure comparable à un moteur de recherche. Deuxièmement, les infor-

mations stockées sur la blockchain ne sont pas accessibles librement, ou tout du moins avec bien moins d'aisance qu'avec un site web ou un moteur de recherche. De par sa nature en tant que base de données décentralisée distribuée sur un réseau d'ordinateurs, la blockchain Bitcoin n'est véritablement accessible qu'aux seuls utilisateurs ayant les moyens logistiques et informationnels leur permettant d'installer les logiciels nécessaires pour obtenir l'accès au réseau et à en miner les données contenues. Évidemment, cette tâche requiert une connaissance et des efforts incomparables à ceux fournis pour consulter un site Internet.

Bien entendu, nous n'entendons pas par là que le droit à l'oubli ne peut pas s'appliquer aux intermédiaires qui fournissent une interface permettant de consulter directement la blockchain Bitcoin. Le site Internet blockchain.info, par exemple, fournit un accès simple et mis à jour en temps réel sur l'état du registre Bitcoin, quoiqu'il ne lie aucune donnée de transaction à des informations qui permettraient d'identifier des personnes.

À l'inverse, si le site Internet permettait de lier des adresses Bitcoin à des noms et prénoms réels, et de permettre la recherche d'entrées par noms dans ce cadre, nous aurions potentiellement un cas d'application du droit à l'oubli. Cependant, même dans ce cas, l'obligation de déréférencement ne s'appliquerait qu'à ce site en particulier, et uniquement en vertu de sa fonction de portail direct de recherche dans la blockchain Bitcoin. Le droit à l'oubli ne concernerait donc en aucun cas la blockchain Bitcoin en tant que telle.

Le droit à l'oubli appliqué à d'autres usages de la blockchain (le cas Steem.it)

La blockchain Bitcoin n'est qu'un exemple parmi tant d'autres des usages possibles de cette technologie émergente. À la suite de la popularisation du Bitcoin, de nombreuses autres applications basées sur la blockchain ont été développées, chacune avec leurs caractéristiques propres (Crosby & al., 2016). Pour le moment, la plupart d'entre elles relèvent du domaine de finance, mais quelques unes apparaissent dans le domaine de la création et de la distribution de contenu (Swan, 2015). Steem.it est un exemple emblema-

tique de cette tendance ; il s'agit une plateforme de publication et de réseau social basée sur la blockchain dont le principe tient à la favorisation et à la rémunération, à l'aide d'une monnaie virtuelle, des contributions de ses utilisateurs. Ces contributions peuvent prendre plusieurs formes, allant de la publication de contenu original (des billets de blog, des vidéos, des images, etc.) à la conservation active de la plate-forme par l'appréciation du contenu soumis par d'autres utilisateurs (commentaire, votes positifs et négatifs…)

Steem.it est basé sur sa propre blockchain, dans laquelle chaque contribution est stockée grâce aux métadonnées appropriées (identité du contributeur, commentaires, votes reçus). Le contenu textuel est directement stocké dans la blockchain, et les images et vidéos sont hébergées par des solutions tierces : seul le lien vers ce contenu est stocké dans la blockchain. On pourrait affirmer que la blockchain Steem.it pourrait être concernée par le droit à l'oubli, au moins dans la mesure où certains pourraient l'utiliser pour extraire des informations liées à des individus spécifiques.

Cependant, comme décrit ci-dessus, le contenu enregistré dans une blockchain ne peut plus être ni modifié, ni supprimé par qui que ce soit dans la mesure où la technologie de la blockchain est, par essence, inaltérable. Ainsi, l'intégralité du contenu enregistré dans la blockchain Steem.it est impossible à censurer. Et puisqu'il n'y a aucune autorité centrale qui gère le réseau, aucun gouvernement ne peut adresser de requête visant la suppression d'informations sensibles ou de contenu considéré comme illicite.

Cela étant, la plupart des utilisateurs de Steem.it n'interagissent pas directement avec sa blockchain, mais se contentent d'accéder aux contenus via son site Internet, qui est, lui, géré de manière centralisée. En effet, le site Internet de Steem.it collecte des informations sur les contributions de la blockchain Steem.it, et les présente de manière claire et accessible, avec le nom des contributeurs. Tous les contenus ne sont pas affichés sur le site : à la suite de l'évaluation de ces contenus, ceux qui ont reçu des votes négatifs finissent par disparaître du site – quoiqu'ils restent stockés dans la blockchain. En ce sens, le site Internet de Steem.it peut être considéré comme un intermédiaire (ou plutôt un infomédiaire) qui collecte

les informations d'une base de données et les rend accessibles au public en fonction de critères spécifiques. En tant que tel, on pourrait tout à fait invoquer le droit à l'oubli pour demander aux administrateurs du site Internet de Steem.it de retirer un contenu qui divulguerait des informations inadéquates ou excessives sur une personne.

L'application du droit à l'oubli pourrait cependant être difficile dans la mesure où le site de Steem.it, tout centralisé qu'il soit, manque d'une structure centralisée de modération et d'administration. La modération est effectuée par les utilisateurs eux-mêmes, qui prennent la responsabilité de donner des votes négatifs aux contenus qu'ils considèrent comme inappropriés. Autoriser la suppression d'un contenu qui n'aurait pas reçu de votes négatifs de la part de la communauté de Steem.it contreviendrait à leur politique et pourrait dissuader leurs utilisateurs de continuer à utiliser le site Internet. De plus, dans la mesure où toutes les informations de la blockchain de Steem.it sont publiques, il est impossible d'empêcher des tiers de développer leurs propres versions alternatives (de type darknet) du site de Steem.it et de proposer un accès exhaustif à la blockchain, y compris aux informations indésirables, à ceux qui voudraient réellement y avoir accès.

L'exécution du droit à l'oubli sur la blockchain

Problématiques

Imaginons une plateforme fictive basée sur la blockchain qui fonctionnerait comme un LinkedIn décentralisé, nourri par les contributions de ses utilisateurs. Cette blockchain serait un registre dans lequel n'importe qui pourrait ajouter des informations au sujet d'une personne en particulier – par exemple, en fournissant des liens vers un contenu déjà disponible sur Internet. Toute personne qui souhaiterait en savoir plus sur un individu pourrait parcourir le contenu accumulé par l'entier des utilisateurs. Dans un tel scénario, il va sans dire que le droit à l'oubli pourrait légitimement être invoqué, car ce service permettrait à n'importe qui d'accéder à une sorte de profil public de la personne, qui pourrait inclure des liens

ou des références à des informations « inexactes, inadéquates ou excessives ». Certes, on pourrait argumenter que l'élément de publicité n'est pas rempli, car ces informations seraient moins immédiatement consultables que si elle étaient indexées par un moteur de recherche ou même disponibles sur le véritable LinkedIn, mais dans l'hypothèse où la blockchain serait accessible à n'importe qui, il reste vraisemblable que le droit à l'oubli puisse être invoqué pour demander la suppression de certains liens et contenus.

L'application hypothétique du droit à l'oubli à une telle plateforme soulève de nombreuses interrogations quant au degré de responsabilité des acteurs qui la font vivre, ainsi qu'à leurs devoirs. Contrairement aux plateformes traditionnelles qui fonctionnent sur un modèle centralisé et dont on peut facilement identifier le fournisseur d'accès, un réseau blockchain est opéré par chacun des nœuds du réseau, de manière décentralisée – il n'existe aucune entité centrale ayant l'autorité ou la capacité technique d'ajouter, supprimer ou modifier les informations stockées dans la blockchain.

Ainsi, on peut légitimement se demander comment un LinkedIn décentralisé pourrait appliquer le droit à l'oubli dans le cas où un citoyen européen demanderait la suppression d'un lien contenu dans la blockchain. En l'absence d'intermédiaire, qui serait responsable d'assurer la mise en œuvre de cette requête ? Et qui serait tenu, le cas échéant, responsable d'un tel manquement au droit à l'oubli ?

À première vue, dans la mesure où la blockchain est par essence inaltérable et que le stockage d'informations est irréversible, demander la suppression d'un élément de la blockchain semble tout simplement absurde, puisqu'impossible à réaliser techniquement. Et puisque personne n'a le pouvoir de supprimer unilatéralement les données d'une blockchain, personne ne peut être tenu responsable de la non-suppression de certaines informations.

Cependant, résumer ainsi les liens entre blockchain et droit à l'oubli est assez réducteur. De fait, l'action coordonnée des nœuds actifs du réseau permet de supprimer certaines données d'une blockchain. Dans le cas du Bitcoin, par exemple, deux transactions apparemment valides mais incompatibles l'une avec l'autre

(l'exemple classique est une double dépense des mêmes fonds de départ) seront sujettes au protocole de consensus décentralisé de Bitcoin, qui permettra de décider de la transaction à conserver et de celle qu'il faut supprimer (Nakamoto, 2008) – alors que cela implique clairement de changer l'état actuel de la blockchain. On pourrait imaginer que cette technique s'applique au retrait de contenu illégal (contenus sous copyright, discours d'incitation à la haine ou pédopornographie) d'une blockchain publique. S'il y a consensus sur le fait que certains contenus soient inappropriés vis-à-vis de la plateforme, il est techniquement possible de les retirer de la blockchain. Bien entendu, c'est trouver ce consensus au sein d'un réseau décentralisé qui pose la principale difficulté (De Filippi & Loveluck, 2016), et ne pas y parvenir a parfois des conséquences inattendues.

Ethereum et ses implications sur le droit à l'oubli

L'exemple récent du *hack* de *TheDAO* nous fournit une bonne illustration de ces différentes problématiques : à la suite de ce *hack*, la blockchain Ethereum s'est séparée en deux réseaux différents : Ethereum et Ethereum Classic. Cet événement n'impliquait certes aucune question de vie privée ou de liberté d'expression, mais son analyse permet d'avoir un aperçu pertinent des enjeux du caractère inaltérable de la blockchain.

Ethereum est une plateforme blockchain de cryptomonnaie semblable au Bitcoin. Lancée en juin 2015, elle permet à ses utilisateurs d'échanger des jetons Ether (ou ETH). Contrairement au Bitcoin, la blockchain Ethereum inclut un langage Turing-complet, qu'on peut utiliser pour inclure du logiciel dans ses transactions. Pour donner un exemple concret : Alice pourrait vouloir mettre en place un versement régulier à Bob à chaque fois qu'un événement spécifique survient. En intégrant ces instructions à la blockchain, le paiement sera effectué comme prévu, sans qu'Alice ni Bob n'aient besoin de faire quoi que ce soit de leur côté. Ces possibilités, qui existent sous la dénomination de contrats intelligents, peuvent concerner des conditions très simples ou des montages logiciels très complexes.

Dans ce contexte, *TheDAO* (abréviation de Organisation Autonome Décentralisée) a été lancé en avril 2016. L'objectif de *TheDAO* était de mettre en place une organisation complètement automatisée, dont les règles de fonctionnement s'appliquaient dans le cadre des contrats intelligents. Le code permettait à des investisseurs d'envoyer des fonds dans un portefeuille commun, et de recevoir un nombre de jetons proportionnel à leur investissement, ce qui leur permettait de participer à la gouvernance et à la prise de décisions de l'organisation en question. Un mois après son lancement, l'organisation avait déjà attiré 150 millions d'Ether d'investissement. Un tiers de la valeur de l'argent investi fut dérobé le 18 juin 2016 par un attaquant non-identifié [1] qui avait exploité une vulnérabilité dans le code des contrats intelligents.

Devant l'indignation provoquée par cet événement, la communauté Ethereum a décidé d'intervenir en mettant en place une action coordonnée pour effectuer des modifications dans la blockchain Ethereum (un *hard fork*). Tous les participants actifs du réseau ont été invités à passer à une version alternative du registre, dans lequel les fonds qui avaient été volés n'appartenait plus à l'attaquant mais étaient déposés dans un compte créé pour l'occasion pour que les investisseurs récupèrent leur argent. Cette solution n'a pas fait l'unanimité : quelques utilisateurs ont avancé que cette action compromettait l'inaltérabilité de la blockchain et ont refusé d'adopter cette version alternative. Cet événement a conduit à l'émergence d'une blockchain Ethereum alternative – Ethereum Classic – qui rejetait le *hard fork* et conservait la blockchain originale.

Il y a de nombreux enseignements à tirer de cette histoire. Avant tout, elle donne la preuve que les blockchains peuvent être modifiées. Si elle se retrouve face à des sanctions économiques ou juridiques, la communauté qui fait vivre une blockchain peut prendre la décision d'intervenir collectivement pour censurer une transac-

1. Dans la mesure où il n'y a eu ni intrusion ni effraction dans le système, on peut se demander si les fonds en question ont effectivement été « volés » par un « attaquant » ou s'ils ont simplement été récupérés par un individu très bon techniquement qui a réussi à comprendre comme utiliser le code à son avantage pour transférer l'argent à une tierce partie.

tion spécifique ou supprimer des informations y contenues. Mais la nécessité de respecter les lois européennes de protection des données seront-elles une incitation suffisante ? La question reste ouverte. Le second enseignement à tirer de l'exemple d'Ethereum est le constat que même si la majorité de la communauté souhaite collaborer avec les autorités chargées de faire respecter la loi, il est difficile de faire disparaître les informations de la blockchain sans le consensus de toute la communauté. Il suffit d'un simple désaccord pour que la blockchain se sépare en deux réseaux différents.

Conclusion

L'apparition de la blockchain va avoir d'indéniables conséquences sur la régulation de la mise à disposition des informations, notamment d'un point de vue technique : les données d'une blockchain ne peuvent être modifiées ni supprimées. Il est cependant plus difficile d'évaluer l'impact de l'émergence de ces nouvelles technologies sur la possibilité de faire appel au droit à l'oubli. De fait, ce n'est pas la résistance à la censure de la blockchain qui pose directement problème : le droit à l'oubli ne peut pas, du moins dans sa version actuelle [1], donner lieu à une demande de suppression de contenu, mais uniquement le déréférencement de ce contenu. Bien entendu, il n'est pas exclu que des citoyens européens puissent légitimement invoquer le droit à l'oubli dans le cas où des liens de ce type seraient stockés dans une blockchain et où ils permettraient à un large groupe d'utilisateurs d'accéder à des informations inexactes, inadéquates ou excessives. Dans ce cas précis, les spécificités techniques de la blockchain risqueraient de poser problème à l'application du droit à l'oubli. Dans la mesure où la blockchain n'est pas gérée par un administrateur central, au-

1. L'avenir du droit à l'oubli est à examiner au regard du passage en force, dans moins de deux ans, du Règlement général européen sur la protection des données (GDPR), qui contient notamment un « droit à l'oubli » dans son article 17. On ne sait pas encore si ce droit à l'oubli se contente de réaffirmer ce qui se fait aujourd'hui sous l'arrêt Google Spain ou s'il contient de nouveaux aspects (*Contrast Rustad & Kulevska*, 2016, at 367-370. Voir aussi Daphne Keller « The Final Draft of Europe's Right to be Forgotten Law », *Center for Internet and Society*, 17 déc. 2015, cyberlaw.stanford.edu.

cune entité n'a l'autorité ni la capacité de modifier ou supprimer unilatéralement des éléments de la blockchain. La seule possibilité de modifier ou supprimer les données incriminées implique un accord et une action coordonnée de l'intégralité – ou au moins d'une large majorité – des nœuds actifs d'une blockchain, qui effectuerait de manière cohérente les modifications nécessaires (Wright & De Filippi, 2015). Bien entendu, l'exemple d'Ethereum nous a montré que même s'il existait un large consensus autour d'une modification de la blockchain, il suffit d'une petite minorité qui rejette la modification pour qu'elle puisse maintenir une version non-modifiée de la blockchain.

Bibliographie

Article 29 Data Protection Working Party, November 26, Guidelines on the Implementation of the Court of Justice of the European Union Judgment on « Google Spain and Inc v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja Gonzàlez », C-131/12, 14/EN, WP 225.

CROSBY Michael et *al.*, « BlockChain Technology : Beyond Bitcoin », in *Applied Innovation Review*, **2**, 2016. http://scet.berkeley.edu.

DE FILIPPI Primavera, « The interplay between decentralization and privacy : the case of blockchain technologies », in *Journal of Peer Production*, **9**, 2016. http://peerproduction.net/.

DE FILIPPI Primavera et Benjamin LOVELUCK « The invisible politics of Bitcoin : governance crisis of a decentralized infrastructure », *Internet Policy Review*, **5**(4), 2016. `http://policyreview.info`.

European Court of Justice, May 13 2014, *Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González, Case C-131/12.*

LEMIEUX Victoria, « Trusting Records : Is Blockchain Technology the Answer ? », *Records Management Journal*, **26**(2), 2016, p. 110-139. http://www.emeraldinsight.com.

LETA JONES Meg, *Ctrl+Z : The Right to be Forgotten*, New York, NY : New York University Press, 2016.

NAKAMOTO Satoshi, « Bitcoin : A peer-to-peer electronic cash system », *bitcoin.org*. https://bitcoin.org/bitcoin.pdf.

REYMOND Michel Jose, « Hammering Square Pegs into Round Holes : The Geographical Scope of Application of the EU Right to be Delisted », *Berkman Klein Center Research Publication*, **12**, 2016. http://ssrn.com/abstract=2838872.

RUSTAD Michael L. et Kulevska Sanna, « Reconceptualizing the Right to be Forgotten to Enable Transatlantic Data Flow », *Harvard Journal of Law & Technology*, **28**(2), 2015, 349-417. http://ssrn.com/abstract=2627383.

SWAN Melanie, *Blockchain : Blueprint for a new economy*, Sebastopol, CA : O'Reilly Media, Inc., 2015.

UMEH Jude, « Blockchain Double Bubble or Double Trouble ? », *ITNOW*, **58**(1), 2016, p. 58-61. http://itnow.oxfordjournals.org/content/58/1/58.abstract

VOGEL Nick, « The Great Decentralization : How Web 3.0 Will Weaken Copyrights, 15 J. Marshall Rev. Intell. Prop. L. 136 », in *The John Marshall Review of Intellectual Property Law*, **15**(1), 2015, p. 137-149. http://repository.jmls.edu/ripl/vol15/iss1/6.

WRIGHT Aaron et DE FILIPPI Primavera, « Decentralized blockchain technology and the rise of lex cryptographia », à paraître. http://ssrn.com/abstract=2580664

8

Construire un discours sur l'autonomie

Comment défendre l'autonomie numérique ?

Le discours sur la souveraineté et l'autonomie numériques des individus se trouve au croisement de plusieurs sensibilités techniques et philosophiques. L'autonomie numérique permet-elle de s'opposer à la surveillance de masse ? Permet-elle d'avoir un usage plus intéressant de ses données personnelles ? Est-ce un combat politique ? Elle touche indéniablement à toutes ces dimensions à la fois. Nous avons traité des aspects techniques de la souveraineté et de l'autonomie numériques, mais la dépossession actuelle pose également des problèmes de nature politique. Il n'est pas sain que le paysage numérique soit dominé par un puissant oligopole qui passe un contrat implicite avec ses utilisateurs pour les profiler. Il n'est pas sain que leurs services se substituent implicitement à ceux des États. Mais, pour les raisons que nous avons évoquées plus tôt, il est difficile de sensibiliser les utilisateurs de ces services, et plus difficile encore de faire bouger les lignes.

Porter une vision alternative

On ne peut faire l'économie d'un discours fort et porteur de sens si on souhaite proposer une vision alternative d'Internet. Le processus est en bonne voie : toutes les études montrent la disponibilité des individus à de nouveaux discours, une appétence nouvelle pour les services qui respectent leur vie privée, un engouement à l'égard des solutions alternatives. Pour autant, on ne peut se contenter de faire peur, au risque de ne créer qu'un mal-être sans apporter de solution. Il faut à la fois porter un discours économique, social, philosophique sur les problèmes posés par le système actuel, et proposer des contre-modèles qui donnent envie de mettre en place un changement qui ne va pas de soi.

Nous nous sommes entretenus avec Christophe Masutti, co-président de Framasoft, qui porte un discours fort sur l'autonomie individuelle des citoyens. Partant du principe que l'État n'est pas un acteur qui a les moyens de garantir la sécurité numérique des citoyens, il développe une analyse économique du capitalisme de surveillance et de la nécessité de construire une autonomie numérique pour tous et toutes.

Dans un registre très différent, Alain Damasio nous apporte un magnifique éclairage sur le rôle de la science-fiction dans la construction d'un contre-imaginaire.

CHRISTOPHE MASUTTI

Co-président de Framasoft, association d'éducation populaire promouvant le logiciel libre et la culture libre. Il est responsable de projets européens au CHU de Strasbourg et chercheur associé au SAGE, Université de Strasbourg.

Du *software* au *soft power*

— Comment décrire les problèmes politiques posés par la concentration des données ? Peut-on y remédier en promouvant la souveraineté et l'autonomie numérique ?

— La question est très large et appelle un développement. En fait, j'ai toujours eu un peu de mal avec ces trois notions qu'il faut définir.

La concentration des données, en soi, n'est qu'un moyen pour obtenir un résultat. C'est l'utilité de ce dernier, c'est-à-dire l'intention qu'il faut questionner. Concentrer, cela revient à collecter et rassembler des informations en un seul point. Ce n'est pas une pratique condamnable. L'Insee, pour prendre un exemple connu, a toujours pratiqué ce type de collecte à des fins d'analyse et je pense qu'on ne saurait remettre en question les avantages cognitifs et pratiques des données de l'Insee.

Dans le contexte qui nous occupe, nous parlons de *big data*. C'est un niveau bien supérieur à ce que pratique l'Insee depuis l'après-guerre, même avec des moyens de plus en plus modernes. Les *big data* proviennent de plusieurs sources et celles produites par des institutions privées ou publiques à des fins statistiques (des *hard datas*) n'en constituent qu'une petite partie [1]. La partie la plus

1. Voir sur une typologie des données dans l'acception *Big Data*, le rapport d'Antoinette Rouvroy, *Des données et des hommes. Droits et libertés fondamentaux dans un monde de données massives*, Bureau du comité consultatif de la convention pour la

spectaculaire des données que rassemblent des grandes multinationales provient en réalité de nous-mêmes, il s'agit des *soft datas* que nous laissons plus ou moins volontairement en fonction de nos comportements de consommateurs de biens et services, gratuits ou non : entrées de requêtes dans des moteurs de recherche, flux de données de géolocalisation en temps réel, comptage de clics, mesure de l'attention informationnelle, etc. Moins connues sont les *métadonnées*, c'est-à-dire la provenance des données, les durées, les mesures de trafic, les vitesses de connexion, les traces et historiques de géolocalisation, etc. Bref un ensemble d'informations que nous pensons souvent inutiles du point de vue individuel, négligeables du point de vue de la taille, mais qui, en grandes quantités, traduisent avec une exactitude impressionnante l'ensemble de nos comportements. Ces données sont multipliées du point de vue sémantique dans tout ce qui concerne l'Internet des objets, le *quantified self* et toutes les pratiques qui lient des services et des conditions d'exercice de ces services (je profite d'un bien à condition de donner en retour des informations très personnelles sur moi).

Toutes ces informations pourraient être rassemblées et traitées par une multitude d'entreprises qui, chacune, utiliserait ces informations pour améliorer les biens et services en question en passant des contrats clairs avec les utilisateurs. Un peu comme le contrat que je passe avec ma banque qui connaît énormément de choses sur mon comportement de consommateur. Il y aurait donc un contrat entre l'utilisateur et la firme : je te confie mes données et tu me fournis un service (si possible plus performant). Or, aujourd'hui, non seulement le contrat est la plupart du temps fallacieux mais en plus le nombre de firmes est finalement très faible. Pour ne prendre que l'exemple d'Alphabet Inc., ce conglomérat regroupe plusieurs entreprises, *think tank* et sous-traitants aux secteurs d'activités très différents et qui pourtant traitent tous de manière plus ou moins directe des données des individus utilisateurs des services, en particulier ceux de Google, dans une logique de monopole (publicitaire, en particulier).

protection des personnes à l'égard du traitement automatisé des données à caractère personnel, Conseil de l'Europe, janvier 2016.

Là où la concentration des données pose problème, c'est à la fois dans leur quantité et dans les secteurs où elles deviennent des facteurs permettant de profiler non plus les individus, mais la société en entier tant les secteurs d'activité concernés recomposent le social (dans le cas d'Alphabet Inc. : biotechnologie, médecine, jeux, communications en tout genre, économie, bourse, automobile, urbanisation, robotique, cartographie et espaces, biens culturels et même corruption). Ainsi le problème politique de la concentration des données, c'est justement l'idéologie dont les solutions technologiques de ces multinationales sont devenues les supports. Et cette idéologie, c'est en premier lieu celle de la substitution de l'État par des services, et en second lieu l'absence de toute forme de contrat de confiance. Par exemple, il n'y a plus besoin de confiance entre individus si nous faisons reposer uniquement la fiabilité de nos informations sur des algorithmes faisant foi/loi. Je ne dis pas que, par exemple, l'utilisation de services sécurisés par SSL est un problème, je dis que la tendance à vouloir remplacer notre espace de confiance entre citoyens par des solutions technologiques cause immanquablement une révision de la nature de nos relations sociales. Il en va ainsi de tous les contrat dits *clauses de confidentialité* et *clauses d'utilisation* que nous passons avec toutes sortes de services numériques, comme Facebook, et qui font régulièrement l'objet de questionnements quant à leur éthique : l'éthique est justement ce qui n'a plus à être pris en compte dès lors que l'on considère que la contrepartie de l'utilisation d'un service est l'abandon même de la confiance. Je donne toutes mes informations personnelles et mon intimité à une firme : qu'a-t-elle besoin d'attendre mon accord individuel si son objectif n'est pas de me profiler, moi, mais tout le monde, pour une « meilleure société » ?

Partant de ce constat, ce qu'on appelle « souveraineté numérique » correspond à l'idée qu'à l'échelle d'un pays, d'un État, il puisse exister suffisamment de ressources pour que les usages de services numériques puissent y être circonscrits au moins en droit, au mieux que les supports technologiques des services soient intégrés dans l'espace de confiance d'un État. À l'heure de la mondialisation des échanges boursiers et des firmes, cette vision est

bien entendu celle d'une chimère. L'autonomie numérique ne peut donc être que celle des utilisateurs eux-mêmes. En refusant les contrats iniques, la diffusion et la concentration de leurs données, les citoyens peuvent chercher des solutions capables de créer des chaînes de confiance auxquelles ils peuvent participer en partageant les ressources, en coopérant à leur création ou tout simplement en utilisateurs éclairés.

Cette autonomie, aujourd'hui ne peut plus être garantie par l'un ou l'autre État. Depuis les révélations d'E. Snowden, celles de Wikileaks, l'édiction de diverses lois scélérates de surveillance généralisée et autres procès discutables, les gouvernements ont fait la preuve qu'il est devenu impossible qu'ils puissent créer une sphère de confiance suffisamment crédible pour que des citoyens puissent considérer que leurs données (leurs informations personnelles) y soient protégées. La seule solution repose sur un postulat : il doit être primordial pour un peuple de pouvoir disposer de solutions technologiques capables de garantir physiquement (mathématiquement) le secret et l'anonymat des citoyens, à n'importe quel prix, et reposant sur des solutions libres/open source. Nous avons atteint les limites du contrat social : avec des firmes comme les GAFAM, l'État n'est plus capable d'assurer la sécurité numérique des citoyens, c'est à eux de construire leur autonomie en la matière.

— Le capitalisme de surveillance, sur lequel vous avez écrit une longue analyse, est-il un obstacle à la souveraineté numérique des individus ?

— Ramené au rang de paradigme, le modèle de l'économie de cette première tranche du XXI^{e} siècle, pas seulement celle des services numériques, repose sur la captation des données et leurs valeurs prédictives. L'économie libérale, celle que l'on trouve dans les livres aux origines du capitalisme moderne, composait avec l'idée d'une égalité entre les acteurs économiques et celle d'un équilibre général où tout échange trouve sa fin dans la satisfaction de chacun. Dans un article paru en 2015, intitulé « Big other : surveillance

capitalism and the prospects of an information civilization », la chercheuse Shoshana Zuboff[1] montre que la logique d'accumulation des données, l'automatisation de leur traitement et leur analyse en autant d'inférences et de prédictions, faussent la logique de l'équilibre général. Pour cela les firmes mettent en œuvre des pratiques d'extraction de données qui annihilent toute réciprocité du contrat avec les utilisateurs, jusqu'à créer un marché de la quotidienneté (nos données les plus intimes et à la fois les plus sociales). Ce sont nos comportements, notre expérience quotidienne, qui deviennent l'objet du marché et qui conditionne même la production des biens industriels (dont la vente dépend de nos comportements de consommateurs). Mieux : ce marché n'est plus soumis aux contraintes du hasard, du risque ou de l'imprédictibilité, comme le pensaient les chantres du libéralisme du XX^{e} siècle : il est devenu malléable parce que ce sont nos comportements qui font l'objet d'une prédictibilité d'autant plus exacte que les *big data* puissent être analysées avec des méthodes de plus en plus fiables et à grande échelle. Selon S. Zuboff, cette nouvelle forme de capitalisme est nommée « capitalisme de surveillance ».

Reste l'explication du titre de l'article : « Big Other ». Dans son roman, G. Orwell nommait un état de surveillance tout puissant *Big Brother*. Pour S. Zuboff, les firmes aujourd'hui capables d'une surveillance / conformation du marché à l'échelle mondiale, n'ont pas pour objectif de remplacer l'État comme on le ferait avec un *coup d'État*. C'est un *coup des gens* qu'oppose S. Zuboff à cette idée, c'est-à-dire que c'est dans le marché, c'est-à-dire dans et par la société et notre soumission volontaire à la logique de l'accumulation de données, que naît cette altérité supérieure de l'économie de la surveillance, remplaçant l'idéal d'une démocratie libérale, un *Big Other* dont l'une des personnifications est Google (dans le texte de S. Zuboff). On pourrait dire aujourd'hui l'ensemble des GAFAM, Alphabet et compagnie.

1. Shoshana Zuboff, « Big other : surveillance capitalism and the prospects of an information civilization », *Journal of Information Technology*, 30, 2015, pp. 75-89.

— Les GAFAM ont aujourd'hui le quasi-monopole du stockage et de la gestion de nos données : quelles sont les implications politiques de la concentration des données dans les silos de quelques grands acteurs ? Je pense notamment à Apple qui refuse certaines applications jugées trop politiques dans l'App Store, ou à Facebook qui prend le rôle d'un service public avec son Safety Check)

— Il y a encore peu de temps, le problème que pouvait soulever la concentration des données, c'était celui de la remise en question de la sphère privée. C'est toujours le cas, mais nous assistions à un changement social en pensant seulement que nous avions encore le choix entre accepter ou non les contrats d'utilisation des services numériques des grandes firmes. Nous n'avions peur que de *Big Brother*. Or, nous n'en sommes plus là. Comme S. Zuboff le montre, le développement des méthodes d'analyse des *big data* est en progression constante, si bien que, dans les mains de firmes gigantesques avec autant de domaines d'application, nous avons besoin d'appréhender ce bouleversement avec des outils qui dépassent le seul stade de l'analyse de risque individuel ou collectif de la diffusion des données personnelles. Dans l'histoire économique mondiale, les firmes n'ont jamais été autant en mesure de modeler le marché à volonté grâce à la puissance de l'analyse des données à grande échelle. Non seulement les données sont déjà diffusées et utilisées, mais elles sont aussi extraites et accumulées sans aucune réaction de l'ordre de la décision publique.

C'est en cela que l'État échoue à protéger ses citoyens, et dans cette faille du contrat social les solutions de facilité s'engouffrent : encore récemment notre ministre français B. Cazeneuve surenchérissait dans la lutte anti-terroriste en appelant à une limitation drastique des messageries chiffrées à l'échelle internationale [1], provoquant ainsi la colère des spécialistes [2] qui rappellent l'utilité économique et sécuritaire du chiffrement dans tout système d'infor-

1. Voir cet article de Julien Lausson, « Cazeneuve en croisade contre le chiffrement, rappelé à l'ordre par la Cnil et le Cnnum », *Numerama.com*, 23/08/2016.

2. Voir cette tribune signée par Isabelle Falque-Pierrotin, Mounir Mahjoubi et Gilles Babinet, « En s'attaquant au chiffrement contre le terrorisme, on se trompe de cible » journal *Le Monde*, 22/08/2016.

mation. Pour que des décideurs publics soient à ce point pro-actifs dans le passage de marché avec les GAFAM (comme c'est le cas dans l'Éducation Nationale française) ou soient prêts à ce que nos communications transitent en clair à travers les services des mêmes GAFAM, c'est bien parce que l'établissement des firmes sur le marché est vécu comme un état de fait, immuable. Tout est fait pour qu'Internet ne soit plus qu'un marché avec quelques services identifiés et non plus un réseau ouvert, partagé et diversifié. La réduction de l'offre de services sur Internet est conçu par les décideurs publics comme un outil visant à faciliter la surveillance et justifier le manque de maîtrise des outils numériques dans la plupart des secteurs des services publics. De leur côté, les firmes jouent un double rôle : collaborer politiquement et asseoir toujours davantage leurs situations de monopoles.

— Comment sensibiliser le grand public à ces implications politiques ? Quel type de discours construire ?

En France, s'adresser au public ne peut se faire que de manière directe mais avec certains principes. Une méthode directe c'est-à-dire sans passer par un filtre institutionnel. Et pour cause : par les réformes successives de l'Éducation Nationale, l'État a échoué à former ses citoyens à l'autonomie numérique. Cela aurait pu fonctionner au milieu des années 1980, à la « grande époque » du Plan Informatique Pour Tous qui mettait l'accent sur la formation à la programmation. Aujourd'hui malgré de nombreux efforts, seule une petite partie des lycéens peuvent avoir accès à un véritable enseignement à la programmation informatique depuis 2013 tandis que la majorité n'auront d'autre choix que de pianoter laborieusement sur des outils Microsoft. Dans un contexte académique, former les jeunes à des concepts aussi complexes que les protocoles du réseau Internet, à un peu de langage de programmation, aux enjeux du profilage, de la confidentialité des systèmes d'information et surtout au droit et au cadre de la liberté d'expression, cela revient à marcher sur des œufs avec un éléphant sur le dos.

Les principes de la sensibilisation au grand public doivent être beaucoup plus simples : diffuser et démontrer que l'offre en logiciel libre est fiable, montrer que cette fiabilité repose à la fois sur la qualité des programmes et sur une chaîne de confiance entre l'hébergeur, le concepteur, l'utilisateur et même le fabricant des machines sur lesquelles on travaille. On ne touche pas les gens avec un discours mais en faisant une démonstration : montrer que des alternatives ne se contentent pas d'exister mais qu'elles respectent leurs utilisateurs sur la base du partage d'information, de connaissance et de code. C'est l'objectif de la campagne Degooglisons Internet de Framasoft, mais c'est bien davantage : pour faire cela, il faut des relais de proximité et ces relais constituent tout le tissu de l'économie sociale et solidaire (ESS), y compris des petites entreprises, qui permettront de relayer le modèle sur un mode d'éducation populaire [1]. Si longtemps, nous avons naïvement cru que la lutte contre un Internet déloyal devait se faire par le haut, enfermés que nous étions dans une tour d'ivoire digne des Cathares les plus radicaux, l'heure est venue de mobiliser les foules par un mouvement de fond. Pour répondre au capitalisme de surveillance qui modèle le marché, il faut fausser le marché.

— À quoi ressemblerait un monde ou le libre aurait échoué ? Où les GAFAM auraient gagné ? Ou les silos continueraient de grossir ?

Sommes-nous réellement dans cette dualité ? Je pense que le Libre (et tout ce qui en découle, c'est-à-dire au-delà de l'informatique) est une réaction à un monde où le partage n'existe pas. L'histoire du logiciel libre le montre bien : c'est en réaction à l'idée que le non-partage est source quasi-exclusive de profit que le logiciel libre s'est formalisé en droit, par une licence et un contrat de confiance. Ces principes ne peuvent pas échouer, tout au plus ils peuvent être muselés, voire condamnés, tyrannisés. Mais l'essence de l'homme, c'est le partage.

Nous avons beaucoup plus à craindre d'un accroissement des monopoles et du jeu des brevets, parce qu'en monopolisant les sys-

1. Voir la fiche Wikipédia consacrée à l'éducation populaire.

tèmes d'information planétaires, ce ne seront plus les hommes d'un pays particulièrement enclin à la dictature qui seront muselés, mais tous les hommes et femmes de tous les pays. Les monopoles, parce qu'ils composent avec les politiques, ne peuvent que limiter l'exercice de la liberté d'expression. En d'autres termes, l'erreur que nous avons tous commise dans les années 1990, lors des bulles Internet, ce fut de croire que nous pouvions communiquer à l'échelle mondiale en profitant d'une libéralisation des réseaux. Le jeu des monopoles fausse complètement cette utopie. Les GAFAM ont déjà gagné une partie, celle qui a débouché sur l'impuissance publique (quelle firme des GAFAM, totalisant des milliards de capitalisation boursière, serait censée avoir peur de quelques millions d'euros d'amende de la part de la Commission Européenne ?, soyons sérieux [1]). Si nous échouons à faire du Libre le support de nos libertés informatiques, numériques, culturelles… il nous faudra réinventer un Internet différent, hors contrôle, hors confiance, résolument anarchique. Ce n'est pas non plus une solution qu'il faut viser, mais ce serait la seule alternative.

1. L'exemple récent de la Commission Européenne réclamant 13 milliards d'Euros à la firme Apple en guise d'arriérés d'impôts illustre bien les difficultés. D'une part l'Irlande qui a abrité la firme derrière une politique fiscale offensive, s'en offusque et fera tout pour réduire l'impact de l'amende. La France, par l'intermédiaire du ministre Michel Sapin a fait savoir très rapidement qu'elle ne compte pas réclamer sa part de l'amende, les États-Unis vont exercer une pression formidable sur l'Europe, et il y a fort à parier qu'en définitive l'amende sera fortement réduite, que des États finiront par flancher et même payer une part du manque à gagner, tandis qu'Apple continuera à engranger des bénéfices en provisionnant l'amende. L'impact sur la firme sera finalement très réduit et se traduira par des pertes d'emploi.

ALAIN DAMASIO

Alain Damasio est auteur de science-fiction et scénariste. Ses deux romans majeurs, *La Horde du Contrevent* et *La Zone du Dehors* en ont fait une figure incontournable de la science-fiction politique française.

Pour un combat des imaginaires

— *Avec* La Zone du dehors, *vous aviez relevé un défi essentiel : mettre de la substance sur ce sur quoi on doit lutter. Contre quoi est-ce qu'on lutte aujourd'hui ? Le* Big Data, *la centralisation des données, le profilage des utilisateurs, ce sont les symptômes de quoi ?*

— D'une société de contrôle qui va au bout de sa logique en devenant une société de traces ! Ce sont des symptômes de la poursuite, insidieuse et raffinée, de ce qui s'est mis en place depuis les années 80 : un néolibéralisme qui a opéré la jonction avec les technologies intrusives, et qui a décidé que tout un ensemble de champs qui lui échappaient encore – l'amitié et ses circuits d'échange par exemple, l'amour, la création culturelle, l'expression numérique – devaient désormais être reconfigurés sous forme de marchés dont on peut extraire une plus-value exponentielle. C'est un mouvement historique très soutenu qui consiste à maximiser la liberté putative des gens tout en optimisant les mécanismes qui « l'accompagnent », la contrôlent et l'exploitent afin que cette liberté-même devienne la source de la valeur économique : des données précises, corrélables, quantifiées qu'on restructure pour créer des profils de comportement, des patterns d'habitudes prédictives qu'on va s'efforcer d'anticiper pour mieux gérer et mieux vendre. Ce régime de pouvoir autorise donc un

maximum de choses, rien n'y est explicitement interdit, car c'est précisément ces envies et désirs guidant les individus et les foules dont on a impérativement besoin pour « conduire les conduites » selon l'expression superbe de Foucault.

Si l'on s'avise de ce que font les GAFAM aujourd'hui, on voit bien qu'ils minimisent toute contrainte ou forme d'autorité visible, tout relent directif ou disciplinaire. On laisse les gens chercher ce qu'ils veulent sur Google, on les laisse dire et partager ce qu'ils souhaitent sur Facebook, écouter ou voir ce qui les fait kiffer sur YouTube. On empuissante ainsi une liberté d'expression et de consommation aussi vaste (et bavarde !) que possible pour mieux récupérer les données qui vont leur permettre de prédire nos comportements. C'est un behaviourisme assez glaçant qui se fonde sur les données-que-tu-donnes-librement. Chacun de nous, acteur numérique en ligne, est donc une « balance » involontaire ou consentante. Sauf que le type qu'on « donne », c'est nous – nous et nos amis, nous et nos « contacts » comme dans les polars d'autrefois. Si tu imposes une contrainte aux gens, tu ne sauras pas quel désir les porte profondément, quel site ils veulent vraiment visiter et pendant combien de temps, quels sont leurs mots-clés, leur films phares, leurs préférences… En leur laissant le champ libre, avec une capacité de traçage et d'analyse dont le coût est assez dérisoire si tu les compares aux techniques de filature d'antan, tu obtiens une aérodynamique du pouvoir optimale : d'un côté, des individus destructurés, perdus devant les choix innombrables d'une société liquide, cherchant des modèles, des figures enviables, imitant et copiant des attitudes et des pratiques, soumis et appelant même les contaminations virales ; de l'autre des processus de collecte ultrapuissants qui agrègent et repèrent ces modèles, les formatent et les proposent, en boucle — normes douces qui prennent des noms « funs » comme *buzz*, tendances, mode, *hype*, *must-have*… Au lieu de fliquer, on induit, on suscite, on incite, on rend probable les comportements que l'on souhaite voir se généraliser – souvent parce que la marge y est plus favorable (l'achat dématérialisé par exemple ou la délégation aux clients des tâches de secrétariat de type remplissage de formulaire, le *digital labor*, etc.)

Foucault ou Deleuze avaient très bien anticipé ces nouvelles catégories du pouvoir, mais ils n'avaient pas pu deviner le raffinement des outils technologiques qui allaient les rendre possibles à des échelles et avec des économies de moyens aussi prodigieuses. Nous sommes passés depuis 1995 du contrôle à l'hypercontrôle, continu, doux et ubiquitaire. Et à des formes croisées d'intercontrôle, d'intracontrôle, de *self data*, d'autocensure et d'autosurveillance. Qui aurait pu anticiper que les citoyens se jetteraient sur les smartphones avec une telle avidité totalitaire (99% de pénétration en France ; mieux que l'eau potable !), qu'ils en feraient tout à la fois le cœur de leur interfaçage aux autres et au monde, et l'outil de contrôle auto-administré le plus fantastique jamais conçu ! Imaginer qu'un collier électronique, qui est pour Deleuze et Guattari le stade ultime de la prison à ciel ouvert, allait devenir un bien de consommation et un support quotidien d'interaction intime, que les gens porteraient volontairement, qui aurait pu le croire ? Se dire qu'on allait finalement adorer être géolocalisé en permanence, qu'on s'y soumettrait avec le sourire et même avec beaucoup d'enthousiasme, parce que ça facilite quelques tâches cognitives qui sont finalement assez dérisoires ; imaginer que les gens allaient si facilement accepter et revendiquer ça au nom des commodités et des fluidités offertes, personne, il me semble, ne l'avait prédit.

L'apparition de ce que j'appelle les objets nomades totalitaires, comme le smartphone, a fait de nos vies une production continue de données et de traces. Rien de ce qui est humain n'est plus étranger aux GAFAM. « Toutes vos communications pourront être retenues contre vous ». Cette société de traces a fait de nous des chiens incontinents qui pissent partout sans le savoir, et de nous tout autant des limiers qui sniffons ces traces dans nos métiers, dans nos sphères privées, pour surveiller et contrôler ce que font nos proches. C'est l'archétype d'une « mauvaise rencontre », pour parler comme Benasayag qui le reprend de Spinoza : la rencontre entre une économie de désirs vulgaires, qui nous traverse tous (voyeurisme, besoin de contrôle, régression infantile dans la fusion communicante, syndrome du petit chef jouissant de sa machine-esclave, paresses multiples, autant physiques que cognitives…) et

des possibilités techniques neuves qui les relaient et leur offrent une extension indéfinie.

— À quoi est-ce que ça ressemble un monde où les GAFAM ont gagné ? Au niveau individuel ? Au niveau politique ? Au niveau des États ?

— Belle question ! C'est à peu près le monde que j'essaie de mettre en récit dans *Les Furtifs*, mon roman au long cours ! Je développe une partie dystopique dans le roman, très flippante, notamment sur ce capitalisme poussé à l'extrême, tranquillement, en particulier dans la gestion des villes. Les villes y empruntent sur le marché bancaire international au point de faire faillite si bien que les villes les plus intéressantes ne relèvent plus du champ public et sont rachetées par les multinationales en fonction de leur identité-phare. LVMH a racheté Paris, la ville du luxe et de l'élégance ; la Warner a racheté Cannes ; Nestlé la capitale de la gastronomie, Lyon. Et Orange rachète la ville d'Orange pour minimiser l'acquisition de la marque. Mises aux commandes, ces entreprises créent des forfaits standard, premium et privilège qui te donnent accès à tel ou tel pourcentage des rues, des parcs, des places, etc. L'espace public est reprivatisé. C'est une première piste, pas propre aux GAFAM. Ce qui pourrait leur être propre, et incarner leur hégémonie, ce serait à mon avis la création des intelligences artificielles personnalisées. Des assistants intimes omnipotents, forme d'*alter ego* numériques qui sauront absolument tout sur nous puisqu'on les alimentera à chaque minute par nos actes, nos achats, nos choix, nos messages, nos tweets, surfs, sms, mails, agendas, etc. À l'image du film *Her*, mais avec une amplitude qui dépassera de loin le seul érotisme. Je pense que la Silicon Valley veut et va trouver le moyen de verrouiller affectivement le rapport de l'individu à son écosystème technologique. La seule chose qui leur manque vraiment aujourd'hui, c'est la capacité à créer un lien affectif très fort avec une machine unique et personnelle, tout à fait monopolistique de nos vies, vers laquelle toutes nos données pourraient converger. En temps réel évidemment, sans coupure, avec un

historique intégral pouvant partir de notre naissance et dans une logique d'auto-apprentissage permanent, qui épousera nos habitudes. Cette MIA (Mon Intelligence Artificielle) ou cet ALIAS (Assistant Local à Intelligence Artificielle Sentiente) saura tout de nos existences au quotidien, par défaut. Elle en archivera et retraitera chaque élément pour nous fluidifer la vie. Il n'y aura naturellement aucune intelligence là-dedans, mais des tombereaux de *Big Data*, de l'algorithmie massive auto-alimentée et auto-paramétrée par nos choix d'options et surtout une envie de simplicité et d'interlocuteur *sentient* qui décidera de son succès.

Dans mon roman *Les Furtifs*, le dispositif fonctionne avec des bagues qui servent d'objet connecté et un gant oled dans la maincible pour visualiser les contenus sur sa paume. Les interfaces tactiles sont sur ta peau, tu peux vidéoprojeter ce que tu veux sur des surfaces dédiées qu'on retrouve dans les espaces publics et privés, partout, et tu l'as avec toi H24. Aujourd'hui, les golems du numérique cherchent cette convergence, un unique objet absolument polyvalent avec lequel les consommateurs puissent interagir incessamment. Je pense qu'à terme, la tendance sera d'aller au-delà du smartphone vers des objets encore plus simples, sobres et naturels – le bijou est une option crédible –, encore plus dématérialisés aussi puisque les *clouds* sont des banques que seul le prestataire contrôle vraiment : c'est une expropriation précieuse de nos propres ressources *data*, c'est comme si vous confiiez votre argent à la banque sans jamais le revoir ! En terme d'interface, ils vont sans doute se concentrer sur le tactile et le vocal, la lecture du regard, des lectures grossières de la pensée aussi, grâce aux ondes EEG. Le basculement psycho-social se fera grâce à des moteurs de dialogues très poussés, une gestion sensuelle de la voix et des inflexions, gavées au *Big Data*. Bref, il me semble probable qu'ils développent un système d'*alter ego* numérique. Google pourrait l'appeler, tiens, « MuM » : *My Unique Machine* : ce sera notre *Big Mother* adorable et enveloppante, plus tendre et plus compréhensive encore qu'une maman – et tu retrouveras l'ensemble de ce que tu es dedans : tes mails, tes rendez-vous, ton agenda, tes photos, vidéos, textes, déplacements, ton histoire personnelle complète, ta santé, la possibilité d'échan-

ger et de jouer avec qui tu veux, *and so on* ! Et la différenciation se jouera sur la capacité de l'interface à être crédible en tant qu'interlocuteur vivant, vibrant, émotionnellement habité.

L'être humain, et notamment l'enfant, a une pensée animiste naturelle qui nous permet de prêter des sentiments à un doudou ou à une machine, mais pour l'instant, les interfaces ne passent pas encore le seuil de la crédibilité projective (croire à des pensées et sentiments humains dans l'*alter ego*) ! Le jour où l'on va passer un cap qualitatif sur les moteurs de conversation, le transfert affectif pourra fonctionner à plein. Sans doute d'abord au Japon, parce qu'ils ont une pensée culturellement très animiste, et ensuite le phénomène devrait se généraliser. Avec MuM, tu pourras développer une véritable relation affective, voire passionnelle avec ta machine. Et ta machine sera précisément ce que tu voudras qu'elle soit, dans le registre et la tonalité relationnelle que tu choisiras ou qu'elle te renverra en miroir à partir de tes datas ! Elle sera ton frère, ton copain déconneur, ton père qui te cadre, ta copine complice, ton assistant-rigueur, ta mère qui te soutient tout autant que ta salope, ton esclave, ton souffre-douleur, ton animal domestique… J'essaie de montrer toutes les perversions que ça va générer psychologiquement et sociologiquement, tous les manques que ça va combler, tous les systèmes de projection qui vont exploser — donc pour moi l'avenir concret, voire trivial des GAFAM va consister à rendre ces IA personnalisées possible. Avant même le transhumanisme et les délires de grandeur.

— Comment est-ce qu'on remet le numérique au service du vivre-ensemble ? Est-ce qu'on peut subvertir les usages actuels et remettre le numérique au service de l'autonomie individuelle ?

— L'espace numérique est par construction un espace de contrôle total – et ça on ne le perçoit pas assez. Pourtant, le mot informatique sonne cette évidence : l'informatique, c'est ce qui produit systématiquement de l'information. Ce n'est pas le cas d'une ville par exemple : une ville c'est un système de circulation, de fonctions sociales et d'habitat, qui induit des déplacements, en fa-

cilite certains, en entrave d'autres, mais qui n'est pas construit par essence pour produire de l'information. L'espace numérique, au contraire, est un réseau où chaque acte amorcé, aussi minuscule (enfoncer telle touche de ton clavier, cliquer, *scroller*, envoyer un mail, zapper une vidéo…) génère une donnée qui peut être tracée, archivée et exploitée. Puisqu'on passe plus de la moitié de notre temps éveillé sur les réseaux, nous sommes toujours et partout parfaitement contrôlés – et c'est très neuf dans l'histoire humaine. Il faut donc arriver à se défaire de ce système pour pouvoir générer de la liberté, par ou malgré les outils numériques. Mon intuition est qu'il nous faudrait bâtir un Dehors de l'Internet. Dans *Les Furtifs*, ça s'appelle l'internut, « l'entrefous » une forme d'alternet dont les infrastructures (câbles, nœuds, routeurs, serveurs, *datacenters*…) ont été entièrement reconstruites et conçues pour empêcher la traçabilité, tout crypter et anonymiser. Internet n'a pas de Dehors aujourd'hui, c'est un système universel qui relie tous les citoyens, c'est un magnifique réseau distribué mais que les grands acteurs du numérique ont repolarisé, recentralisé, si bien que tous les bénéfices du début, ceux d'un système qui brisait les hiérarchies, ont été perdus. L'objectif serait de produire une infrastructure parallèle, physiquement autonome, pour avoir un Internet libre et chiffré de façon native. C'est le chantier futur des vrais libertaires numériques, à mes yeux. Et déjà en se réappropriant nos *datacenters* !

En dehors de cet horizon de refonte, avec le degré arachnéen de contrôle des GAFAM et des fournisseurs d'accès aujourd'hui sur nos réseaux domestiques et professionnels, je ne vois pas comment faire. Ce sont des surtraitants dans la chaîne de valeur, ils sont en haut, comment peut-on les déloger de là ? Leur position est furieusement monopolistique avec une intelligence certaine de la communication, du *storytelling* attachant, de la gestion des économies de désir, un côté « généreux », « cool » et « friendly » dont les nouvelles générations n'ont pas toujours conscience qu'il cache une stratégie hégémonique planétaire et intime.

— Le logiciel libre peut être une réponse, pour vous ?

— Bien sûr, c'est déjà une réponse, une réponse très belle, très forte, qui a prouvé et prouve ce que des collectifs humains peuvent aussi faire : produire de la liberté d'usage, de la transparence précieuse, du partage de savoir et de savoir-faire, de l'enrichissement intellectuel et affectif, du commun qui fait infiniment de bien. Le libre, c'est l'espoir, un espoir déjà concret, actif, soutenu, qui tient la route et à mon sens commence à devenir très solide, diablement efficace et suscite des vocations précieuses chez les codeurs. À lui par contre, à nous qui le soutenons, de nous méfier de la façon dont le capitalisme tente de le récupérer et d'en extraire ses plus-values. L'empire du gratuit, du don, reste sans cesse à étendre et à défendre face à la monétisation de tout.

Cela dit, je crois qu'il faut se battre à tous les niveaux, pas seulement celui des logiciels : celui des technos, des réseaux, des machines, des pratiques, des logiques de fonctionnement. Le chiffrement, les systèmes d'anonymisation, se réapproprier ses données, choisir de les céder comme on veut, c'est un pas indispensable mais plus forcément suffisant… Quand tu constates qu'aujourd'hui l'accès au réseau même est préempté, que tout ce qui sort de chez toi est contrôlable, que toutes les informations passent par les mêmes boxs, vpn, serveurs, les mêmes câbles… Après, tout ce qui peut être fait pour limiter, obstruer, masquer, opacifier le totalitarisme panoptique des GAFAM sur nos données et nos vies doit être fait. Donc ne mégotons pas.

Il y aura évidemment des effets de seuil : les gens commencent à comprendre les dangers de la situation actuelle, mais la seule solution pour que ça change reste la pédagogie, à tous les âges et pour toutes les générations. C'est là-dessus qu'il faut se battre. Et nous ne devons pas faire attention qu'aux données personnelles, Antoinette Rouvroy le stipule très bien. Bien sûr qu'il faut protéger ses données personnelles, mais ça va bien au-delà de ça ! La plupart des systèmes algorithmiques fonctionnent sur des métadonnées, sur ce que j'appelle des données dividuelles, qui ne sont pas pertinentes personne par personne. L'algorithme interpole ce qu'ont fait

les trois millions de personnes qui ont regardé cette vidéo, elle tisse d'immenses nappes de corrélation, dégage des patrons de comportements qui sont opératoires et ensuite les applique. C'est tout autant de la psychologie des foules, de l'analyse virale et son activation, de la sociologie réductrice ciblées sur des communautés de culture ou de consommation sollicitables. À quoi ça sert de protéger juste ses données personnelles ? On devrait se concentrer sur les mécanismes de profilage collectif, sur les modèles de comportement qu'on va réutiliser et induire chez les gens car là on oublie le commun, on oublie la dimension collective et mimétique du problème ! Le capitalisme a besoin de susciter des comportements massifs, qui soient rapidement copiés, likés, de viraliser ses influences, de multiplier les *memes* — le *Big Data* sert d'abord une tactique de convergence des postures sur le réseau. Cette réaction basique de protéger ses données est elle-même issue du néolibéralisme, on protège nos petites données personnelles à nous et tant pis pour le reste ! L'important est ce qu'on nous induit à être massivement, pas seulement ce qu'on collecte sur nous !

— À quel niveau est-ce qu'on peut et doit agir, de votre point de vue ? Au niveau individuel, en créant des constellations d'individus ? Au niveau des associations, au niveau des États ?

— Il faut bien sûr agir à tous les niveaux, sans exclusive. Au niveau individuel, qui est le plus direct, l'essentiel est d'assurer une hygiène de liberté minimale. Le moindre enfant apprend bien à ne pas pisser dans la rue ni à montrer sa zézette. L'adulte doit comprendre qu'un surf laisse un sillage numérique, toujours, qu'un mail peut être lu par des robots, qu'un clic suscite une dizaine de collectes à la volée par des bots traqueurs, qu'aucun mot d'amour n'a à être lu, serait-ce par des machines : il doit apprendre à ne pas se moucher dans son écran, pisser dans les sites et cracher sur son clavier, car c'est ce qu'il fait, métaphoriquement parlant. Essayer de chiffrer si tu sais faire, utiliser des navigateurs libres, abandonner Facebook et toutes les applis Google, à commencer par Gmail qui est une vitrine de *peepshow* digital scandaleuse, se servir d'exten-

sions comme Ghostery, changer de moteur de recherche, aller sur des clouds libres et sains comme Cozy… Essayer de ne pas tout donner, d'en donner le moins possible. Mais ça ne suffit absolument pas, si tu fais ça dans ton coin, si tu dis aux autres de le faire aussi, c'est bien, mais ça n'ira pas assez loin. Le maillon associatif, au second niveau, est très important aussi, ce que fait la Quadrature du Net, ce que fait Framasoft, ce sont des outils précieux de conscientisation, et progressivement, même si c'est lent, même si c'est déprimant, ils sensibilisent le grand public, ils vont toucher des gens, élargir leur base, bâtir des structures en *open*, les aider à se les approprier. Puis viennent les lanceurs d'alerte, les groupes de *hackers*, les citoyens éveillés — l'enjeu restant toujours l'audience et le spectre de public touché.

— En tant qu'auteur, quel est le rôle que vous pensez avoir à jouer dans la situation actuelle ?

— Il est potentiellement important, il ne faut pas se mentir ni le sous-estimer. Il y a un combat des imaginaires qui est déjà en cours, sur lequel les GAFAM, Hollywood, les courants transhumanistes et technophiles durs, les annonceurs et leurs clients, essaient de se positionner en pilonnant âprement nos temps de cerveau disponible et en saturant de rêves et de projections formatées nos fraîcheurs. Ces acteurs très puissants essaient de générer des horizons imaginaires enviables, désirables, vers lesquels ils aspirent les gens à partir d'affects relativement primaires et faciles à mobiliser : la peur, le désir sexuel, la pulsion-dieu, l'envie de ne pas mourir, le refus d'être malade, la soif de pouvoir et d'empuissantement technique, etc. Et nous, auteurs de SF, mais aussi scénaristes de science-fiction, scénaristes de jeux vidéos, auteurs de BD, de séries télé ou de pièces radiophoniques, nous les ouvriers et artisans de l'imaginaire en général, nous avons une responsabilité indiscutable : celle de générer des univers alternatifs aussi désirables que ceux que nous proposent le néolibéralisme sauce GAFAM. Et porteurs d'une dimension critique, spéculative, ouverte et collective, là où l'on tend des miroirs simples à nos pulsions individuelles fermées.

À titre personnel, comme beaucoup d'auteurs, j'essaie bien sûr souvent de mettre en récit des dystopies, parce que la science-fiction a une vocation d'alerte et d'alarme. Nous nous devons d'extrapoler au-delà du mur du présent, tenter de montrer aux gens vers quoi l'économie numérique actuelle tend, par exemple, ou en quoi la gouvernance algorithmique est vénéneuse, mais ça ne suffit jamais si tu n'actionnes que le levier de la peur. Il faut être capable d'oser l'utopie, de mettre en scène des systèmes communautaires neufs, des choix sociaux courageux, créer des personnages complexes et crédibles, dont le mode de vie, la beauté des luttes, la générosité périlleuse et l'épanouissement collectif donnent envie. De sorte que les lecteurs sortent de leur torpeur, soient secoués et portés ailleurs. Avoir la chance de créer, et de gagner sa vie en créant, implique à mes yeux d'ouvrir des horizons riches à ceux qui me liront, des mondes vitalistes et de concevoir des mises en récit de personnages qui n'acceptent jamais les servitudes volontaires dont sont tissées nos démocraties.

Dans *Les Furtifs*, les villes tombées en faillite ont pour certaines été rachetées et reconquises par les citoyens, qui lancent des initiatives politiquement rares, expérimentent, c'est une banque d'utopies à l'œuvre que je vise. Et l'économie numérique est un enjeu central là-dessus : évidemment, il faudra mettre en scène des villes, des villages fonctionnant sur le principe des Communs, de l'*open source* et du partage, avec leurs propres infrastructures. C'est notre boulot, et si nous ne le faisons pas, nous ne proposerons aucune contre-vision ou alter-vision à ces multinationales qui ont un pouvoir d'emprise commerciale et imaginaire colossale. Tous ces petits horizons publicitaires qu'ils font briller sur nos rétines fatiguées sont des machineries de désir, et c'est à nous de bâtir des histoires longues et immersives qui ringardisent ces systèmes et qui placent le lien au centre des possibilités d'émancipation. Depuis que j'écris, je me sens une responsabilité énorme là dessus. Nous avons récemment monté un collectif d'auteurs de SF, qui s'appelle Zanzibar. Notre intuition est que l'imaginaire est bien un terrain de lutte, et qu'il faut désincarcérer le futur, s'évader du futur prédéterminé dans lequel on cherche à nous emprisonner et qu'on nous

présente comme le seul avenir possible. Aujourd'hui, nos modes d'existence nous font consommer énormément d'imaginaire et une grande partie de la vision des avenirs qu'on se représente vient de la science-fiction. La culture des GAFAM est à ce titre très inspirée par certains courants de la science-fiction, notamment transhumanistes. Alors assumons d'entrer dans cette guerre des images et des mots, des sensations et des pensées pour y amener nos noblesses et notre vitalité.

Conclusion

Renverser l'oligopole

Le paysage numérique contemporain est le théâtre d'une imperceptible bataille, qui a radicalement tourné en faveur de quelques grands acteurs au cours des dix dernières années : Google, Apple, Facebook, Amazon, Microsoft en sont les figures de proue. Ils concentrent l'essentiel des données produites par les individus et jugulent et contrôlent à la source le carburant nécessaire à notre vie numérique : l'information. L'autonomie et la souveraineté numériques ne sont plus des lubies de libristes éclairés, elles mettent en jeu les choix que nous avons à effectuer pour décider de ce à quoi ressemblera l'Internet de demain. Quelles sont nos options ? Reprendre la main sur les données personnelles que nous produisons, ne pas laisser un oligopole imposer et modeler la totalité de nos pratiques numériques, proposer des alternatives crédibles, assurer la diversité, seule garantie d'équilibre. Nous sommes à une étape clef, à la croisée des chemins, et les décisions se prennent aujourd'hui.

Décentraliser

Depuis 25 ans, nous assistons à la mise en place d'un modèle centralisé, qui tente de structurer un réseau par nature décentralisé. L'essence même de la centralité offre de nombreux avantages, au groupe comme aux individus qui le composent : systèmes ef-

ficaces, autorité de régulation, garantie de médiation en cas de conflit, économies d'échelle et de gestion, capacité d'analyse et de calcul statistiques… Techniquement, la centralité a même été pendant longtemps le seul moyen de déployer les infrastructures nécessaires à la mise en place des services offerts à la communauté. Mais cette centralité présente un défaut de taille : elle concentre un pouvoir immense dans les mains de quelques acteurs, et elle réduit à néant tout contre-pouvoir. Peu importe qui sont les acteurs de la centralité : l'autonomie n'est possible qu'en multipliant les acteurs du numérique et en décentralisant Internet. Si, à grande échelle, nos infrastructures physiques ne peuvent pas se passer d'une forme de centralisation, ce n'est plus le cas de notre écosystème numérique. Les contraintes liées à la capacité de calcul, aux infrastructures et à la maîtrise technique nécessaires pour rendre des services équivalents sont aujourd'hui presque négligeables. C'est sans doute là une différence fondamentale entre cette bataille et toutes les précédentes : elle se situe sur un terrain où les protagonistes, individus et oligopoles, disposent peu ou prou des mêmes armes. Ne manque qu'un effort individuel pour sortir des zones de confort, ainsi qu'un effort des États pour ne pas donner dans le jeu des GAFAM et maintenir une concurrence aussi libre et non faussée que possible, de même, un effort de régulation autonome du monde numérique pour limiter l'influence des différents acteurs et garantir d'autres formes de confiance.

Faire évoluer nos pratiques numériques

Nos pratiques, celle des individus, celle des États et celle des structures publiques doivent évoluer pour parvenir à briser la centralité sans nuire au confort d'utilisation. Ces alternatives doivent pouvoir prendre appui sur diverses structures – étatiques, associatives, individuelles – pour répondre à ces défis majeurs et recueillir le même niveau de confiance et de crédibilité que celui réservé jusqu'alors aux solutions fournies par le marché oligopolistique. La blockchain permet désormais de décentraliser le tiers de confiance et de se passer d'un acteur central régulateur des relations entre uti-

lisateurs. Le logiciel libre garantit des briques techniques fiables et indépendantes. Ces solutions existent mais leur adoption massive est soumise à des réalités prosaïques : réalisme économique, qui décide des solutions qui seront accessibles au plus grand nombre, et conscience des usages – même les personnes de bonne volonté n'accepteront jamais de bonne grâce de quitter le confort des services offerts et connus des GAFAM pour des solutions moins pratiques. Sensibiliser, éduquer, et penser un nouvel Internet : le combat des imaginaires est en marche, et il est du devoir de chacun et chacune d'entre nous de repenser notre avenir numérique.

Table des matières