Mathieu Labonde
Lou Malhuret
Benoît Piédallu
Axel Simon

INTERNET ET LIBERTÉS

15 ANS DE COMBAT DE LA QUADRATURE DU NET

Vuibert

Mathieu Labonde
Lou Malhuret
Benoît Piédallu
Axel Simon

15 ANS DE COMBAT DE LA QUADRATURE DU NET

Vuibert

Mathieu Labonde
Lou Malhuret
Benoît Piédallu
Axel Simon

INTERNET ET LIBERTÉS

15 ANS DE COMBAT DE LA QUADRATURE DU NET

Vuibert

À Philippe Aigrain, cofondateur historique de La Quadrature du Net, informaticien et humaniste, militant infatigable, chercheur et intellectuel, qui a œuvré toute sa vie pour que l'on continue à s'indigner au bénéfice du plus grand nombre.

SOMMAIRE

INTRODUCTION

La Quadrature du Net défend, depuis sa création, les libertés fondamentales dans l'espace numérique.

Mais qu'est-ce que cela veut dire, au juste ?

Nous ne défendons pas les « libertés numériques » ou les *digital rights* ; les droits et les libertés ne sont pas différents qu'on soit dans un espace numérique ou un espace physique. La Poste n'a pas plus de légitimité à ouvrir notre courrier que Google à fouiller dans le contenu de nos messages. La censure arbitraire ne doit pas s'abattre davantage sur un texte publié sur Facebook que sur un article dans un journal.

Si les libertés sont « fondamentales », c'est qu'elles précèdent le reste et doivent être défendues en tout temps et en tout lieu. Au tournant du millénaire, nous avons été un certain nombre à constater que dès qu'il s'agit des « nouvelles technologies de l'information et de la communication », un effet d'émerveillement se produit. Un effet tel qu'il peut donner l'illusion que les atteintes aux libertés en ligne ne seraient pas dangereuses, ne compteraient pas. Rien n'est plus faux, il n'y a pas de distinction intrinsèque à faire que l'on soit d'un côté ou de l'autre du clavier, de l'écran, en ligne ou hors ligne : les libertés fondamentales, telles que la vie privée, la liberté d'expression, d'association ou le droit à un procès équitable, demandent la même exigence pour rester entières, valides et protectrices.

Au début de la Quadrature, il y avait une idée, une utopie : l'horizontalité apportée par Internet permettrait à chacune et à chacun de

se saisir des outils, de créer, de réutiliser, de contribuer, de bâtir un monde à l'image de toutes et de tous. Et, portant cette idée, un enthousiasme : humour geek, mèmes, montages, détournements, petits bouts de codes développés sur un coin de table pour amuser la galerie ou, mieux, améliorer un peu le monde, déjà, à son échelle.

Au fil des ans, nous avons lutté pour défendre ces libertés, auprès de la classe politique – principalement des députés et eurodéputés – et dans les médias, tentant d'expliquer quand il le fallait les risques posés, mais aussi les possibilités offertes par le numérique. Nous avons lutté avec et grâce à des gens comme vous et nous, qui se sont saisis de ces sujets pour parfois ne plus jamais les lâcher et en devenir experts. Plaidoyer citoyen dans les couloirs du Parlement, puis contentieux contre l'État, la Quadrature s'est rêvée en David contre Goliath, car Internet nous avait appris que la connaissance était à portée de clic, que tout pouvait s'apprendre, et il nous avait donné faim de tout savoir, de tout faire par nous-mêmes.

Aux premiers jours, tout était possible, car nous avions conscience d'être de celles et ceux qui comprennent les enjeux de la technologie dans une société démocratique. Les décisions politiques absurdes seraient forcément gommées lorsque nous les pointerions du doigt devant les parlementaires, dans les médias ou, au pire, devant la justice. La réalité était plus sombre.

Car ce réseau Internet qui nous a rassemblés et nous a profondément changés n'est pas qu'un vecteur de connaissance et de culture. Le numérique charrie aussi la publicité ciblée et la surveillance généralisée, la concentration du pouvoir et la censure, la reproduction et le renforcement des inégalités. Dans un monde où l'information est pouvoir, sa concentration met en danger l'exercice des droits démocratiques, et les décisions hostiles aux libertés fondamentales sont, dans nombre de cas, bel et bien volontaires.

Quinze ans après la création de la Quadrature, nous choisissons de continuer à opérer dans cet espace à la croisée de la technique, du droit et de la politique. Un champ parfois peu accessible, souvent mis à mal par

des intérêts privés ou des gouvernements peu regardants, mais tellement utile et nécessaire.

Nous avons été qualifiés de gauchistes, de libéraux, d'idéalistes, de naïfs…

Nous avons été qualifiés de citoyennistes, et cela nous convient très bien.

Nous avons été qualifiés de radicaux, et cela nous convient très bien.

Nous avons été qualifiés de lobbyistes, mais si nous en sommes, c'est d'un type bien particulier : nous ne défendons pas d'intérêts particuliers. Nous défendons une vision particulière de l'intérêt général. Nous faisons du plaidoyer, pas du lobbying.

Nous sommes de ceux qui refusent toujours le terme de « propriété intellectuelle », créé de toutes pièces à la fin des années 1960 par certains acteurs privés afin de pouvoir utiliser le champ lexical du vol pour décrire leurs adversaires.

Nous soupirons devant l'usage du terme « contenu » pour décrire les œuvres d'art et les créations de l'esprit, la créativité du genre humain réduite à ce qu'on peut mettre dans une boîte, avec l'idée que le contenant serait ce qui compte.

Nous aspirons à un monde où les valeurs originelles d'Internet – partage, ouverture, décentralisation – seraient de nouveau primordiales et sources d'émancipation.

Ce livre raconte l'histoire d'une organisation qui rêvait d'un Internet émancipateur, un idéal mis à mal par les gouvernements et les multinationales dès que ces derniers ont pris conscience du pouvoir financier et sécuritaire que procuraient ces outils. Cette histoire est racontée par quatre militants qui en ont vécu les origines, les utopies et les principes de réalité, les désillusions et les espoirs.

PARTIE : DÉFENDRE INTERNET
(-)

1. AUX ORIGINES DE LA LUTTE

La technique et l'informatique sont fortement liées aux questions sociales. Augmentation de la productivité, déplacement ou confirmation de pouvoir, gains financiers… : elles ont entraîné dans l'histoire nombre de bouleversements fondamentaux, avec leurs lots de résistances et d'opposants. Dès 1811, déjà, en pleine révolution industrielle, alors que la production textile se mécanisait en Angleterre, les artisans tondeurs et tricoteurs, dits luddites, se révoltaient contre les manufacturiers en organisant la destruction délibérée des machines. Plus proche de nous, en France, au début des années 1980, le Comité pour la liquidation ou la destruction des ordinateurs (CLODO) s'attaquait aux outils informatiques que ses membres, anonymes, considéraient comme des instruments de répression et de contrôle, en incendiant des bureaux d'entreprises. En Allemagne, le Chaos Computer Club (ou CCC), rassemblement de hackers, parvint à politiser, dès 1984, les sujets numériques (vie privée, cybersécurité…) auprès du gouvernement. Quelle que soit leur virulence, ces mouvements sont toujours issus des rangs des créateurs et des premiers utilisateurs des outils concernés, qui cherchent naturellement à en influencer l'usage.

Le développement continu des technologies impose une adaptation régulière des méthodes et des outils utilisés par leurs opposants. Si les premiers groupes évoqués ci-dessus risquaient la peine de mort, la société reconnaît désormais la légitimité d'un certain niveau de contestation. Il faut dire que la numérisation du monde a transformé la nature de leur

combat : que détruire, lorsque les machines peuvent se trouver n'importe où sur la planète, et que leur contenu est reproduit à l'infini, rendant la suppression d'une donnée pratiquement impossible ?

Le CCC, par exemple, s'est constitué alors qu'Internet était encore confidentiel, aux mains d'une minorité de personnes et d'organisations (entreprises, États…). Dix ans après naissait le Web, bientôt démocratisé et popularisé grâce à l'ADSL et à sa connexion constante, aux forfaits sans limite de consommation de données, et aux smartphones qui actent le passage à la mobilité. Constitution de monopoles géants, numérisation des services publics… : le contexte a évolué à vitesse grand V, tout comme les risques dus au numérique dans son ensemble. Aujourd'hui, ce ne sont plus seulement les travailleurs et les spécialistes qui sont touchés, mais toute la société.

INTERNET : LES PREMIERS PAS

Quand, à la fin des années 1990, Internet commence à percer aux dépens du Minitel, de nouvelles questions se posent : extraterritorialité, responsabilité juridique des acteurs techniques, service public de l'accès au réseau, origine et choix de l'investissement pour cet accès…

Ces réflexions quant au « terrain politique » d'Internet rappellent celles qui, vingt ans plus tôt, ont émergé au lancement des radios libres : quel droit de diffusion ? Quels droits d'auteur ? Quid de l'anonymat ? Comment transformer un outil d'émancipation en un système majoritairement commercial ?… Dans les années 1970, de nombreuses personnes testèrent cet espace de liberté radiophonique inédit, avant de rapidement déchanter lorsque le financement publicitaire fit irruption.

Lancé en 1980 par les PTT, service public, le Minitel proposait des services relativement contrôlés. Leur mise à disposition était soumise à autorisation ministérielle, le paiement pour y accéder apparaissait directement sur la facture téléphonique. France Télécom y prélevait sa part, et toutes les communications passaient par son réseau.

Malgré toutes ces contraintes, c'est à partir d'un Minitel que Laurent Chemla, entrepreneur, pirata en 1986 le serveur de Café Grand-Mère, et se retrouva inculpé pour « vol d'énergie » – le délit de piratage informatique n'existant pas encore[1]. De ce premier contact avec le droit naissent les premières réflexions sur la manière dont ce dernier s'articule avec les réseaux et l'informatique. Chemla participe d'ailleurs à la création de l'Association des utilisateurs d'Internet (AUI), fin 1995[2]. Ses objectifs, alors que la majorité de la population n'a pas encore entendu parler de la Toile, sont déjà de défendre et de chercher à obtenir des libertés sur Internet.

Fin 1995, le gouvernement Juppé tente de faire passer une réforme des retraites supprimant les régimes spéciaux. Les conséquences sociales ne se font pas attendre : une grève géante est déclenchée dans tout le pays. Pendant un mois, l'Île-de-France est totalement bloquée par l'absence de trains et de métros. La Poste suit largement le mouvement. À cette époque, toute la communication passe par le courrier. Les postiers manquent ainsi, en ne le distribuant plus, d'étouffer leur propre mouvement contestataire. Internet est déjà disponible, mais très peu connu du grand public. Les militants se voient donc contraints d'apprendre à échanger des e-mails, à créer et à animer des forums, et même à utiliser les *newsgroups*, des forums de discussion spécialisés organisés hiérarchiquement.

Au beau milieu des années 1990, celles et ceux qui utilisent Internet l'imaginent comme un espace de libertés tel qu'il n'en a jamais existé avant. Un espace dans lequel, pour la première fois, les individus peuvent vraiment jouir d'une réelle liberté d'expression. L'imprimerie a permis au peuple de lire, Internet va-t-il lui permettre d'écrire ? Quoi qu'il en soit, le monde politique et les lobbies de la propriété intellectuelle voient d'un très mauvais œil l'accès toujours plus étendu du grand public à ce réseau de communication sur lequel ils n'ont que très peu de contrôle…

QUAND LA LÉGISLATION S'EN MÊLE

En 1996 est voté aux États-Unis le *Telecommunications Act* (la loi sur les télécommunications). Parallèlement, un traité sur le droit d'auteur dans l'environnement numérique est signé par plusieurs dizaines de pays sous l'égide de l'Organisation mondiale de la propriété intellectuelle (OMPI), organisme des Nations unies[3].

Le premier provoque une vive réaction parmi les intellectuels américains, à l'instar de John Perry Barlow, parolier de l'influent groupe de rock américain Grateful Dead et cofondateur de l'Electronic Frontier Foundation, qui rédige sa « Déclaration d'indépendance du cyberespace »[4], au forum de Davos. Ce texte lyrique, épique, témoigne de l'utopie, du rêve qu'ont les geeks de l'époque d'un Internet totalement autonome. Derrière cette première pierre, la volonté est d'affirmer que les gouvernements ne peuvent prétendre à s'approprier la Toile.

Le second traité, plus technique, entraîne quant à lui la levée de boucliers de la Free Software Foundation (FSF), une organisation américaine promouvant les logiciels libres, créée par Richard Stallman. Elle se dresse contre ce qui deviendra en 1998 le *Digital Millennium Copyright Act* (DMCA). Ce texte – dont on entend encore parler aujourd'hui à travers les fameuses « requêtes DMCA », que reçoivent quotidiennement des hébergeurs de contenus pour leur demander de supprimer ceux considérés comme violant la propriété intellectuelle – vise notamment à entériner et à protéger les *Digital Rights Management* (DRM). Les DRM sont des outils de contrôle du contenu. Ils limitent l'usage des œuvres légalement acquises par les acheteurs selon le bon vouloir de leur propriétaire. Imaginez un livre qui disparaît définitivement de votre étagère une fois qu'il a été lu trois fois ! Dans le droit européen, ces traités seront transcrits au sein de la directive EUCD 2001/29/CE.

Mais revenons en France. En 1996, toujours sous le gouvernement Juppé, on débat à l'Assemblée nationale de la loi de réglementation des télécommunications. L'amendement Fillon est présenté. Alors ministre

délégué à la Poste, aux Télécommunications et à l'Espace, il promet de prendre en compte les avis des professionnels du secteur du numérique, et demande à son cabinet de commander un rapport. Dans le cadre de sa rédaction est lancée la première consultation du public en ligne d'initiative gouvernementale en France. Elle est organisée par l'Internet Society France, branche française tout juste créée d'une association internationale visant à promouvoir le réseau Internet. Une belle idée en théorie, mais un coup d'épée dans l'eau, car en réalité l'amendement Fillon est déposé le jour même de l'ouverture de la fameuse consultation !

François Fillon souhaite, avec ce texte, transférer la responsabilité des contenus disponibles sur Internet au Comité supérieur de la télématique, émanation du Conseil supérieur de l'audiovisuel (CSA). Ce comité aurait pour mission de rendre des « recommandations » sur les services accessibles via un fournisseur d'accès à Internet (dit FAI, un *access provider*, selon les termes de François Fillon). Les FAI deviendraient donc pénalement responsables de la fourniture d'un service non validé. La responsabilité des contenus leur serait alors transférée et ils se retrouveraient de fait à censurer Internet pour ne livrer qu'une série de services autorisés par l'administration. La tentative de transformation d'Internet en réseau minitel de seconde génération fait rire les connaisseurs du réseau. Malgré les tentatives de François Fillon, qui va jusqu'à défendre son amendement sur… Usenet[5], un réseau de forums populaire à l'époque parmi les utilisateurs, le Conseil constitutionnel sonne la fin de la récréation et censure les dispositions imposant aux FAI une responsabilité sur les contenus circulant sur leur réseau[6].

Aux débuts d'Internet, les FAI ne sont pas les seuls dans le viseur des autorités. L'« affaire Estelle Hallyday », en 1998, lance les hostilités sur le rôle des hébergeurs. Des photos dénudées de la mannequin, issues de la presse people, sont scannées puis déposées sur un site Web qui se trouve sur les serveurs de l'hébergeur (gratuit) AlternB. Une plainte en référé est alors déposée contre ce dernier, qui est finalement condamné à

verser des dommages et intérêts à la plaignante, pour de sulfureux clichés publiés sur… un des 45 000 sites environ hébergés sur ses serveurs.

Imaginez que La Poste soit tenue pour responsable du contenu des lettres et des colis qu'elle transporte. Elle se verrait obligée de les ouvrir tous pour prendre la décision de les transporter ou non, et, bien sûr, elle en laisserait une bonne partie sur le carreau ! Certains contenus (la pédopornographie, par exemple) seraient faciles à détecter, mais pour tout un tas d'autres (Cette poudre, est-ce de la farine ou de l'anthrax ? Cette arme est-elle factice ?), ce serait bien plus compliqué. De la même manière, rendre responsables les hébergeurs des contenus déposés sur leurs serveurs revient à donner à des opérateurs privés un rôle d'enquêteurs et de justiciers.

La condamnation de Valentin Lacambre, président d'AlternB, ouvre une brèche importante permettant à n'importe qui d'attaquer un hébergeur pour les données qu'il stocke. Très médiatisée, elle instaure un précédent juridique de censure, et politise toute une génération qui comprend que l'ignorance technique du pouvoir judiciaire met en danger ce nouvel outil prometteur qu'est Internet.

DROITS D'AUTEUR *VS* PARTAGE

Les ingénieurs travaillant sur la technologie Internet ne sont pas les seuls à être confrontés aux décisions politiques qui réglementent leur domaine de compétence contre leurs intérêts.

En mai 2004, ce sont les développeurs de logiciels qui sont à leur tour menacés. Le Conseil européen (qui réunit les chefs d'États et de gouvernements des États membres) vote un texte en contradiction avec les positions habituelles du Parlement européen sur les brevets logiciels. Il autorise les entreprises à protéger des morceaux de code informatique. Les partisans de cette mesure affirment qu'elle poussera à l'innovation : une personne pouvant protéger sa création prendra selon eux plus de risques que si tout le monde peut la copier. Ses opposants prévoient au

contraire que les grandes entreprises, qui disposent de plus gros moyens, bloqueront l'innovation, en déposant des brevets qui empêcheront tout nouvel entrant de pénétrer le marché du développement informatique.

Cette attaque contre le métier de développeur mobilise toute une communauté qui n'a pourtant pas de culture syndicale[7]. Des relations se nouent, à travers les forums, les événements, les mailing lists, les plus motivés analysent les textes de loi, imaginent des solutions, réfléchissent à des actions…

En 2004, c'est la Fédération Informatique et Libertés, rassemblant des associations (telles Globenet et Acrimed), des ONG (Privacy International) et des particuliers engagés dans la défense de la vie privée et de la liberté d'expression, qui monte au front et s'élève contre la loi pour la confiance dans l'économie numérique, abrégée en LCEN[8].

Les mesures s'enchaînent en France et, à la rentrée 2005, est présenté le projet de loi sur le droit d'auteur et les droits voisins dans la société de l'information, surnommé DADVSI, visant à renforcer la lutte contre la contrefaçon sur Internet. Il est la transposition de la directive européenne EUCD 2001/29/CE « sur l'harmonisation de certains aspects du droit d'auteur et des droits voisins dans la société de l'information ». Il en reprend les grandes lignes, soit : la mise en place de dispositifs de lutte contre le partage d'œuvres sur Internet et l'interdiction de diffusion de logiciels permettant de casser les dispositifs techniques de protection du droit d'auteur (les DRM).

Ces deux propositions vont à l'encontre de l'idée que l'on se fait à l'époque de l'usage d'Internet : une ouverture sur le monde, des échanges, des découvertes, un accès illimité à la connaissance et à la culture – comme en témoigne la mobilisation des artistes en faveur de la « licence globale[9] ».

Elles montrent à quel point le pouvoir politique ambitionne de changer le visage du réseau pour le mettre à disposition de la consommation, et non de l'échange de culture. C'est une remise en cause des promesses qu'il apporte pourtant, et sur lesquelles les fournisseurs

d'accès, France Télécom y compris, surfent pour vendre leurs abonnements.

Le 2 décembre 2005, une pétition est lancée par Loïc Dachary, fondateur de la Free Software Foundation France (FSF France), contre ce projet de loi DADVSI. Elle recueille les signatures de « 173 628 particuliers et près de 1 000 organisations – dont plus de 230 entreprises menacées », selon le site Web EUCD.info, ayant pour but d'informer les internautes sur les conséquences de la directive EUCD et sa transposition dans le droit français. Cette pétition en ligne, qui est la première en France à dépasser les 100 000 signatures, prouve que quelques militants peuvent parvenir à mobiliser l'opinion sur des sujets pourtant relativement techniques. En parallèle, certains d'entre eux entrent en contact avec des députés et des sénateurs. Il en est, parmi ces derniers, qui tentent sincèrement de comprendre les enjeux et convient des spécialistes du numérique pour se faire expliquer les conséquences du texte DADVSI. Ce type d'échange perdurera lors des débats sur la loi Hadopi et bien après.

Christophe Espern, membre de la FSF France, qui a rapidement pris les rênes de l'initiative EUCD.info, cherche du soutien. Quand Jérémie Zimmermann, administrateur de l'April, une association qui défend les logiciels libres, apprend l'existence de cette initiative, il décide de lui apporter son aide pour cette campagne. La stratégie est alors fondée sur une guérilla législative visant à faire admettre aux députés deux idées principales : le bien-fondé de l'usage du logiciel libre, et l'obligation d'interopérabilité des logiciels.

Ensemble, ils mobilisent d'autres militants qui tentent de diffuser plus largement la pétition et de faire parler d'elle dans les médias, sortent des statistiques, rédigent des discours qui sont lus dans l'hémicycle par des parlementaires convaincus de la légitimité de ces propositions, ou encore proposent par leur truchement des amendements – pour certains adoptés en séance. Malgré des revirements au Sénat et face au Conseil constitutionnel, ils arrivent à imposer dans le texte DADVSI l'obligation d'interopérabilité, qui va permettre, malgré les DRM, de pouvoir lire des

fichiers protégés avec n'importe quel logiciel. Une petite bombe, qui est prévue pour tuer le principe même des verrous techniques.

Le bilan de cette campagne est mi-figue mi-raisin. Quelques belles victoires arrachées (bien qu'elles ne soient valables qu'en France), dont celle d'avoir forcé la tenue d'un vrai débat dans l'hémicycle sur le logiciel libre et les limites du droit d'auteur, mais les participants sont exsangues et ont travaillé des mois sans aucun revenu. Ils se sont toutefois fait connaître du public, à travers les forums et les médias, se constituant au passage un fichier de presse, et une base de soutiens solides qui leur sera bien utile pour la suite.

NAISSANCE DE LA QUADRATURE DU NET

En 2007, Benjamin Bayart coorganise les Rencontres mondiales du logiciel libre (RMLL), à Amiens. Il est alors président de French Data Network (FDN), plus ancien fournisseur d'accès à Internet associatif (FAI), qui a pour devise de pouvoir « faire son Internet soi-même ».

Voyant les services en ligne se concentrer entre les mains de quelques géants, que ce soit pour la recherche en ligne, la rédaction d'e-mails ou tout autre échange d'informations, il présente sa conférence « Internet libre ou Minitel 2.0 ?[10] ». Elle sera un important outil de communication permettant à de nombreuses personnes de prendre conscience que le beau jouet technologique décentralisé est en train d'échapper à ses créateurs, à celles et ceux qui voient toujours en lui un outil d'émancipation des peuples. Par exemple, Orange, la marque issue de France Télécom et qui possède alors de fait un quasi-monopole sur le réseau téléphonique et Internet en France, empêche (techniquement et commercialement) toutes velléités d'émancipation[11]. La vidéo de la conférence enregistrée ce soir-là fera des centaines de milliers de vues, et continue à être diffusée aujourd'hui.

2007 est aussi l'année de l'élection de Nicolas Sarkozy. Très vite, dès le mois de novembre, le nouveau président de la République désigne

Internet comme un ennemi, un territoire à conquérir, à « civiliser[12] ». Il passe ainsi en quelques mois seulement du discours de campagne proposant d'aider les industries culturelles à évoluer sur la Toile[13] à une déclaration de guerre. Denis Olivennes, alors patron de la Fnac, se voit missionné pour produire un rapport sur « Le développement et la protection des œuvres culturelles sur les nouveaux réseaux », qu'il remet à la ministre de la Culture, Christine Albanel. Ce rapport préfigure ce que sera la future loi Hadopi.

En entendant le président, Jérémie Zimmermann et Christophe Espern sont furieux. Ils décident de contre-attaquer en lançant une nouvelle initiative. Mais cette fois, elle n'est pas dédiée à un projet de loi particulier. Le défaut du précédent projet était de porter le nom d'une loi particulière, et donc d'être « jetable » : EUCD.info a disparu une fois la loi DADVSI entérinée. Il faut donc trouver un nom qui traverse les années.

Ce sera « La Quadrature du Net ».

« La quadrature du cercle est le symbole d'un problème qu'on ne peut pas résoudre, alors que, pendant de nombreuses années, beaucoup de gens étaient persuadés du contraire. Les politiques pensent aujourd'hui pouvoir "civiliser Internet", mais ils se heurtent au réel de l'infinie capacité du réseau », explique Jérémie Zimmermann.

Début mars 2008, après plusieurs mois de réflexion, Jérémie Zimmermann et Christophe Espern contactent plusieurs de leurs amis militants pour leur proposer de rejoindre l'association. Il s'agit de Philippe Aigrain, Gérald Sédrati-Dinet et Benjamin Sonntag.

Philippe Aigrain, chercheur en informatique et entrepreneur, a participé à l'aventure des radios libres dans les années 1970, avant d'explorer les potentialités démocratiques d'Internet et de devenir un ardent défenseur des logiciels libres et des biens communs. Ses productions (livres, tribunes) et positions politiques font de lui une figure de la communauté. Gérald Sédrati-Dinet, dit Gibus, est un ingénieur en logiciel libre. Expert des brevets logiciels et de leurs dangers, en particulier du brevet unitaire, il a été le vice-président de la Foundation

for a Free Information Infrastructure (FFII). Benjamin Sonntag est un militant engagé, entrepreneur du Web et du logiciel libre.

Débattant de l'organisation de la toute nouvelle association, tous prennent l'engagement qu'elle soit une force de proposition autant qu'une force d'opposition. Ils souhaitent qu'elle fasse le pont entre l'éthique des logiciels libres, l'éthique des hackers, la connaissance des technologies et des processus politiques et législatifs, et qu'elle aille stopper les processus politiques à la racine, en particulier à Bruxelles.

Les principes fondateurs de La Quadrature du Net

- Se réapproprier collectivement la connaissance, étudier les dossiers, mais en se faisant plaisir.
- Utiliser la technologie et Internet pour aider à l'émancipation du public, en inventant des outils qui améliorent la participation, créent du collectif (on dit aujourd'hui *empowerment* ou « capacitation »).
- Réinventer ses propres pratiques politiques, en se sentant libre de tester de nouvelles approches du militantisme, telles que la guérilla juridico-politique et parlementaire ou le contentieux – soit le fait d'attaquer directement les lois et les décisions politiques devant la juridiction dédiée, même en n'ayant aucune chance de réussite, juste pour communiquer, maintenir la pression, ou même troller les politiques.

La Quadrature du Net reçoit alors, trois mois avant sa présentation en conseil des ministres, de la part d'une source anonyme, la fuite de l'ensemble du projet Hadopi, du nom de l'organisme de régulation qu'il propose de créer : la Haute Autorité pour la diffusion des œuvres et la protection des droits sur Internet. C'est le début du combat fondateur de l'association, son premier dossier. Nous publions donc dès mars 2008 notre premier communiqué de presse signé « La Quadrature du Net »[14].

2. HADOPI, OU L'HISTOIRE D'UN PASSAGE EN FORCE

Après l'envoi de ce premier communiqué de presse de lancement, les choses s'organisent à la Quadrature. Jérémie Zimmermann et Christophe Espern sont à la manœuvre et élaborent les premiers outils de communication : logo, canal IRC, mailing list… Le nom de domaine (laquadrature.net) est déposé quelques semaines plus tard, le 16 mars 2008, par Benjamin Sonntag, nommé à l'infrastructure. Dans la foulée, un wiki est créé.

Dès le début, toutes les communications de la mailing list sont chiffrées. Nous nous appliquons à mettre en œuvre deux principes importants : héberger nos propres services pour profiter de la capacité d'Internet de permettre à tous d'être un morceau de la Toile, et sécuriser les communications entre les bénévoles en utilisant des technologies de chiffrement.

Un financement de 20 000 euros de la Fondation Soros est décroché pour couvrir les déplacements et les dépenses diverses de la Quadrature. Cet argent est donné sans contrepartie, la Fondation Soros acceptant nos conditions de totale indépendance. Quand ce financement passera à 50 000 euros, les cofondateurs poseront la règle des 30 % : un financement ne pourra dépasser 30 % du financement total de l'association, pour éviter une dépendance de fait. La Quadrature n'ayant pas d'existence juridique, Benjamin Bayart propose que la FDN soit destinataire des fonds. Il crée pour ce faire, avec Valentin Lacambre et Arnaud Luquin, une émanation de l'association : FDN² (le Fonds de défense de la

neutralité du Net). C'est cette association qui va recevoir les fonds destinés à la Quadrature, mais aussi prendre en charge l'embauche des salariés.

Le travail quotidien de la Quadrature est pris en charge par Jérémie Zimmermann et Christophe Espern, qui rendent des comptes aux autres membres lors de réunions hebdomadaires et via les canaux de discussion. Les activités sont diverses et, comme à l'époque d'EUCD, ils doivent multiplier les compétences : développement Web, graphisme, rédactionnel, prise de parole, analyse juridique… Ils tiennent à bout de bras, par un engagement militant, une association qui, malgré sa petite taille, a déjà vocation à influencer le débat public.

La fuite du projet de loi précurseur de ce qui deviendra la Hadopi lance la Quadrature dans le combat du droit d'auteur dans le domaine numérique. Ce choix s'inscrit naturellement dans la lignée d'EUCD.info contre la DADVSI, ajoutant à la lutte contre les DRM la sauvegarde de la culture du mème, du remix et du *peer-to-peer*, au sein d'un mouvement général pour la protection de la liberté d'expression.

Le travail de l'association balance entre l'analyse juridique pointue, qui prend de longues heures de lecture, de compréhension et de structuration, la réflexion autour d'idées concrètes et crédibles, et la production de mèmes agrémentant les communiqués de presse. Faire rire, produire du contenu grinçant, devient notre marque de fabrique. Le but : s'attaquer à l'image policée des décideurs qui, le plus souvent, déroulent tranquillement leur argumentaire sans opposition, et proposer une autre lecture de l'histoire face à celle de la *realpolitik* de ceux qui sont au pouvoir.

Pour gagner en visibilité, la Quadrature décide d'investir dans la communication. Nous publions communiqué de presse sur communiqué de presse, répondons à toutes les sollicitations, et veillons particulièrement à notre image dans les médias. La stratégie ne prend pas, seules les publications spécialisées (*PC INpact*, *Numérama* ou quelques autres) reprennent régulièrement nos textes.

LA RIPOSTE GRADUÉE A BON DOS

Depuis quelques mois, à Bruxelles, au Parlement européen, on discute du « paquet Télécom », un ensemble de textes visant à réguler les télécommunications. Il comprend notamment deux propositions de directives-cadres dont l'objectif est d'amender des directives existantes (dont la directive « Vie privée et communications électroniques » [*E-Privacy*]). Chaque texte a son domaine de compétences : l'accès aux moyens de communication électroniques, leur cadre réglementaire, leur statut de service universel, le sort des données à caractère personnel, etc. Ils datent tous du début des années 2000 et doivent déjà être refondus pour répondre à la réalité des nouvelles pratiques. C'est ce à quoi s'attellent les institutions européennes (Parlement, Commission, Conseil et États membres).

En 2008, la France de Nicolas Sarkozy saisit cette occasion pour tenter d'imposer dans ce nouveau « paquet Télécom » une justification européenne de la loi Hadopi et de la « riposte graduée » qu'il a tant de mal à faire passer dans son propre pays. Il s'agit d'autoriser les producteurs de biens culturels à se livrer à des missions de police, et les fournisseurs d'accès à sanctionner les internautes sans passer par l'autorité judiciaire[1]. Un premier vote au Parlement tacle sévèrement le projet en avril[2]. Certains amendements (notamment issu du lobby français du cinéma) prônent l'abaissement du niveau de protection des données personnelles, d'autres visent à légaliser les *spywares* des industries culturelles, à institutionnaliser leur influence, ou à leur permettre de déterminer les technologies sans-fil utilisables demain. Le dernier amendement étudié nie l'existence d'un droit à redistribuer des œuvres du domaine public ou sous licence libre.

Le Parlement européen crée une commission chargée de proposer des solutions pour développer une industrie culturelle sur Internet. Présidée par Viviane Reding, elle confie à Guy Bono, eurodéputé français du Parti socialiste, le soin de rédiger un rapport d'initiative sur « Les industries

culturelles en Europe ». C'est là l'occasion d'une prise de position forte : la coupure de l'accès à Internet est dite disproportionnée en cas de violation du droit d'auteur, car « en contradiction avec les libertés civiques ainsi qu'avec les principes de proportionnalité, d'efficacité et de dissuasion ». Guy Bono ajoute : « La coupure de l'accès à Internet est une sanction aux effets puissants qui pourrait avoir des répercussions graves dans une société où l'accès à Internet est un droit impératif pour l'inclusion sociale. » Le 10 avril 2008, le rapport est adopté de justesse.

Apprenant à l'automne qu'un amendement est déposé au « paquet Télécom » par ce même Guy Bono, sur la base de ce rapport, et conscients de l'importance qu'il aura ensuite dans leur combat contre la Hadopi, Jérémie et Christophe partent à Bruxelles rencontrer des députés européens pour les convaincre de le voter. Le 24 septembre, c'est chose faite : le Parlement européen adopte l'amendement 138 (ou « amendement Bono ») au « paquet Télécom ». C'est un puissant signal envoyé au gouvernement Fillon qui, au sein de sa loi Hadopi, a justement prévu cette coupure de l'accès à Internet… La Quadrature invite alors « le Premier ministre à prendre acte de ce vote et à ne pas déposer devant le Parlement français le projet Olivennes ». Malgré cela, le gouvernement fait la sourde oreille, et la France profite de sa présidence de l'Union au second semestre 2008 pour vite faire retirer cet amendement. La voie se dégage pour la Hadopi[3]…

Les négociations et le travail sur les textes se poursuivent néanmoins. L'amendement est rétabli et de nouveau voté par le Parlement en mai 2009, mais refusé par le Conseil en juin. Pour trancher, un comité de conciliation, composé des ministres de vingt-sept États membres, doit se réunir à partir de septembre 2009. C'est là que la Quadrature tire la sonnette d'alarme, et publie coup sur coup plusieurs articles et plusieurs lettres ouvertes où le thème de la neutralité du Net est absolument central.

Le comité de conciliation achoppe bien entendu sur l'amendement 138, maintenu par le Parlement et refusé par le Conseil. Mais de nouveaux amendements inquiétants se sont invités dans la discussion au

fil des lectures. Dans des argumentaires écrits en anglais (à l'usage des eurodéputés de toutes origines, et des partenaires militants dans les autres pays de l'Union), la Quadrature redoute notamment ceux des grands opérateurs américains, dont AT&T. Ces opérateurs ont obtenu que figurent dans le texte des formulations qui laissent aux opérateurs la possibilité unilatérale de « limiter l'accès et/ou l'usage de certains services et applications », ou de ralentir le trafic à volonté.

Le vote final sur le « paquet Télécom » du 24 novembre 2009 ne satisfait ainsi pas du tout l'association. Le communiqué publié le jour même est un aveu de déception : le texte ne consacre pas formellement la neutralité du Net dans l'Union européenne, la version finale est nettement en retrait par rapport à l'amendement 138 et comporte beaucoup trop de failles dans lesquelles les opérateurs pourront s'engouffrer. « L'Union européenne vient de rater une occasion historique d'affirmer l'importance cruciale de l'accès libre à Internet », écrit Jérémie Zimmermann, porte-parole de La Quadrature du Net[4]. La première bataille paraît à demi perdue, mais la guerre est loin d'être finie.

UN NOUVEAU CYCLE POUR LA QUADRATURE

Fin 2008, après plusieurs années de combat associatif, Christophe Espern décide de quitter la Quadrature, laissant Jérémie Zimmermann seul à la manœuvre. Devant la lourdeur de cette tâche, les militants voient l'avenir de l'association s'assombrir, mais décident de rebondir et d'embaucher une personne à temps plein pour épauler Jérémie[5].

La Quadrature, qui a frôlé la fermeture, continue donc de se structurer. Dorénavant, les décisions seront prises collégialement avec l'ensemble des cofondateurs : deux cofondateurs valident, sinon on ne publie pas.

Pour permettre à la population de se réattribuer la compétence juridique, bien trop longtemps laissée aux seuls juristes, nous publions le 9 février 2009 le rapport « Hadopi, "Riposte graduée" : une réponse

inefficace, inapplicable et dangereuse à un faux problème[6] ». Ce document de 42 pages comprend une analyse juridique du texte, et résume aussi les études sur la consommation de biens culturels, démontrant par la même occasion l'erreur originelle ayant amené à croire que la surveillance des réseaux *peer-to-peer* et la menace d'amendes allaient « sauver la culture ».

L'association y dénonce le fait qu'avec la Hadopi les fournisseurs d'accès à Internet se retrouvent chargés de surveiller ce que téléchargent les internautes et donc d'analyser la nature du trafic ; une violation flagrante de la neutralité du Net. Elle rappelle que la Commission européenne soutient cette analyse, insistant sur le fait que « les moyens de sécurisation des accès proposés par la Hadopi ne doivent en aucune manière conduire à imposer, même indirectement, aux fournisseurs d'accès une obligation de contrôle des contenus qu'ils font transiter, une telle obligation de surveillance étant contraire au droit européen. »

Excellente surprise : ce texte est lu ! Y compris par des gens et dans des milieux que l'équipe n'imaginait pas atteindre. Le journal *Le Monde*, qui ne faisait pourtant pas partie des destinataires de notre mailing, rédige un encart dans ses pages « Culture », informant ses lecteurs de l'existence du rapport et en proposant un résumé.

Pour nous, les militants, quelque chose est en train de basculer. Quelques jours plus tard, Jérémie Zimmermann fait sa première apparition sur un plateau télé dans l'émission « Plein Écran » sur LCI[7]. Il y retrouve Pascal Nègre, alors président multi-casquettes des sociétés de gestion des droits SCPP et SCPA et d'Universal Music France. Cédric Ingrand, journaliste spécialiste du numérique pour la chaîne, salue ses invités, avec sous le bras le fameux rapport de la Quadrature, qu'il a lu et annoté. Ce n'est pas un débat qui se déroule alors, mais une analyse point par point du rapport, pendant laquelle Pascal Nègre fait figure de spectateur[8]. Il refusera ensuite d'en discuter et restera un fervent opposant à toutes les propositions émanant de l'écosystème anti-Hadopi, que ce soit sur les plateaux ou sur les réseaux sociaux.

Dans la foulée, une idée germe dans l'esprit de Jérémie, de Benjamin et du reste de l'équipe. Comment montrer son opposition à la loi Hadopi directement sur Internet ? L'opération *Blackout* voit le jour le 25 février 2009, inspirée par une action similaire mise en place en Nouvelle-Zélande contre une loi identique tout juste repoussée. Elle invite les internautes à peindre leurs sites en noir pour indiquer leur opposition au projet de loi, ou même à en couper l'accès. C'est la première opération de grande envergure de la Quadrature auprès du grand public, et c'est un succès.

UNE HADOPI PEUT EN CACHER UNE AUTRE

Malgré ce travail d'analyse et son influence croissante dans le débat public, la Quadrature ne peut empêcher l'avancée de la loi Hadopi au Sénat et à l'Assemblée nationale. En avril 2009, le gouvernement décide de passer le texte en « procédure accélérée » : après une seule lecture et un vote des deux Chambres, une commission mixte paritaire, réunissant des députés et des sénateurs, est chargée de proposer un texte commun au Sénat et à l'Assemblée nationale. Cette version, validée par le Sénat, est, de manière surprenante, rejetée par l'Assemblée nationale le 9 avril au matin à 21 voix contre 15. On parle alors des « députés ninjas », cachés derrière les piliers de l'hémicycle, arrivés en force au dernier moment pour supplanter en nombre les supporters de la mesure.

« Formidable victoire pour les citoyens ! » déclare alors la Quadrature, saluant « la puissance du réseau » qui a permis d'influencer les politiques pour en arriver là. Christine Albanel, ministre de la Culture, se dit « déterminée à se battre » pour que la loi soit finalement adoptée. Et l'affaire ne traîne pas. Faisant totalement fi du résultat d'un vote du Parlement, le gouvernement décide de représenter le texte le 29 avril. Il est adopté le 12 mai, par 296 voix contre 233. Les députés de la majorité auront suivi inconditionnellement les ordres de l'exécutif, sans rien connaître du dossier[9] !

Quelques jours avant, pourtant, à Bruxelles, l'amendement 138 a été réintroduit… Poussés par la pression populaire et par le retournement de situation au Parlement français, plus de 60 députés décident de saisir le Conseil constitutionnel le 19 mai. Le 10 juin, celui-ci censure le texte sur la coupure administrative de l'accès à Internet. Cette décision est historique en ce qu'elle reconnaît l'accès à Internet comme un droit fondamental. Le Conseil constitutionnel impose ainsi qu'il n'y ait qu'un juge qui puisse couper un accès Internet : « Considérant qu'aux termes de l'article 11 de la Déclaration des droits de l'homme et du citoyen de 1789 : "La libre communication des pensées et des opinions est un des droits les plus précieux de l'homme : tout citoyen peut donc parler, écrire, imprimer librement, sauf à répondre de l'abus de cette liberté dans les cas déterminés par la loi" ; qu'en l'état actuel des moyens de communication et eu égard au développement généralisé des services de communication au public en ligne ainsi qu'à l'importance prise par ces services pour la participation à la vie démocratique et l'expression des idées et des opinions, ce droit implique la liberté d'accéder à ces services[10]. »

La liberté d'accès au réseau mondial, devenu bien commun de l'humanité, est donc reconnue comme un droit. Cela ouvre pour les militants d'immenses perspectives : tout ce qui entrave, empêche, diminue, ou conditionne cet accès est désormais une atteinte à un droit fondamental reconnu à chaque personne. Pour la Quadrature, c'est une victoire considérable.

Le 23 juin, Christine Albanel est remplacée par Frédéric Mitterrand. Mais rien ne change dans la guerre contre les « pirates ». Le 25 juin, le gouvernement présente le texte Hadopi 2, censé répondre à la censure, deux semaines plus tôt, de la première version. Cette nouvelle mouture remet le juge dans la boucle pour la décision finale.

E-G8 : LE VIEUX MONDE FACE AU CYBERESPACE

Une seule situation, une seule image suffit parfois à résumer toute une époque politique. En mai 2011, Nicolas Sarkozy, désireux de jouer un rôle international de premier plan, et de se réconcilier avec le monde du Web après la bataille de la Hadopi, convoque le e-G8, une sorte de sommet mondial du numérique qui doit se tenir à Deauville à la veille d'un G8 plus classique.

Facebook, Google, Amazon sont présents, tandis que Free, France Télécom ou PriceMinister[11] représentent les ambitions françaises. Tout cela ronronne dans l'autosatisfaction, jusqu'à une table ronde sur la propriété intellectuelle qui rassemble : le PDG du groupe de presse Bertelsmann ; Pascal Nègre, patron d'Universal Music France ; le directeur des Éditions Gallimard ; Frédéric Mitterrand, ministre de la Culture ; et John Perry Barlow, auteur de la fameuse « Déclaration d'indépendance du cyberespace ». Ce dernier écoute patiemment la discussion qui se tient en français et prend enfin la parole, avec lenteur : « D'abord, je vous remercie de m'avoir invité, mais je suis un peu surpris, surtout en voyant les autres membres de cette table ronde, parce que j'ai l'impression qu'on ne vient pas vraiment de la même planète. Il se trouve que je suis le seul ici à vivre de ce que ces messieurs appellent "la propriété intellectuelle". Je ne vois pas ma création et mon moyen d'expression comme une "propriété". Une "propriété", c'est quelque chose qu'on peut me prendre. Si je ne la possède plus, quelqu'un d'autre la possède. L'expression, ça ne marche pas comme ça[12]. » Ce que la Quadrature s'efforce de crier depuis des mois, sans être entendue, il l'affirme calmement, d'une voix posée, et on l'écoute. L'ambiance dans la salle est électrique, et les récits dans la presse rendent bien ce qui est un coup de tonnerre dans un ciel trop bleu[13].

Bien sûr, la Quadrature est sur le coup. Outre le fait d'avoir créé un site de campagne contre le e-G8[14], dehors, les militants déroulent une banderole : « *Governments & Corporations United to Control the Net* » (« Gouvernements et grandes entreprises : unis pour le contrôle de l'internet »). À l'intérieur du e-G8, Jérémie Zimmermann prend la parole : il tient à la main l'étude publiée par la Hadopi, qui montre que les

consommateurs de contenus téléchargés sont aussi les personnes qui consomment le plus de produits payants.

3. LE COMBAT CONTRE L'ACTA

Début 2012, en plein hiver, plusieurs milliers de Polonais sont dans la rue, par - 10 °C. Ils manifestent. L'objet de leurs craintes ? Un obscur traité commercial multilatéral, l'Accord commercial anti-contrefaçon, ou *Anti-Counterfeiting Trade Agreement* : l'ACTA. Un traité international qui n'a de commercial que le nom.

Comment un traité sur le « renforcement des droits de la propriété intellectuelle » peut-il susciter une telle mobilisation populaire, amener Google et Wikipédia à afficher un bandeau noir sur leur plateforme, et créer des remous jusqu'en plein cœur de la vie politique états-unienne ?

STRATÉGIE DU VAMPIRE CONTRE CULTURE DU SECRET

La première fois que nous entendons parler de l'ACTA, c'est lors de la fuite d'un document de discussion, « trouvé sur une photocopieuse » du Parlement européen, puis publié par WikiLeaks en 2008. Rapidement, d'autres suivent, dans la presse ou ailleurs, et cela ne fait plus de doute : un traité d'une importance majeure est dans les tuyaux, scandaleusement négocié en dehors du processus démocratique.

Nous ne sommes pas les seuls, à la Quadrature, à nous méfier : en mars 2010, le Parlement européen lui-même dénonce par une déclaration officielle « des négociations commerciales qui sortent du cadre décisionnel normal de l'Union[1] ».

Effectivement, des représentants non élus de plusieurs États – pour la France, issus du ministère des Finances, pour les États-Unis du ministère du Commerce – se réunissent discrètement depuis des mois dans des hôtels, à Genève, à Washington ou encore à Rabat, pour défendre leurs intérêts. Leurs intérêts, ce sont ceux de leurs ministères, c'est-à-dire majoritairement ceux des industries du copyright, pas ceux de leurs citoyens.

Face à cette culture du secret, de l'ombre, de l'absence caractérisée de transparence, place à la lumière, à la « stratégie du vampire » ! La Quadrature décide, avec d'autres organisations, d'exposer au grand jour ces négociations secrètes et de braquer les projecteurs sur les protagonistes français (hauts fonctionnaires habitués à la discrétion, qui nous en voudront beaucoup de les avoir ainsi nommés – ou en tout cas assez pour nous faire un procès).

Avec Act Up, nous décidons fin juin 2010 d'aller rendre une petite visite aux conspirateurs d'ACTA. Le neuvième round de leurs négociations se déroule au cœur des montagnes suisses, dans un hôtel 5 étoiles qui donne directement sur le lac de Lucerne. Comment les atteindre et leur rappeler l'existence d'autres partis non invités à la table ? Nous apercevons au loin un loueur de pédalos, à 10 francs suisses de l'heure. Banco : quelques heures plus tard, nous pédalons sous le soleil, nous nous plaçons sous les fenêtres de l'hôtel et sortons nos banderoles et nos mégaphones. Personne ne sort, personne ne vient nous chasser, c'est en quelque sorte un coup d'épée dans l'eau. Mais une fois les pédalos rendus, une bonne douche de prise, nous nous dirigeons vers le centre-ville et investissons une terrasse pour boire quelques verres, quand arrivent… tous les négociateurs de l'ACTA, sortis de leur hôtel pour prendre un verre eux aussi. Après quelques sarcasmes, la discussion s'engage entre les deux partis et nous voilà invités à expliquer nos arguments à ces interlocuteurs de l'ACTA, qui se présentent comme tout à fait ouverts aux critiques des associations.

Nous ne ratons pas cette occasion et demandons le lendemain, dans une salle du luxueux hôtel, à avoir la confirmation des fuites dont nous

disposons. La sentence tombe : le texte prévoit bien de transférer des pouvoirs de sanction à des acteurs privés en sanctionnant pénalement ces derniers. Ambiance glaciale.

C'est le début d'une lutte contre un projet pernicieux, né sur des coins de table. Nous allons dépenser notre énergie sans compter et espérer que les étoiles finissent par s'aligner.

LA VÉRITÉ SUR L'ACTA

L'ACTA, c'est le fourre-tout supranational des tenants (pour ne pas dire des extrémistes) de la « propriété intellectuelle », ce concept juridiquement pratique mais intellectuellement bancal, car il réunit un éventail d'éléments sans réel lien les uns avec les autres : les brevets, le droit des marques, le droit d'auteur, les indications géographiques. Quel lien rigoureux existe-t-il entre le droit régissant l'appellation d'origine contrôlée du cantal AOP, la production de médicaments génériques et le copier/coller de photos sur Internet ? À peu près aucun, mais le vocable « propriété » a une conséquence fort pratique : la possibilité de décrire celles et ceux qui ne la respectent pas comme des pirates ou des voleurs. Pour les défenseurs de cette vision conservatrice, télécharger, c'est voler.

L'un des principaux enjeux du traité est d'instaurer une protection extrêmement agressive du copyright. D'une part, l'ACTA souhaite placer une responsabilité pénale sur les intermédiaires techniques des échanges d'œuvres sur Internet (comme les fournisseurs d'accès), y compris à but non marchand. La répercussion immédiate semble évidente : pour éviter le moindre risque, les intermédiaires techniques surveilleront leur réseau et leurs utilisateurs de très près, censurant à tout va sans chercher de nuance, leur responsabilité pénale étant en jeu. Un responsable de FAI peut ainsi payer une amende forfaitaire parce qu'un internaute a envoyé un MP3 à un autre. Et cette caricature, publiée par un dessinateur sur son propre blog, droit à la parodie ou infraction au copyright ? Dans le doute,

coupons l'accès ! En résumé, l'ACTA transforme les intermédiaires techniques en police et justice privées du copyright.

D'autre part, il s'agit d'inscrire, dans le texte comme dans les têtes, l'idée selon laquelle chaque téléchargement d'œuvre correspond à une vente perdue. En ce sens, le partage d'œuvres dans son ensemble est un manque à gagner colossal. Les représentants des gros ayants droit (c'est-à-dire les majors) n'ont jamais réussi à défendre correctement cette position devant un juge, et pour cause : elle est parfaitement fantaisiste. Elle fait fi des nombreuses études qui montrent qu'une fois les différents effets économiques pris en compte, l'impact du partage à but non marchand pour les artistes est soit légèrement positif, soit neutre. Si l'on ne peut prouver juridiquement qu'un téléchargement équivaut à une vente perdue, reste à l'inscrire dans le droit. C'est tout l'objectif des industries culturelles.

Dans le contexte de l'ACTA, il ne semble pas exagéré d'évoquer un certain « colonialisme » des œuvres de l'esprit. À l'exception du Maroc, la liste des pays participant aux négociations le reflète : Australie, Canada, Corée du Sud, États-Unis, Japon, Nouvelle-Zélande, Singapour, et bien sûr l'Union européenne qui, embarquant d'un coup vingt-sept pays, pèse d'un poids tout particulier sur l'accord, sa composition et la formulation de ses différents articles.

Force est de constater que l'ACTA vise à protéger à tout prix les intérêts des pays occidentaux (aux puissantes économies de services fondées sur le travail intellectuel) aux dépens des autres nations. Quelle hypocrisie, alors que l'histoire nous enseigne qu'ils n'ont eux-mêmes aucunement respecté les droits d'auteur et les brevets lorsqu'ils étaient en train de se développer aux XVIII^{e} et XIX^{e} siècles. Désormais chantres de la propriété intellectuelle, ils demandent la main sur le cœur que l'on ait une pensée pour les pauvres artistes et inventeurs… Les États-Unis en tête… Eux qui, au XVIII^{e} siècle, reproduisaient sans vergogne les œuvres d'auteurs anglais, oubliant tout copyright. Charles Dickens en fit les frais de son vivant, allant jusqu'à s'attirer les foudres de ses fans américains lors d'une tournée littéraire où il profita de sa notoriété pour attirer

l'attention sur ce problème et montrer son mécontentement clair et explicite[2].

Que ce même pays tente désormais de « copyrighter » tout ce qu'il peut et d'en tirer profit aurait de quoi faire sourire si ça n'était pas doublé d'une agressive injonction à un respect total et absolu de tous droits de propriété intellectuelle pour les pays encore en développement. On comprend mieux, dans ce contexte, pourquoi la Chine n'est pas à la table des négociations… Étant l'une des principales cibles de l'ACTA, elle n'a aucun intérêt à en faire partie. Et après tout, autant commencer par un noyau dur d'États signataires pour ensuite mieux faire pression sur d'autres.

HANTER LES COULOIRS DU PARLEMENT EUROPÉEN

Pour contrer ce texte dangereux et inacceptable, la stratégie de la Quadrature est simple : aller au contact, au Parlement. Mais encore faut-il y entrer… Depuis plusieurs mois, nous rencontrons régulièrement des députés qui soutiennent la position de l'association, en particulier au sein des Verts. De précieuses aides pour pénétrer là où tout se joue.

Quand nous arrivons dans le hall du Parlement, nous appelons un ou plusieurs députés, selon notre nombre, et leur demandons de nous ajouter sur la liste des invités. Reste à attendre qu'un assistant parlementaire vienne nous chercher à l'accueil. Le règlement prévoit que nous sommes alors sous sa responsabilité. En réalité, une fois entrés, nous partons « faire notre vie » dans les étages du bâtiment.

Distribuer des flyers à l'entrée des sessions des commissions, travailler les amendements avec nos alliés, parcourir les couloirs, frapper à toutes les portes pour diffuser nos arguments auprès des députés : autant d'actions qui pourraient mettre celles et ceux qui nous ont permis d'entrer en porte-à-faux. Résultat, dès que nous apercevons l'ombre d'un vigile, nous déguerpissons et nous changeons d'étage.

Rapidement, nous connaissons cet immeuble comme notre poche, tout comme les gens qui y travaillent. Besoin d'un accès wifi ? Le service informatique nous fournit les codes. Des affiches pour décorer en douce les couloirs et les ascenseurs ? Le service de reprographie nous les imprime, en A2 quadrichromie. Et le règlement intérieur ? Qu'à cela ne tienne, la Quadrature est organisée. Notre efficacité nous permet de sortir de l'hémicycle après avoir suivi un vote concernant notre sujet de préoccupation, de finaliser dans la foulée un communiqué préparé la veille au soir avec les éléments du jour, de le faire imprimer, et de distribuer à la sortie des députés un texte dénonçant ce qu'ils viennent justement de voter, à leur grande stupeur.

DE LA BULLE BRUXELLOISE À L'ACTIVISME EUROPÉEN, ET AU-DELÀ

Parler aux parlementaires, la Quadrature commence à savoir faire. Mais comment expliquer succinctement un sujet aussi complexe qu'ACTA aux non-spécialistes, qui n'ont pas forcément envie de lire un texte sur un sujet aussi aride ? Coup de chance, un soutien de la Quadrature, Benoît Musereau, nous contacte : il est graphiste et nous propose de réaliser une petite vidéo sur ACTA et ses dangers. Nous nous mettons au travail, allant jusqu'à enregistrer nous-même la voix off (en anglais, pour maximiser la portée du message), dans la grande tradition du « fait maison » de la Quadrature !

Le 28 octobre 2011, trois vidéos sont prêtes et mises en ligne sur notre site, hébergées sur les serveurs d'Octopuce ; des miroirs sont ajoutés sur YouTube et Dailymotion. La première dénonce ACTA en un peu plus de deux minutes, les deux autres se concentrent sur les dangers du traité pour Internet et pour les brevets et les semences.

Les vidéos peinent à sortir des cercles militants. Néanmoins, une surprise nous attend. Quelques jours plus tard, alors qu'il est au Parlement européen, Jérémie se retrouve assis à côté de Peter Sunde alias Brokep de The Pirate Bay (TPB), plateforme de partage *peer-to-peer* de

renommée internationale. Il lui montre la vidéo. Et c'est ainsi qu'elle se retrouve sur la page d'accueil de TPB. Il va sans dire qu'en 2011 le taux de fréquentation de leur site est infiniment supérieur à celui de laquadrature.net. En quelques minutes, Octopuce voit ses serveurs exploser, nous décidant à renvoyer les internautes vers le miroir YouTube. Notre vidéo finira à plus de 2 millions de vues rien que sur YouTube, un chiffre assez incroyable à l'époque. Quant aux sous-titres, initialement uniquement disponibles en français et en anglais, ils sont rapidement traduits en plus d'une dizaine de langues par des bénévoles. La communauté Internet se mobilise et nous restons émus devant une telle réponse.

Une autre composante fondamentale de la campagne contre l'ACTA est la collaboration européenne des militants. Alors qu'à l'échelle internationale les signatures du traité se multiplient (États-Unis, Australie, Canada, Corée du Sud, Japon…), en Europe, rien n'est encore joué. Face au danger, les différentes organisations de défense des libertés fondamentales dans l'espace numérique font plus que jamais front commun. Aux côtés de la Quadrature, nous comptons désormais Bits of Freedom aux Pays-Bas, Netzpolitik.org puis Digitale Gesellschaft en Allemagne, Panoptykon Foundation en Pologne, ou encore Open Rights Group au Royaume-Uni. European Digital Rights (EDRi), à Bruxelles, coordonne ce réseau d'organisations. Chacune d'elles agit dans son pays pour empêcher le gouvernement national de signer l'accord, mais participe également à l'action collective pour éviter une signature des vingt-sept États de l'UE. Nous dialoguons avec nos collègues européens, étudions les nouvelles fuites, discutons des prochaines étapes du processus de négociation, élaborons une stratégie commune…

Mais au-delà des mouvements activistes, le combat passe à une dimension supérieure, celui de la mobilisation de l'opinion. Elle est d'abord portée par des milliers de Polonais, qui défilent dans les rues de Varsovie et de Cracovie en janvier 2012 pour protester contre la signature d'ACTA, à valeur hautement symbolique. Encouragés par ce mouvement qui prend forme sous nos yeux, nous mettons en ligne le mois suivant un

tract intitulé « NO to ACTA! », en français et en anglais. En moins de deux semaines, celui-ci est traduit spontanément dans toute l'Europe et même au-delà, en vingt et une langues[3].

Aux États-Unis, la campagne contre ACTA prend la forme d'un combat contre ses déclinaisons locales, les propositions de loi *Stop Online Piracy Act* (SOPA) et *Protect Intellectual Property Act* (PIPA). Une opération *blackout* est organisée par l'ONG Fight for the Future, à laquelle participeront près de 115 000 sites, dont Wikipédia, Reddit, Tumblr ou WordPress. Les actions vont de l'affichage d'un simple bandeau au blocage complet du site, en passant par une pleine page insérée avant d'y avoir accès. Même Twitter et Google arborent un bandeau ou un logo modifié pour indiquer leur participation à l'opération[4].

Cette opération est un succès au fort impact médiatique. Elle change la trajectoire des propositions de loi. Le *New York Times* va même jusqu'à parler de passage à « l'âge adulte politique du secteur des technologies ». Une incroyable collaboration internationale se met en place, nous préparant à la dernière ligne droite.

LE COUP DE GRÂCE

Le 2 juillet 2012, les membres de la Quadrature retournent au Parlement. Le vote de l'ACTA est proche, alors même que le texte est en train d'être étudié à la Cour de justice de l'UE. La question est de savoir s'il est compatible avec la législation européenne ; la réponse est attendue dans plusieurs mois. Pourquoi donc voter ce texte maintenant ? Curieux calendrier.

Et c'est reparti pour un tour des bureaux ! Dans l'un des premiers, une attachée parlementaire est au téléphone. Lorsqu'elle raccroche, elle nous demande d'approcher. Nous nous présentons : « Bonjour, nous sommes bénévoles de La Quadrature du Net, nous venons vous parler du vote de demain, sur l'ACTA. » Son sourire disparaît à mesure que nous

parlons, elle nous coupe la parole, se lève et vient vers nous en faisant de grands gestes : « Dehors ! Dehors ! C'est à cause de vous que nous recevons des milliers d'e-mails et que le téléphone n'arrête pas de sonner ! Je ne veux plus entendre parler de vous ! » Mi-amusés, mi-surpris, nous reculons sur le palier, alors qu'elle nous referme la porte au nez. Nous regardons sur notre liste quel est le député de cette attachée parlementaire que nous avons tant choquée. C'est Jean-Marie Cavada.

À côté, nous tombons sur une députée allemande. Après la présentation de notre exposé, la députée nous remercie, nous confie qu'elle est plutôt pour l'ACTA, convaincue qu'il est dans l'intérêt de l'Europe de signer ce traité, mais annonce qu'elle s'abstiendra, dans l'attente de la décision de la Cour de justice. Nous sortons de cet entretien sur un petit nuage. Nous avons discuté avec une opposante, une députée européenne, avec qui nous avons échangé des arguments pendant une dizaine de minutes. C'est donc possible !

Ce jour-là, nous en rencontrons des dizaines d'autres. On nous écoute, on nous congédie d'un geste… Nous ne saurons jamais combien de députés nous avons réussi à convaincre… Le 4 juillet, le texte est rejeté. La Quadrature est là, au balcon, assistant au vote. Pas d'explosion de joie ou de déception dans la grande salle du Parlement. Ce n'est qu'un vote parmi d'autres, et seul un bruissement se fait entendre. La séance se poursuit, comme si les défenseurs de l'ACTA, négociant dans l'ombre depuis tant d'années, ne s'étaient pas pris un mur de plein fouet.

Nous rejoignons la cafétéria, où nous pouvons enfin nous laisser aller à afficher notre joie. Nos alliés passent nous voir, et tout le monde s'auto-congratule après cette longue et dure bataille politique.

Mais si la victoire, réelle et durement acquise, n'est que relative, c'est que l'ACTA s'inscrit dans une perspective plus globale…

4. CES POLITIQUES QUI N'ONT RIEN COMPRIS

Comme la Hadopi 2 avait remplacé la Hadopi en France, l'ACTA s'inscrivait dans la lignée des traités anti-piratage américains PIPA et SOPA. Bien que certains projets tombent à l'eau, personne n'en doute alors : d'autres suivront.

L'insistance du pouvoir à vouloir faire passer sous une forme ou une autre des textes pourtant régulièrement retoqués trahit un monde fermé sur lui-même, qui ne représente plus les citoyens, davantage perméable aux lobbies plutôt qu'à la société civile. Du point de vue des militants, cet éternel retour des mêmes formules copiées-collées énerve, alors que nous avions pourtant l'impression d'avoir gagné. Comment relancer sans cesse la machine et l'engouement populaire sur les mêmes arguments ? Heureusement, la culture geek est résiliente. Elle s'empare de toutes les occasions possibles pour créer et rire.

Et mieux vaut avoir de l'humour et de l'autodérision quand on est sous le feu des critiques ! Lors des débats Hadopi, en 2008-2009, les députés ont reçu des quantités de messages, argumentés et personnalisés, comme ils en avaient rarement vu. Sortant de ses gonds, la ministre de la Culture de l'époque, Christine Albanel, a carrément accusé l'association de falsifier ces milliers d'e-mails. Quelques semaines plus tard, le cabinet de celle qui a vanté les mérites du fameux « pare-feu OpenOffice[1] » a expliqué sans ciller dans une dépêche AFP que La Quadrature du Net n'était que « cinq gus dans un garage qui font des e-mails à la chaîne[2] ». Bien que cette dépêche ait ensuite été réécrite pour supprimer ce passage,

l'association s'est dite flattée de tant d'attention de la part du ministère en communiquant ainsi : « Cela prouve que l'action des nombreux citoyens épris de liberté qui contactent leurs députés commence à porter ses fruits. Cela révèle la peur de la ministre de se retrouver confrontée aux réalités techniques et à l'opinion des citoyens. »

Loin de nous formaliser des insultes de la ministre, nous baptisons les bureaux de l'association le « Garage », tout comme le compte Twitter communautaire des bénévoles.

LE *PEER-TO-PEER*, QUÈSACO ?

La question de l'ignorance des réalités techniques se pose, effectivement…

On se souvient de Jacques Chirac, interrompant une présentation des fonctionnalités d'Internet à la Bibliothèque nationale de France en 1996 pour demander ce qu'est une souris. On se rappelle l'interrogation (légitime) d'une partie de la presse en 2009, doutant du fait que Nicolas Sarkozy ait déjà envoyé un e-mail[3]… Et François Fillon, alors fringant Premier ministre, de déclarer sans sourciller qu'il « est un vrai geek[4] » car il utilise un iPhone, possède deux Macs et des appareils photos numériques. Fichtre ! Depuis, la Hadopi est passée. Mais les choses ont-elles changé ?

Dès le début des années 2000, le *peer-to-peer* (ou « pair-à-pair » en français) est sur toutes les lèvres, représentant un espace miraculeux donnant accès au cinéma, à la musique, et même à des séries télé souvent inédites en France. Il permet l'échange direct de données entre les ordinateurs reliés à un même réseau comme Internet, sans passer par un serveur central. Mais pour la classe politique, le *peer-to-peer* n'est qu'un excellent candidat au titre de fossoyeur de la culture française. Un danger manifeste donc, que les décideurs peinent pourtant à définir…

Des journalistes du site Bakchich.info et de Canal + s'exercent à une sorte de micro-trottoir sur la moquette des couloirs de l'Assemblée[5]. Ils

interrogent les députés en leur demandant d'expliquer ce qu'est le *peer-to-peer* avec leurs propres mots, voire ce qui le différencie du BitTorrent ; BitTorrent étant – c'est tout le piège de la question – un des multiples types de réseaux *peer-to-peer*.

L'effet comique est immédiat :

Bakchich : « Est-ce que vous savez ce qu'est le *peer-to-peer* ? »

Henri Plagnol [député UMP du Val-de-Marne, favorable à la Hadopi] : « Oui, bien sûr ! »

Bakchich : « Alors, expliquez-nous… »

Henri Plagnol : « Bah, le *peer-to-peer*, c'est tout simplement pouvoir… euh… s'adresser en direct par… euh, tout ce qui est technologie numérique des personnes qui sont dans la même situation que vous. Hein, donc c'est un… C'est quelque chose de très positif et qu'il faut encourager ! »

Un autre :

Bakchich : « Est-ce que vous savez ce qu'est le *peer-to-peer* ? »

Jean-Pierre Grand [député UMP de l'Hérault] : « Non. »

Bakchich : « Non ? Ou le *streaming* ? »

Jean-Pierre Grand : « Euh non. Moi je parle français, excusez-moi (*il s'en va*). »

Comment prendre au sérieux une classe politique qui montre des velléités à contrôler ce qu'elle comprend soit mal, soit pas du tout ? Leur insistance à faire passer la loi Hadopi est tournée en ridicule jusque sur les plateaux de télévision. Nous y intervenons le plus souvent possible, arborant fièrement nos tee-shirts « Hadopi, même pas peur ! », appelant la population à ne pas craindre ce « gendarme du Net » qui promet d'être une belle usine à gaz. Par exemple, techniquement, la loi est censée faire la chasse au « défaut de sécurisation d'accès à Internet », un délit aussi vaseux que sa terminologie, que tout le monde se refuse à expliquer concrètement, le décret d'application de la loi devant alors préciser tout ça « plus tard ».

En lisant l'étude publiée par la Hadopi en janvier 2011, on est d'ailleurs frappé par la mise en avant du thème de la « sécurité », primordial puisque le détenteur de la ligne est tenu responsable devant la loi des usages « illicites » qui seraient faits de sa connexion. La Haute Autorité peut ainsi mieux coincer les contrevenants : si votre wifi reste ouvert à tous les vents, on ne pourra jamais vous coller une amende pour ces usages avec certitude mais vous serez condamné quand même pour « défaut de sécurisation » de votre connexion à Internet !

La sécurisation, c'est simple en théorie, compliqué en pratique. Et les recommandations officielles pour être « sécurisé » font toujours défaut. À l'époque d'ailleurs, certaines personnes ne manquent pas de faire remarquer que le ministère de la Défense se refuse à utiliser le wifi, ne s'estimant pas en mesure de sécuriser suffisamment les accès sans-fil. Mais ne vous inquiétez pas, vous, vous y arriverez !

La Hadopi en elle-même attire les moqueries à plus d'un titre et n'est pas à un paradoxe près ! Morceaux choisis. Elle publie en janvier 2011 une étude à l'occasion du MIDEM, le grand raout annuel des industries de la musique. Sur cette dernière, est écrit noir sur blanc que les personnes qui téléchargent des contenus « illicites » dépensent aussi en moyenne plus d'argent dans des biens culturels « licites ». Autrement dit, bien loin d'être des pirates ou des voleurs, les téléchargeurs sont aussi des personnes qui font vivre l'industrie culturelle marchande, et leur grand appétit de biens culturels emprunte toutes les voies existantes, qu'elles soient légales ou non, payantes ou non[6].

En juin 2011, la soirée de lancement de la campagne de communication de la Hadopi – une campagne chiffrée à 3 millions d'euros tout de même[7] ! – doit créer l'événement et redorer le blason d'une loi que tout le monde redoute et que personne ne comprend. Nous prenons la direction des beaux quartiers de Paris et nous regroupons devant l'espace Pierre-Cardin, choisi pour cette petite sauterie. C'est l'occasion pour la Haute Autorité de présenter son label « PUR » (pour « promotion des usages responsables ») (*sic*), qui doit être apposé sur les

sites de téléchargement « autorisés ». Même la presse se moque : « Hadopi perdue en naze campagne », titre *Libération*[8].

Bafouillements, contresens, bêtises en pagaille : les députés n'y connaissent rien et n'y comprennent rien. Le bon mot « *peer-to-peer* : le pire du pire[9] » tourne, nous rions et sommes nombreux à rire, un peu jaune toutefois…

S'il est possible, ponctuellement, de faire passer de l'intérieur quelques idées dans certains cas très exceptionnels, le fossé est grand entre les députés – et la classe politique dans son ensemble – et la population, qui a une expérience concrète et positive d'Internet. Même les membres de la garde républicaine nous confient, sur le trottoir devant l'Assemblée nationale qu'ils ont pour mission de protéger, qu'à la caserne tout le monde utilise les réseaux *peer-to-peer* pour télécharger les derniers films et séries.

L'incompréhension entre entreprises et décideurs d'un côté, et milieu geek de l'autre, s'est illustrée à l'international par l'histoire d'un site Internet d'un genre particulier : The Pirate Bay. Monté en 2003 par trois Suédois, le site est mondialement connu pour être le plus grand répertoire de liens pour télécharger des contenus via les logiciels de torrent.

Techniquement, c'est un site Web permettant la mise en relation des fameux « pairs » (c'est-à-dire les ordinateurs des uns et des autres connectés à Internet) et le partage de fichiers entre eux. Adossé à un *tracker*, le site public thepiratebay.org sert d'index de fichiers torrent. Ces derniers, contrairement à ce que paraissent (ou font semblant de) penser les industries du disque, du film et du jeu vidéo, ne sont ni des films, ni des albums, ni des jeux. Ils se comportent comme des « tables des matières » renvoyant à d'autres fichiers (le plus souvent des films, des albums, des jeux…). Ils ne contiennent rien d'autre qu'une liste comprenant les points de rendez-vous (les *trackers*), le nom des fichiers concernés et d'autres informations techniques. Une fois chargés dans le bon logiciel, ces fichiers torrent permettent d'être mis en contact avec des pairs qui, eux, possèdent tout ou partie des fichiers en question, et peuvent en envoyer une copie.

Cette distinction, assez technique, convenons-en, entre hébergement de fichiers sous copyright et mise à disposition d'un « index d'index » est la base sur laquelle les trois larrons de TPB estimaient leur site légal.

Malgré ce mode de défense assez audacieux, le 31 mai 2006, la police suédoise organisa un raid contre The Pirate Bay. Elle saisit du matériel informatique dans douze *data centers* différents. Rendu inaccessible, TPB fit la une des médias internationaux, la Motion Picture Association of America, qui défend les intérêts des plus grands studios hollywoodiens, se gargarisant du succès de l'opération.

À peine trois jours plus tard, le site resurgit, boosté par sa couverture médiatique. Ses visiteurs étaient deux fois plus nombreux qu'avant sa fermeture. C'est le pied de nez des partageurs de culture. L'*effet Streisand*, ce phénomène qui se produit lorsque la volonté d'empêcher la divulgation d'informations que l'on aimerait garder cachées déclenche le résultat inverse, est décuplé. Rien n'arrête le partage sur Internet.

SE RENCONTRER POUR MIEUX LUTTER : LES QUADR'APÉROS

Début 2011, il devient évident que la Quadrature doit pouvoir compter ses soutiens autrement que par les seuls dons. Nos actions demandent une forte participation humaine. Pour rassembler le cercle des proches et partager un calendrier politique, nous mettons en place le principe d'un rendez-vous régulier, mensuel, rassemblant en un même lieu les sympathisants.

Le premier Quadr'apéro se tient ainsi le 25 mars 2011[10], au Loop (pour « Lieu ouvert ou pas »), *hackerspace* parisien situé à l'époque à côté de la place de la République. Le programme de la soirée (et de celles à venir) : se rencontrer, discuter autour d'un verre, et faire le point sur l'actualité touchant aux sujets de la Quadrature.

Deux mois plus tard est organisé un événement de plus grande ampleur, sur un week-end : le Quadrature Communication Camp. Plus

d'une centaine de bonnes volontés se retrouvent pour deux jours de travail, d'échanges et d'ateliers politiques.

Si le second, exigeant une importante consommation d'énergie militante, ne sera pas réitéré sous cette forme, mais à une échelle plus petite avec des ateliers sur une soirée, le premier est pérennisé, et rassemble toujours autant. Il permet régulièrement à de nouveaux visages de croiser les habitués et les membres de l'association et d'échanger, de se tenir au courant, voire de participer à des actions futures. La Quadrature a trouvé là un axe important de communication et d'extension de sa communauté. L'événement, très parisien, essaime ponctuellement dans d'autres villes.

Les premiers Quadr'apéros ont lieu dans des *hackerspaces*, en extérieur, ou sont hébergés par une fondation. Et puis, un jour, le temps est venu : nous louons enfin nos propres locaux ! Fini le télétravail pour les salariés de la Quadrature. Les ressources permettent d'héberger une équipe grandissante. Travail quotidien, interviews, Quadr'apéros, ateliers divers, nous avons désormais un lieu dédié. L'activité se développe-t-elle parce qu'on a les bons outils, ou acquiert-on les outils parce que l'activité se développe ? Question classique de l'existence d'Internet : le réseau de réseaux existe-t-il parce qu'il est nécessaire à cette étape du développement humain, ou son arrivée transforme-t-elle la société qui l'adopte ?

Nos bureaux ancrent en tout cas l'association dans le réel. Nous n'avons d'autre choix que d'aller de l'avant. Au sous-sol, nous aménageons un espace avec un grand filet de camouflage militaire. C'est parfois là que se déroulent des interviews, dans une ambiance de guérilla communicationnelle. Une guérilla que l'on retrouve bien dans les premiers temps de l'association. Rien ne doit passer. Aucune bourde de nos décideurs ne doit être passée sous silence. Nous ne lâchons pas la bride. Évidemment, sortir des communiqués tous les deux jours n'est pas tenable sur la durée, et l'équipe va devoir apprendre à économiser ses forces. Mais le ton est posé : les politiques doivent compter avec la Quadrature.

OPÉRATION DATALOVE

Courant 2012, la Quadrature se positionne pour participer au futur débat européen sur le droit d'auteur. C'est l'opération Datalove.

Nous défendons une réforme positive de celui-ci qui mettrait fin à la guerre contre le partage, en prenant en compte les droits du public, l'accès à la culture, tout cela dans le cadre des nouvelles pratiques culturelles rendues possibles par les technologies numériques.

L'enjeu est d'ouvrir les yeux des députés européens sur les usages réels des artistes, usages souvent en opposition avec le droit et pourtant générateurs de brassages culturels, créateurs de nouvelles identités artistiques. Dans l'espoir de planter des petites graines dans les têtes de ces messieurs-dames du Parlement, nous nous rendons à Bruxelles pour leur distribuer des clés USB Datalove, chargées de contenu culturel remixé[11].

Pour monter l'opération (l'édition de 1 000 clés et le voyage en Belgique de plusieurs militants), une campagne de financement participatif a été lancée en septembre ; une première dans l'histoire de la Quadrature. C'est en réalité un moyen d'intégrer toute la communauté dans la stratégie de l'association : quand nous proposons quelque chose qui sort de son activité habituelle, soit les soutiens suivent et financent, et nous passons à l'action, soit ce n'est pas le cas et nous laissons tomber.

Ce projet-là est rapidement financé. Deux mois plus tard, le 28 novembre, nous sommes six militants à faire le déplacement pour remettre les clés Datalove aux députés[12]. Cette campagne est un moment motivant pour nous. Rencontrer les élus donne l'occasion d'échanger des propos constructifs. Nous n'avons pas peur de nous faire courir après par le service de sécurité, ni de nous faire envoyer sur les roses par des députés énervés. La clé USB est un cadeau qui, ne valant que quelques euros, présente peu d'effet corruptible, mais c'est un bel objet, en forme de vraie clé tatouée d'un cœur. Nous l'avons collée sur une feuille cartonnée sur laquelle se trouve, en anglais, le texte suivant :

Chers membres du Parlement européen,

Après le rejet d'ACTA, nous, citoyens, ressentons le besoin de partager avec vous ces éléments de culture digitale que nous construisons chaque jour sur l'internet libre, ouvert, neutre et donc universel.

Cette clé USB Datalove a été financée de manière participative par des citoyens de toute l'Europe. Vous y trouverez une collection de musiques, films et livres qui nous sont chers et qui ont été créés avec la même passion du partage, de la réutilisation des œuvres culturelles et de la promotion de ces pratiques. C'est ainsi que la culture se crée de nos jours !

Nous espérons que cela vous aidera à comprendre qu'il est urgent que les pratiques culturelles que rendent possibles les technologies numériques soient encouragées plutôt que réprimées, grâce à une profonde réforme positive du copyright.

« Toute personne a le droit de prendre part librement à la vie culturelle de la communauté, de jouir des arts et de participer au progrès scientifique et aux bienfaits qui en résultent. »

Article 27.1 de la Déclaration universelle des droits de l'homme

Bon visionnage, bonne écoute, bonne lecture… et bonne réutilisation !

La Quadrature du Net

Ce projet est un appel du pied aux élus. Nous souhaitons leur prouver que leurs actions vont parfois à l'encontre de l'intérêt du public.

OPÉRATION BOOK SCANNER

Et puis il y a des moments de grâce, où deux mondes se rencontrent, comme l'opération *Book Scanner*, par exemple. Au printemps 2014, le ministère de la Culture organise l'événement Silicon Valois, « espace éphémère de travail créatif, de réflexion et de rencontres autour des enjeux de la culture et du numérique » : une fois l'idée lancée, le personnel du ministère doit lui donner corps et trouver des innovations techniques et culturelles à mettre en avant.

Un des organisateurs en parle à un membre de la Quadrature qu'il connaît par ailleurs. Dans la discussion, on évoque le *Book Scanner* : une structure en bois et en verre pour caler un livre ouvert, deux appareils photos pour photographier les pages, et un PC portable pour traiter les images et publier un PDF du livre à la fin[13]… L'équipe de l'événement adore l'idée : cet outil à fabriquer soi-même sera donc exposé au rez-de-chaussée du ministère de la Culture, du 15 au 28 mai 2014[14]. Trois bénévoles se relayent durant deux semaines pour faire la démonstration de la numérisation d'un livre, depuis le scannage jusqu'au fichier epub. L'œuvre de Victor Hugo va y passer… ainsi que le roman de la ministre de l'époque, Aurélie Filippetti, *Un homme dans la poche*. Réussir à faire la promotion du partage aux agents du ministère de la Culture, alors qu'on s'oppose depuis des années sur la même idée, c'est une petite victoire qui ne se refuse pas…

Cela prouve qu'en 2014 le dialogue avec nos représentants politiques est possible. Nous jouons alors sur notre jeunesse et notre maîtrise des nouvelles technologies, si peu comprises de nos élus, pour tenter d'insuffler de nouvelles idées. Par la suite, malheureusement, nos relations se dégraderont…

5. CES POLITIQUES QUI VEULENT TOUT CONTRÔLER

Le vieux monde est grand et lourd, son inertie forte. Il est lent à réagir, comme ces navires géants qui continuent de naviguer droit devant sans réussir à virer de bord. Mais le pouvoir est fort, et quand il veut reprendre la main, c'est une main de fer qu'il brandit.

Devant les nouveautés du numérique et les nouvelles formes d'organisation et d'expression de la contestation, les pouvoirs institutionnels, pourtant riches de leur légitimité et de leur savoir-faire de haute volée, passent d'abord pour des dinosaures, des machines dépassées, voire des idiots. Mais c'est seulement dans un premier temps.

Alors jeunes geeks de la Quadrature (et d'ailleurs), nous avons cru que le pouvoir politique était un peu à la traîne, et qu'il suffirait de lui expliquer les choses (en riant au passage de sa ringardise) pour que tout rentre dans l'ordre après quelque temps de confusion. Ce qui apparaît finalement met fin à notre naïveté : le pouvoir ne cherche pas à comprendre. Il est avant tout fidèle à lui-même, et suit dans le domaine du numérique la logique qui est la sienne dans tous les autres domaines : imposer ses intérêts, avec les méthodes qu'il maîtrise.

Bousculées, désarçonnées par une mobilisation inattendue et imprévisible, les institutions se tournent vers leurs interlocuteurs et leurs partenaires habituels. Parmi ceux-là, se trouvent bien sûr les entreprises privées, loyales et de bon conseil, et notamment les grands groupes internationaux.

De nombreux travaux d'économie politique l'expliquent, soit en exhumant les textes fondateurs, soit en constatant la réalité : le rôle attribué par le néolibéralisme à l'État est celui de protecteur du libre marché, qu'il doit préserver et faciliter[1]. Ainsi, les entreprises seront constamment aidées, défendues, soutenues, et leurs obligations considérées comme des entraves à lever. Il s'agit de démolir les barrières, d'araser les obstacles, d'élargir les voies de circulation, mais toujours en faveur des entreprises privées et des besoins du marché. Toutes les autres considérations sont dès lors secondaires, même dans des domaines d'ordre moral. Et pour une association qui défend des choses aussi immatérielles que des libertés ou des droits, c'est un obstacle récurrent. Au nom d'un « réalisme » à sens unique, les grandes idées sont souvent balayées par le sens des affaires.

Cela ne veut pas dire que la lutte ne vaut pas la peine d'être menée : on n'est jamais à l'abri d'une victoire. Les activistes peuvent changer la perception des choses et infléchir leur cours cynique. L'histoire de la défense de la neutralité du Net en est un bon exemple. Elle montre aussi qu'aucune victoire n'est définitive. Et que la bataille reprend sans cesse.

LA NEUTRALITÉ DU NET : BATAILLE POUR UNE DÉFINITION

Le fossé entre la logique de l'État et la réalité des pratiques du Net s'est révélé particulièrement flagrant en 2008, au moment de la bataille sémantique entre « piratage » et « partage ». Dès 2009, la Quadrature doit mener une autre bataille de vocabulaire, mais il ne s'agit pas cette fois d'imposer un autre mot en face des mots du pouvoir : nous cherchons à imposer dans le débat public une notion positive que nos adversaires jugent mauvaise. Le motif de la querelle est d'ailleurs assez paradoxal, puisqu'il est question de définir « la neutralité du Net ».

De quoi parle-t-on ? La neutralité est un principe fort de l'internet, dès son origine : le réseau transporte (ou du moins doit transporter) toutes les données de la même manière, quelles que soient leur nature,

leur origine et leur destination. La neutralité du Net n'a donc rien à voir avec une quelconque neutralité d'opinion : on ne parle pas de ce que les gens racontent en ligne, ni des obligations des hébergeurs ou des auteurs des sites, mais bel et bien du réseau matériel lui-même, et du rôle des fournisseurs d'accès qui connectent les gens entre eux. Il s'agit d'une impartialité technique. Certaines personnes préfèrent d'ailleurs parler de « neutralité des réseaux ».

Le Net est un réseau, et même un « réseau de réseaux », par lequel circulent de nombreuses données, dont le Web – avec ses sites, ses pages, ses forums, ses services commerciaux et son célèbre « www » – n'est qu'une partie seulement. Le réseau Internet véhicule beaucoup d'autres échanges et d'autres données en dehors du Web proprement dit : un téléchargement de document, un transfert de fichiers par le protocole FTP, l'envoi d'un e-mail, le flux d'images d'une chaîne de télévision ou d'un service de vidéo à la demande, les échanges de données entre deux personnes qui jouent en ligne au même jeu vidéo, des données météo, des transactions bancaires, des données de navigation pour des voitures connectées, etc. Ces différents formats d'échanges suivent des protocoles techniques distincts, réunis dans ce qu'on appelle par simplification la « couche TCP/IP » : dans tous les cas, des câbles et des serveurs transportent des paquets de données, que le réseau doit considérer comme étant tous égaux.

Pour les fournisseurs d'accès à Internet (FAI) privés, cette neutralité du réseau n'a pas de sens, ni d'un point de vue technique, ni d'un point de vue commercial. D'un point de vue technique, il est tout à fait préférable d'avoir une connaissance fine des flux de données pour mieux les réguler, par exemple pour que la vidéo ne monopolise pas le débit d'une ligne, afin d'assurer un service fluide et homogène. D'un point de vue commercial, c'est encore plus intéressant : si l'on peut appliquer des traitements différents à des trafics de nature différente, alors on peut aussi les facturer à la carte, et décliner une offre commerciale de façon très lucrative. Par exemple, on peut imaginer une gradation de forfaits : forfait basique pour pouvoir juste envoyer et recevoir des e-mails, forfait

standard pour les e-mails et la navigation Web, forfait mélomane pour écouter de la musique en *streaming*, forfait cinéphile pour regarder de la vidéo à la demande, etc.

Au lieu de cela, nos abonnements nous donnent tout simplement accès à Internet, et c'est très bien comme ça. Mais pour les opérateurs de réseaux, la neutralité est considérée comme une contrainte absurde et contre-productive : on a besoin d'intervenir pour maximiser le fonctionnement, on a besoin d'intervenir pour bloquer les attaques, on a besoin d'intervenir pour augmenter ses revenus, etc.

Mais alors, d'où vient ce principe de neutralité, et comment s'est-il imposé ? On peut déjà se rappeler que le réseau Internet est le fruit de la collaboration de militaires et d'universitaires. Ces deux corporations, pourtant très étrangères l'une à l'autre, partageaient dès le départ des attentes communes au sujet d'Internet : qu'il soit résistant, et qu'il permette un partage homogène de l'information. Pour les militaires, en raison des nécessités du commandement, la fluidité et la rapidité des échanges avec toutes les parties de l'armée étaient vitales. Pour les universitaires, l'enjeu était de diffuser le plus largement possible le savoir humain, né de la circulation des idées et constitué par le jeu permanent de la confrontation et de l'échange.

Dès lors, l'homogénéité et la résistance du réseau ont marché ensemble de manière inséparable : si le réseau est bien conçu, c'est-à-dire décentralisé, alors chacun de ses points peut accéder à l'information, et à l'inverse rien d'essentiel au fonctionnement global n'est perdu si l'un de ses points est détruit. Pour les universitaires, cela assure la circulation des connaissances, et leur sauvegarde, dans le respect d'une vision égalitaire et généreuse de la société. Pour les militaires, c'est la garantie d'un commandement et d'un renseignement efficaces, et la certitude de pouvoir continuer les opérations même si des serveurs sont détruits : les données qu'ils contiennent existent ailleurs, et les routeurs trouveront le meilleur chemin disponible pour aller les chercher. L'homogénéité du réseau Internet est donc capitale pour sa solidité et son efficacité. Chaque dissymétrie comporte un risque de blocage, d'étranglement, de

centralisation, donc de faiblesse structurelle. La neutralité puise sans doute une partie de sa légitimité dans cette logique de résistance et d'égalité fonctionnelle voulue par les créateurs du réseau.

La neutralité du Net est d'ailleurs un sujet défendu par la Quadrature depuis sa fondation, comme en témoigne le nom de la coquille associative constituée en 2008 pour payer le premier salaire de l'association : le Fonds de défense de la neutralité du Net (FDN²)…

Quels sont donc les enjeux de la neutralité du réseau pour une association de défense des droits et des libertés ? Tout est déjà dans le premier article consacré exclusivement à la neutralité du Net et publié le 4 septembre 2009 : « Il est crucial de préserver la neutralité du Net ! ». Il lance un cri d'alerte : « Elle est aujourd'hui menacée par les opérateurs de réseaux qui voient des opportunités commerciales dans le contrôle des flux d'informations qu'ils véhiculent[2]. »

On pourrait être tenté de croire que la menace est purement rhétorique, une exagération de militants qui n'hésitent pas à grossir le trait pour inquiéter et attirer l'attention. Et pourtant, les opérateurs (FAI) ont mille et une idées pour gagner de l'argent en bidouillant leur réseau. Par exemple, ils inventent le *zero rating* : certaines données ne sont pas décomptées du forfait de l'utilisateur. Les FAI favorisent ainsi leurs propres services connectés, ou ceux avec lesquels il a passé les meilleurs accords commerciaux (telle messagerie instantanée, tel bouquet de chaînes de télévision, tel réseau social, etc.). En revanche, les données liées à l'utilisation d'autres services (même similaires) sont bien décomptées. Les utilisateurs qui veulent économiser leur petit forfait pour qu'il dure tout le mois sont donc bien orientés, par l'opérateur du réseau et par le fonctionnement même du réseau, dans leurs pratiques du Net : la neutralité est largement brisée. Aujourd'hui, en France, les forfaits Internet et téléphoniques sont souvent « illimités », c'est-à-dire plafonnés si haut qu'on ne se soucie guère du volume de données que l'on consomme. Mais le *zero rating* est encore pratiqué dans d'autres régions du monde.

Autre astuce des opérateurs pour contourner l'obligation de neutralité : les « services spécialisés », ou « services gérés ». Les exemples les plus simples sont le téléphone et la télévision numérique. Aujourd'hui, de très nombreux foyers téléphonent et reçoivent la télévision en passant par la box de leur fournisseur Internet. Prenons la télévision : ces flux d'images de plus en plus lourds (haute définition, 5K, etc.) sont priorisés par rapport aux autres usages, sur la ligne ADSL ou fibre de l'abonné. Si vous étiez en train de télécharger un film ou une série pour ce soir, et que vous allumez le journal télévisé de 20 heures, vous verrez votre débit de téléchargement chuter[3]. La contrainte technique est légitime : en privilégiant le flux télé, l'opérateur s'assure que le client verra une vidéo fluide et de bonne définition, ce qui est le service pour lequel l'opérateur est payé. En revanche, s'il profite de cette tolérance pour privilégier uniquement les chaînes de télévision avec lesquelles il a passé un accord commercial, alors l'exception technique à la neutralité du Net devient un abus de position dominante.

Les « services gérés » sont un cas particulier des exceptions à la neutralité tolérées pour des raisons techniques, et réunies sous le terme de *Quality of Service* (*QoS*). Elles comportent par exemple des possibilités de réduire volontairement (mise en forme) ou de prioriser (ordonnancement) certains flux de données par rapport à d'autres, pour que l'ensemble du réseau reste fluide. Mais les fournisseurs d'accès associatifs, des opérateurs locaux souvent présents en zones rurales, et qui n'ont pas l'ambition commerciale des grands FAI nationaux, expliquent que ces exceptions ne sont en réalité pas des nécessités absolues, mais bel et bien des facilités offertes par le législateur à des entreprises qui usent et abusent de l'opacité technique de leur métier pour obtenir des passe-droits sous prétexte d'efficacité technique.

Il n'est pas évident de défendre Internet en tant que bien commun et service universel, quand on a pour interlocuteurs des opérateurs commerciaux privés qui se livrent une concurrence de chaque instant. C'est pourquoi la Quadrature tient aussi, à côté de son discours humaniste et universaliste, un discours audible par les entreprises privées

et par les gouvernements libéraux qui les représentent : celui de la libre concurrence.

Déjà, dans la lutte contre la loi Hadopi et sa « riposte graduée », on avait eu recours à des arguments piochés dans le champ de sensibilité de l'adversaire. Tout comme, à l'automne 2009, les articles de la Quadrature à destination des ministres chargés de la conciliation du « paquet Télécom » étaient remplis de cette rhétorique des entreprises, de ce langage des décideurs. De fait, ne pas respecter la neutralité du Net revient à introduire dans le droit une distorsion de concurrence : « Si un fournisseur d'accès porte atteinte à la neutralité du Net, il peut très facilement favoriser ses services par rapport à ceux de ses concurrents[4]. » En poursuivant le raisonnement, on peut même montrer que ce déséquilibre est une entrave à l'innovation technique.

Bien sûr, ces arguments en faveur de la compétition ouverte et de la libre concurrence doivent être entendus en gardant en tête que nous, militants de la Quadrature, sommes des *libristes*, c'est-à-dire des partisans et des pratiquants de la culture du logiciel libre, disponible pour tous et modifiable par tous. Vouloir un Internet « libre, neutre et ouvert » où des groupes privés ne bride pas les possibilités et ne montent pas la garde à l'entrée, c'est aussi la meilleure garantie de donner ses chances à un écosystème partageur, humaniste et mondial.

À côté de ces arguments destinés aux entrepreneurs, on trouve aussi des arguments politiques plus généraux qui sont devenus des classiques de la Quadrature : en l'espèce, l'enjeu consiste à faire reconnaître l'accès à Internet comme un droit pour chacun.

OPÉRATION RESPECTMYNET

On l'a déjà dit, militer pour la neutralité du Net, c'est défendre un principe généreux mais non lucratif, contre les intérêts commerciaux de la plupart des opérateurs techniques, qui ne lâcheront jamais l'affaire, vu

la taille du gâteau. Il faut donc sans cesse réorganiser la défense et tenir bon.

Après le texte européen mollasson de novembre 2009, on aurait pu penser qu'une forme de compromis et de statu quo avait été trouvée. En France, l'ARCEP, l'autorité régulatrice des télécoms, semble prendre au sérieux l'enjeu de la neutralité et travailler sur le sujet. Mais en plein été 2011 – alors que nous mettons beaucoup d'énergie dans l'action transnationale contre le traité ACTA –, de mauvais signaux nous parviennent de Bruxelles.

La commissaire européenne chargée de la société numérique, Neelie Kroes, reçoit officiellement les opérateurs et des dirigeants d'entreprises connues pour leur lobbying hostile à la neutralité du Net. Elle explique publiquement que ce qu'ils demandent est sans danger réel, et même bon pour les affaires, et que le marché régulera les choses de lui-même (avec sa fameuse petite main qu'on ne voit pas, mais qui pousse chacun à choisir finalement le bon opérateur). La menace sur la neutralité du Net est directe, précise, imminente[5]. Mais la commissaire feint de penser que les petits écarts et les bidouillages des opérateurs ne sont pas des atteintes réelles à la neutralité, et qu'il n'existe aucune nécessité de légiférer fermement en la matière. En somme, on agira plus tard, et seulement en cas de besoin…

Une campagne militante européenne se met aussitôt en place, pour collecter et publier des exemples concrets d'atteintes réelles à la neutralité du Net. Les internautes de toute l'Union européenne sont invités à témoigner sur un site unique : RespectMyNet.eu. Le site n'est plus en ligne aujourd'hui, ce qui rend difficile d'évaluer a posteriori le succès de l'opération. Mais on reconnaît les méthodes chères aux fondateurs de la Quadrature : l'appel aux bénévoles, le *crowdsourcing*, l'émulation et le travail en commun.

La mobilisation permet de ralentir les attaques contre la neutralité du Net. Une des commissions du Parlement européen adopte en octobre une résolution sur « l'internet ouvert et la neutralité du Net » appelant, bien que mollement, à les préserver.

Un peu plus tard, en 2012, la Quadrature répond à une consultation de l'ARCEP sur la neutralité du Net et rédige des propositions positives, toujours valables aujourd'hui[6]. Et le temps passe de cette manière, d'escarmouche en escarmouche.

Le dénouement n'arrivera qu'en avril 2014, par le biais d'un règlement sur le « marché unique européen des communications électroniques ». À la Quadrature, les têtes ont changé[7], mais le plaidoyer auprès des parlementaires européens, des commissaires et des émissaires français n'a jamais baissé d'intensité – en particulier en direction de la commissaire Kroes, toujours aussi rétive à trancher, et des parlementaires susceptibles de contrebalancer son influence.

Le 3 avril 2014, la Quadrature publie enfin un communiqué de victoire. Sur la photo qui illustre l'article, on voit même le sticker logo emblématique de l'association, un pi noir, appuyé contre une bouteille de champagne qui ne demande qu'à être ouverte. Le ton est au soulagement : « Le texte adopté inclut une définition rigoureuse de la neutralité du Net, en lui conférant une portée normative. Tout en permettant aux opérateurs de développer des offres d'accès avec une qualité de service optimisée pour des applications qui ne pourraient pas fonctionner correctement sur l'internet "classique", ce texte encadre efficacement de tels "services spécialisés" en assurant qu'aucune discrimination ne puisse être réalisée entre les différents fournisseurs de telles applications et en protégeant la bande passante allouée à Internet[8]. » Le compte est bon.

Malgré les réserves de prudence – le texte peut encore être modifié par les gouvernements réunis dans le Conseil de l'Europe, et il faut donc rester mobilisé –, le communiqué ne cache pas la jubilation des membres de l'association : « La victoire d'aujourd'hui sur la neutralité du Net est la plus importante pour la protection des libertés en ligne depuis le rejet de l'ACTA en juillet 2012. »

Un sentiment rare et précieux, d'autant plus que, sur d'autres fronts, les nouvelles ne sont pas bonnes du tout…

LOPPSI : LA CENSURE SANS JUGE

Il faut s'imaginer l'état d'esprit post-Hadopi. La chasse acharnée au téléchargement illégal crée une ambiance de paranoïa : l'internaute français lambda, qui télécharge un film de temps en temps, découvre qu'il est techniquement sous surveillance et que son activité sur Internet est potentiellement répréhensible. Sans compter le « défaut de sécurisation » potentiel de sa connexion… L'idée que l'on puisse cliquer sur un lien et recevoir la visite de la police n'a plus rien de délirant. Et c'est sans doute un effet de la loi que le gouvernement Fillon n'est pas vraiment fâché de voir s'installer dans les esprits…

Mais comment le fait de télécharger des films a-t-il pu faire l'objet d'une telle répression, et amener des législateurs à décider d'espionner les activités en ligne de millions d'internautes ? Hypnotisés sans doute par les discours angoissants de l'industrie culturelle, pour laquelle il était plus facile de réprimer à court terme que d'évoluer à toute vitesse, ils ont cédé à la pente de la facilité, et à l'esprit du temps. Il y a peut-être dans cette réaction disproportionnée un fond psychologique de peur et d'incompréhension.

Toutefois, les politiques ont bien compris que le réseau est aussi une formidable machine de surveillance, que les gens installent eux-mêmes, et avec enthousiasme. Parmi les propositions de la Quadrature au sujet de la neutralité du Net[9], on lit ceci : « Il est nécessaire d'encadrer l'utilisation des technologies d'inspection des paquets de données afin de protéger le secret des correspondances et l'intégrité des communications électroniques. » C'est-à-dire qu'un paragraphe sur la gestion technique des réseaux se termine sur une phrase qui évoque littéralement l'espionnage des correspondances.

De quoi s'agit-il ? La technologie de l'inspection profonde des paquets de données, ou *Deep Packet Inspection* (DPI) en anglais, consiste à jeter un œil à l'intérieur de l'enveloppe qui transporte les données (le paquet) pour voir ce qu'il contient. Normalement, un routeur « neutre » a

besoin de lire seulement l'en-tête du paquet, pour savoir dans quelle direction l'orienter, mais si on rompt la neutralité du Net, pour des raisons techniques ou policières, alors il est important de connaître la nature des données transportées, pour savoir si elles sont prioritaires… ou suspectes. Les techniques sont les mêmes. Autrement dit, si la neutralité du Net est capitale, c'est aussi parce qu'elle est un frein à la surveillance de nos échanges numériques. Et dans la tête des législateurs peureux et sans imagination : contrôler, c'est surveiller.

Nous le savions bien et pourtant, l'article que le magazine *Next INpact* publie le 6 juin 2008 est une surprise : « Exclusif : le gouvernement veut un filtrage de masse des réseaux[10] ». L'objet du scoop, c'est une initiative discrète du gouvernement Fillon : « Le gouvernement tente actuellement de faire signer d'ici le 10 juin par les FAI, les opérateurs de télécoms et les prestataires (fournisseurs en ligne et éditeurs) une charte dite sur la "confiance en ligne". Ce document, issu du ministère de l'Intérieur, est une petite bombe pour ces fournisseurs de tuyaux plus habitués à la neutralité de leur fonction. »

Que contient cette charte ? Les FAI qui la signent s'engageraient à filtrer les connexions en *peer-to-peer* (la voie privilégiée du téléchargement « illicite » à l'époque), à lutter contre le spam, à informer les internautes sur les arnaques en ligne (*phishing*, *spywares*), à bloquer l'accès des mineurs aux sites pornographiques, à filtrer les contenus accessibles aux mineurs (vaste programme) et, bien sûr, à dénoncer à la police les sites pédophiles et les contenus répréhensibles (racisme, négationnisme, etc.). C'est une des premières tentatives de l'État de faire porter tout le poids de la police du Net sur les épaules des intermédiaires techniques et des hébergeurs.

La Quadrature réagit aussitôt et publie un article le même jour : « Le but du pouvoir exécutif français n'est pas de lutter efficacement contre la criminalité avec des mesures adéquates car nécessaires, appropriées et proportionnées. Il s'agit de contrôler par tous les moyens le seul média libre qui ne lui obéit pas », déclare Christophe Espern, ajoutant : « Il y a quelque chose d'odieux à utiliser la lutte contre la pédopornographie

comme alibi à Big Brother. Les services de police concernés ne demandent pas de telles mesures. Parler de confiance en ligne dans ce contexte relève de la novlangue[11]. »

La fin de l'article énumère de façon très claire les axes d'action de l'association : « La Quadrature du Net appelle donc les citoyens à contacter immédiatement leurs députés pour leur demander d'interpeller le gouvernement lors des prochaines questions d'actualité. Elle les invite à se former aux techniques d'anonymisation et de chiffrement et publiera prochainement un guide permettant aux citoyens de se protéger de l'arbitraire numérique. Elle appelle en outre les intermédiaires techniques à refuser catégoriquement toute forme de collaboration avec ces projets indignes d'une démocratie. » On reconnaît la mobilisation des citoyens, la formation pratique, et l'interpellation des décideurs : les industriels, les législateurs ou même l'exécutif.

Les termes du débat sont donc posés : il faut surveiller Internet parce que les gens téléchargent des films et parce qu'il faut traquer les pédophiles.

En mai 2009, moins d'un an après l'affaire de la charte, le gouvernement Fillon dépose un projet de loi intitulé « loi d'orientation et de programmation pour la performance de la sécurité intérieure » (LOPPSI). Le mot « performance » peut surprendre – il doit même surprendre – mais il est révélateur de la cohérence idéologique du néolibéralisme à la française : dans un sens la protection de la rentabilité économique conduit à faire des lois répressives (Hadopi), et en retour les lois sécuritaires empruntent le vocabulaire de l'efficacité. La productivité, on le sait, est entrée dans le vocabulaire de la police sous le quinquennat de Sarkozy, et la rentabilité dans celui de l'ensemble de la fonction publique, jusque dans les hôpitaux et les écoles. Mais revenons à nos lois sécuritaires.

Le 27 mai 2009, la Quadrature livre sa première lecture du projet de loi LOPPSI. Pour l'association c'est une évidence : l'action (nécessaire) contre les sites pédopornographiques sert de prétexte à une prise de contrôle du Web tout entier. Il s'agit par exemple d'instaurer une liste

noire de sites à bloquer, régulièrement mise à jour et transmise aux FAI. Un procédé fastidieux et peu efficace, trop facile à contourner, disent les spécialistes.

Il s'agirait surtout, et c'est ce qui inquiète le plus, de donner à la police le pouvoir administratif de supprimer directement des contenus ou des sites d'apparence illicite, sans la décision d'un juge. Ce qui causerait un scandale dans la rue et révolterait tout le monde de façon légitime (sanction arbitraire de la police, contrôle des discours et des actes…) paraîtrait donc aux yeux du gouvernement et de l'opinion publique parfaitement légitime quand cela se passe sur Internet. Tout le travail de la Quadrature va donc consister à expliquer au gouvernement et à l'opinion publique que non, cela n'est pas possible.

6. LA FIN DE L'INNOCENCE

Alors que les luttes autour d'Internet ont toujours été relativement bon enfant dans leurs modes d'action, les geeks que nous sommes s'aperçoivent d'un changement de paradigme. Nous prenons peu à peu conscience que la défense des libertés sur Internet couvre des enjeux bien plus importants que nous le pensions. Avec la Hadopi, le risque principal auquel s'exposait un utilisateur était de recevoir un recommandé et, éventuellement, dans un futur lointain et peu probable, de se voir suspendre sa connexion. Mais petit à petit, des figures majeures de la « résistance » sur Internet se font attaquer de manière bien plus violente que ce qu'on aurait pu imaginer, avec des conséquences parfois dramatiques. Cette succession de « défaites » fait entrer les militants dans une nouvelle ère, qui laisse derrière elle l'innocence, ou peut-être la naïveté, des premières années.

LE RENVERSEMENT DE LA BATAILLE CULTURELLE

Vous vous souvenez qu'en 2006 la police avait saisi du matériel informatique appartenant à The Pirate Bay. Après le resurgissement du site à travers de nombreux miroirs, les geeks étaient restés sur la « victoire » de l'*effet Streisand*. Mais pendant ce temps, la police suédoise a continué son enquête. Le procureur a rédigé un dossier à charge de 4 000 pages. Le 31 janvier 2008, les cofondateurs sont accusés de «

promotion de la violation du droit d'auteur », et un an plus tard, le 17 avril 2009, ils sont reconnus coupables et condamnés à des peines de prison.

En France, plus personne ne rit des recommandés de la Hadopi.

Petit à petit, à la Quadrature et tout autour de nous, il y a une prise de conscience. Les excités du droit d'auteur, les teigneux de la censure, les obnubilés du contrôle des réseaux viennent de faire passer la lutte pour le droit au partage dans une autre dimension. Les citoyens européens peuvent-ils maintenir le rapport de force ? Le jeune Parti pirate, qui défend une réforme du droit d'auteur et lutte contre les monopoles privés et les brevets, passe de 15 000 à 40 000 membres.

Du côté hacker, les Anonymous font parler d'eux. Ces pirates informatiques et activistes politiques (« hacktivistes ») issus du forum anonyme 4chan défendent depuis 2003 la liberté d'expression. Pour protester contre la sentence rendue contre les cofondateurs de TPB, ils lancent l'opération *Baylout*, et attaquent en DDoS[1] le site de la Fédération internationale de l'industrie phonographique (IFPI).

À la Quadrature, nous dénonçons de notre côté une « persécution politique du partage ». Entre panique et élan révolutionnaire, organisation citoyenne et culture du hacking, la résistance s'organise.

Aux États-Unis, cette résistance est notamment incarnée par Aaron Swartz. Ce jeune prodige du MIT décide de faire bénéficier le monde de son accès universitaire aux articles de recherche publiés sur la base de données du JSTOR[2]. Il branche ses disques durs dans la salle des machines de l'université et entreprend de récupérer chacun des articles de la base. Entre septembre 2010 et janvier 2011, il télécharge ainsi presque 5 millions d'articles, soit la quasi-totalité du JSTOR. Rien ne l'empêche de le faire : il est bien titulaire d'un accès à la base, et celle-ci ne prévoit aucune limitation du nombre de téléchargement par personne. Il sera pourtant poursuivi par une procureure américaine. Au fur et à mesure de l'enquête, Aaron et sa famille se retrouvent harcelés par le FBI. Après deux ans de pressions, il se suicide le 11 janvier 2013.

Aaron était, comme beaucoup de geeks, un idéaliste. Enthousiaste, il voulait libérer les données, pour le fun autant que par principe. Cet utopiste pointait l'absurdité du copyright apposé sur des articles académiques pour lesquels les auteurs n'étaient pas rémunérés – même si le JSTOR demandait des contributions financières pour y accéder. En face de lui s'est déployé le formidable bras armé du gouvernement fédéral américain : le FBI et les poursuites judiciaires d'une procureure qui requérait trente-cinq ans de prison pour des articles que Swartz n'avait finalement jamais publiés et qu'il avait même retournés au JSTOR. Les soldats zélés du copyright ont fini par faire un mort.

Son décès donne lieu à un élan de solidarité international dans le milieu hacktiviste. Sur Twitter, plusieurs universitaires décident de partager leurs publications en accès libre. TPB publie, sur l'un de ses nombreux miroirs, une archive des documents exfiltrés du JSTOR par Aaron. Quelques jours plus tard, le site Internet de la *Sentencing Commission* des États-Unis est remplacé par une vidéo dénonçant le traitement de l'activiste par la justice américaine. La même vidéo menace, en réponse, de divulguer des informations de l'armée américaine, de la *Missile Defense Agency*, et de la NASA. C'est Lauri Love, un hacker suédois affilié à Anonymous, qui sera pointé du doigt pour cette action. Il sera arrêté par la National Crime Agency anglaise en octobre 2013, à la suite des accusations et de la demande d'extradition des États-Unis.

Quelques années plus tard, alors que l'on suit encore, par intermittence, la traque du dernier cofondateur de TPB, Svartholm Warg, exilé au Cambodge pour fuir sa sentence, c'est un autre site bien connu des amateurs de séries télévisées qui fait parler de lui. Le 19 janvier 2012, le site de *streaming* MegaUpload affiche désormais les logos du FBI et du département de la Justice américaine, suivi du message : « Les noms de domaines liés au site MegaUpload.com ont été saisis, par décision de la Cour de Justice des États-Unis. »

Un quart d'heure après l'annonce, Anonymous est déjà sur le pont et lance l'opération #OpMegaUpload. Leur attaque en DDoS vise cette fois

une quantité impressionnante de cibles : Universal Music, la Recording Industry Association of America, la Motion Picture Association of America, l'U.S. Copyright Office, Hadopi, l'Utah Chiefs of Police Association, Broadcast Music Incorporated, Warner Music Group, le FBI et Sony. En parallèle, des milliers de messages de protestation sont publiés sur la page Facebook du FBI.

Mais la Quadrature et les défenseurs du libre partage n'ont pas le temps de s'apitoyer sur leur sort. La censure des contenus culturels, poussée par les ayants droit, laisse petit à petit la place à une censure plus large contre les contenus désapprouvés par les gouvernements. Et alors qu'on discute en France de la légitimité de la censure pour lutter contre la pédopornographie, le terrorisme, la prostitution ou les discours de haine, à quelques milliers de kilomètres de là, la censure totalitaire des réseaux est déjà en place.

LES GEEKS PRIS DANS LA GUERRE

La nuit est déjà bien avancée en Europe, elle commence tout juste aux États-Unis, et quelques geeks insomniaques discutent sur IRC[3]. Ils sont membres de Telecomix, un *cluster* de membres de toute l'Europe, sous pseudonymes, qui veut lutter contre les lois sur la surveillance.

Proche de la Quadrature, du Parti pirate suédois et d'autres mouvements similaires en Europe, Telecomix s'est engagé à ses débuts contre le « paquet Télécom » français et la loi suédoise FRA (qui autorisait la surveillance de masse de l'ensemble des communications électroniques entrant et sortant du pays). Le groupe, créé en 2009, met en avant des méthodes qualifiées d'« hacktivistes ». Au centre de leur éthique politique, le *datalove* (sorte de philosophie selon laquelle les données doivent être partagées) et la crypto-anarchie (l'idée que le chiffrement systématique des échanges en ligne permet de créer un « bruit » et de protéger les personnes qui en ont besoin en les rendant moins visibles).

Toujours est-il que même les hacktivistes, parfois, s'ennuient. Ce soir-là, ils ont entendu une rumeur sur un blocage d'Internet en Syrie. Alors ils lancent, juste pour voir, un petit programme de *mapping* d'adresses IP. Cartographier l'internet syrien : l'idée d'une soirée décontractée chez les hackers…

À l'issue de leurs investigations, ils font un constat surprenant. Le trafic Internet entre la Syrie et le reste du monde transite par une poignée d'adresses IP. En effet, des serveurs, fournis par la société BlueCoat au gouvernement syrien, interceptent tout le trafic entrant ou sortant du pays. Ils l'analysent, le surveillent, parfois le bloquent. Telecomix vient de découvrir toute une infrastructure de surveillance de la population, appliquée au pays tout entier, entre les mains d'un gouvernement autoritaire. Comment faire pour alerter cette population ?

Le 15 septembre 2011, la quasi-totalité du trafic Internet syrien est redirigée vers une page Web rédigée en anglais et traduite en arabe. Son titre ? « *Your Internet activity is monitored* » (« Votre activité Internet est surveillée »). Sa signature ? « Nous sommes Telecomix. Nous venons en paix[4]. »

La page renvoie vers une collection d'outils de contournement de la surveillance et de la censure, avec un lien vers l'IRC du groupe. Sur l'IRC justement commencent à arriver des Syriens surpris qui demandent, en arabe, ce qu'il se passe. C'est le début de conversations par traductions Google interposées pour expliquer la situation, aider à installer des VPN[5]… Le tout dans l'anonymat le plus total. On ne donne pas son nom, sa localisation, ses infos personnelles. Personne ne se connaît, tout le monde se méfie, et à raison, des espions se cachent partout.

Les membres de Telecomix, sans rien avoir vraiment planifié, deviennent les fers de lance du soutien des hackers aux révolutions des Printemps arabes[6]. French Data Network propose ses serveurs aux Tunisiens, pour héberger les vidéos des exactions du régime, censurées localement. En Égypte, lorsque le trafic Internet est coupé par le

gouvernement, Telecomix envoie de vieux modèles de modems capables de se connecter au Web via le réseau téléphonique…

À force de traîner sur les réseaux, Telecomix parvient à identifier des machines au comportement particulier. Il s'agit de serveurs mettant en œuvre de la *Deep Packet Inspection*, une technique d'analyse en profondeur des informations passant par les équipements du réseau. Ces outils déployés par des agences gouvernementales, en deux mots, permettent aux gouvernements de surveiller l'activité des internautes dans leur pays. Extrêmement dangereux pour la liberté d'expression et la démocratie, ils sont développés et vendus par des entreprises occidentales, notamment françaises.

Collaborant avec des journalistes, Telecomix se lance dans l'identification de ces sociétés[7]. Amesys, filiale de la française Bull, officie en Égypte, où elle collabore avec Hosni Mubarak, le président-dictateur, qui sera, après la révolution, condamné à la prison à perpétuité (il risquait la peine de mort) pour « meurtre et tentative de meurtre sur des manifestants, abus de pouvoir et de biens sociaux, et atteinte aux intérêts de l'État ». À ses côtés, toujours en Égypte, on peut lister l'anglaise Gamma, qui fournit son logiciel FinSpy. Ou encore l'américaine Blue Coat, qui est également installée en Syrie, à Bahreïn, au Qatar, aux Émirats arabes unis, en Chine, en Russie ou encore au Venezuela.

En Iran, c'est Trovicor, de l'allemande Siemens, qui se charge du DPI. Au Maroc et aux Émirats, il s'agit de DaVinci, de l'italienne Hacking Team. En Syrie et en Libye, on retrouve encore une société française, Qosmos. Une autre, française encore, Alcatel, en Birmanie. Oui, la liste est longue. Déjà en 2012, l'exportation d'armes numériques se porte bien. Le débat est relancé pour savoir si on doit réguler l'export d'armes numériques de la même manière que les armes de guerre.

Le jeu du chat et de la souris se poursuit entre les geeks, portés par l'élan politique constitué autour de Telecomix, et les gouvernements dictatoriaux. Avec les Printemps arabes, c'est l'émulation : nous participons à la libération des peuples. Mais cette participation est

douloureuse : les longues nuits passées à conseiller les Syriens sur leurs moyens de protection numérique, la récupération des vidéos d'assassinat et de torture, la disparition du jour au lendemain de contacts dont on soupçonne qu'ils aient été arrêtés et torturés… Tous ces éléments contribuent à l'épuisement de la communauté hacktiviste, conduisant nombre d'entre eux au burn-out, à la dépression, et, parfois, au suicide.

On pourrait penser que l'exemple de la censure généralisée donné par les gouvernements totalitaires en Tunisie ou en Syrie aurait servi d'avertissement pour les démocraties occidentales. On pourrait penser que les enquêtes identifiant du matériel français utilisé par des dictateurs auraient tiré la sonnette d'alarme autour des moyens que nos services de renseignement ont déjà à leur disposition. On pourrait penser que la nomination de la France dans la liste des « pays sous surveillance » du rapport 2012 de Reporters sans frontières[8] aurait inquiété les citoyens.

Mais le vrai choc de la surveillance arrive juste un peu plus tard, quand un lanceur d'alerte de la NSA contacte WikiLeaks en juin 2013. Le nom d'Edward Snowden va bientôt faire la une des médias internationaux.

L'ÉMERGENCE DES LANCEURS D'ALERTE

WikiLeaks, ONG fondée en 2009 par Julian Assange[9], a pour but de publier des documents classifiés provenant de sources anonymes. L'association gagne en notoriété en révélant, en avril 2010, des documents confidentiels détaillant les agissements de l'armée américaine au cours de sa guerre « contre la terreur[10] », qualifiés de crimes de guerre. Parmi ceux-là, une vidéo de 2007 d'un raid aérien sur Bagdad en Irak, au cours duquel un soldat en hélicoptère ouvre délibérément le feu sur un groupe de civils, comprenant des journalistes de l'agence Reuters. Dix-huit personnes perdent la vie, dont deux enfants, au cours de trois frappes aériennes successives.

En juillet 2010, WikiLeaks publie les *Afghan War Diaries*. Il s'agit de plus de 90 000 documents et rapports de l'armée américaine en Afghanistan datés de 2004 à 2009. Ils révèlent des morts civils, des tirs de l'armée américaine contre son camp, et l'augmentation des attaques talibanes. *Der Spiegel*, *The New York Times* et *The Guardian*, qui se coordonnent pour la publication des premiers articles, affirment dans un communiqué qu'ils sont unanimement convaincus de l'intérêt public légitime qu'il y a à publier ces documents.

En novembre 2010, ce sont presque 250 000 télégrammes diplomatiques américains qui sont mis au jour (*Cablegate*). Ceux-ci traitent, entre autres, d'affaires d'espionnage, de torture, d'ingérence politique, de problèmes de sécurité nucléaire, de ventes d'armes, de corruption, et, plus généralement, des opinions et connaissances des uns et des autres sur leurs pays voisins.

Chelsea Manning, ancienne analyste militaire américaine, est très vite pointée du doigt par son administration. Elle est accusée d'être à l'origine de ces trois fuites et est condamnée en août 2013 à trente-cinq ans de prison. Reconnue responsable de la plus grande fuite de documents de l'histoire américaine, elle aura permis de révéler les sévices des forces américaines sur des prisonniers d'Abou Ghraib en Irak et de Guantanamo à Cuba, et l'utilisation, jusqu'alors niée par l'État, de drones d'attaques militaires. La peine prononcée à son encontre est plus lourde que celles des militaires reconnus coupables des actes de torture qu'elle a dénoncés. Par ailleurs, de nombreux rapports font état de ses conditions de détention, décrites par le rapporteur spécial des Nations unies sur la torture comme « cruelles, inhumaines et dégradantes ».

Mais revenons en France, fin 2010. Les documents de WikiLeaks sur le *Cablegate* sont hébergés sur un serveur de l'hébergeur français OVH. Éric Besson est alors ministre chargé de l'Industrie, de l'Énergie et de l'Économie numérique, poste qu'il prend peu après avoir clôturé le débat sur l'identité nationale pour lequel il avait été mandaté par Nicolas Sarkozy. Il demande aux autorités compétentes de mettre en œuvre des actions afin que WikiLeaks ne puisse plus être hébergé en France. Devant

les pressions exercées par le gouvernement, Octave Klaba, fondateur d'OVH, devra saisir la justice française. Il ne recevra néanmoins aucune notification officielle de contenu illicite.

Quelques mois plus tard, en novembre 2013, vient la condamnation de Jeremy Hammond à dix ans de prison. Hacker américain affilié aux Anonymous, il a publié en 2012 avec WikiLeaks des informations privées de l'entreprise Stratfor obtenues illégalement. Ces documents font état de la surveillance par le gouvernement de groupes écologistes en Inde, de militants du mouvement Occupy Wall Street, ou encore d'activistes de l'association PETA, qui œuvre pour la défense des animaux.

Cette série de condamnations contre des activistes, couplée à l'enfermement de Julian Assange dans l'ambassade d'Équateur à Londres, marque un tournant dans la pression judiciaire contre les hackers. Alors qu'ils pensaient avoir l'opinion publique avec eux, et que celle-ci leur permettait toujours de s'en sortir, les geeks déchantent.

Le 31 juillet 2013, la Quadrature plante les piquets de tente de sa Tea House[11] au Festival OHM, aux Pays-Bas, au cœur d'un rassemblement international de plus de 3 000 hackers. Dans ce champ au milieu de nulle part, de la fibre optique a été tirée et enterrée pour subvenir aux besoins de ces accros des données, diffuser en direct les conférences qui se succèdent dans les grandes tentes amphithéâtres, partager les fichiers sur les réseaux de PirateBox. En face de la Tea House, une tente en forme de Tardis[12], derrière elle, le Noisy Square, considéré comme l'endroit le plus militant.

Si les hacktivistes et les informaticiens se sont toujours côtoyés très cordialement, les choses commencent à changer. Les organisateurs du camp OHM sont notamment sponsorisés par Fox-IT, une entreprise épinglée peu de temps avant par WikiLeaks pour avoir développé un outil d'interception des communications et engagé des relations commerciales avec des pays comme l'Égypte ou l'Iran. L'entreprise a son stand à l'entrée du camp et s'en sert pour recruter.

Les entreprises ont toujours recruté des informaticiens, et les informaticiens ont toujours travaillé dans des grandes entreprises aux stratégies plus ou moins éthiques. Mais voilà, depuis les Printemps arabes et les révélations de WikiLeaks, les communautés hackers ont compris que le manque d'éthique fait des morts.

D'ailleurs, au sein de la Tea House, assis sur des coussins, autour de grandes tables rondes, les geeks discutent des dernières révélations publiées par WikiLeaks. À peine un mois auparavant, Edward Snowden, ancien employé de la CIA et de la NSA, a lancé l'alerte sur les agissements des agences du renseignement américain. On parle de PRISM, mais on ne sait pas encore très bien ce que cela recouvre. Les États-Unis nous surveillent, mais jusqu'où faut-il pousser la paranoïa ? S'ils savaient ! Même alors, on avait sous-estimé, et largement, la réalité des compétences de la NSA.

Julian Assange, fondateur et porte-parole de l'association, participe au camp d'OHM, grâce à une connexion en direct depuis l'ambassade d'Équateur à Londres. En 2013, il n'est plus possible de parler d'informatique sans parler d'éthique. De censure, de surveillance, de contrôle des populations.

La discussion se poursuit en décembre, à un autre rendez-vous important de la culture hacker : le Chaos Communication Congress. En cette trentième édition, le 30C3, Julian Assange (à distance) et Jacob Appelbaum, journaliste et figure de proue du réseau Tor[13], lancent un appel : « *Sysadmin of the world, unite !* » (« Administrateurs systèmes du monde entier, unissons-nous ! ») Le message est de résister aux sirènes des organismes politiques et des entreprises privées de surveillance qui viennent recruter les meilleurs informaticiens, jusque dans les événements communautaires comme le Congress.

Mais alors que les révélations tombent au fur et à mesure que les journalistes du monde épluchent les documents fournis par Edward Snowden ; alors que la situation des pays arabes dégénère sous les yeux de Telecomix qui continue à archiver tant bien que mal les vidéos d'assassinat et de violences ; alors que jouer à produire des *effets*

Streisand peut désormais conduire en prison… Est-il encore temps de s'unir ? N'avons-nous pas déjà perdu ?

En France, le Sénat vient d'adopter le projet de loi relatif à la programmation militaire. Envers et contre tout, la Quadrature continue tant bien que mal la lutte. Mais en 2013, c'est certain, l'hacktivisme a passé un cap. C'est la fin de l'innocence…

PARTIE : DE L'OBSESSION (ANTI)TERRORISTE À LA SURVEILLANCE DES GÉANTS DU WEB - (-)

1. DU PRÉTEXTE À LA PANIQUE ANTITERRORISTE

Quelques mois à peine se sont écoulés depuis les révélations d'Edward Snowden sur l'espionnage massif des citoyens, conduit par la NSA américaine, quand la loi de programmation militaire (ou LPM pour les initiés) arrive au Parlement français. Elle est présentée au Sénat le 2 août 2013, où elle est discutée au mois d'octobre. Devant l'amplification des menaces terroristes qui pèsent sur la France, la LPM reprend les propositions du « Livre blanc sur la défense et la sécurité nationale[1] » paru le 29 avril 2013 et approuvé par le président de la République, François Hollande.

Parmi ces propositions figure le renforcement de l'accès aux données informatiques par les services de renseignement de la police et de la gendarmerie. Il s'agit d'accéder à la fois aux données de connexion (logins de connexion, métadonnées d'un e-mail ou de SMS) et au contenu des correspondances. Pour la majorité parlementaire, la volonté est « d'harmoniser » les différents cadres existants. Néanmoins, au fur et à mesure des débats, on comprend qu'« harmoniser » signifie surtout « étendre l'accès », en permettant aux services de renseignement de s'adresser non plus seulement aux fournisseurs d'accès à Internet (FAI), mais aussi aux hébergeurs de contenus. La LPM cherche aussi à allonger la liste des administrations qui peuvent accéder à ces données : aux ministères de la Défense, de l'Intérieur et des Douanes s'ajoutent désormais ceux de l'Économie ou encore du Budget.

Enfin, elle veut élargir la nature des données concernées elle-même, pour y inclure par exemple la géolocalisation. Jean-Pierre Sueur, sénateur de la majorité et auteur de l'amendement, explique que cela permettra d'encadrer des pratiques qui « existaient sans bases juridiques ». En d'autres termes, les services de renseignement demandaient et utilisaient déjà ces données, alors que celles-ci n'étaient pas explicitement prévues par la législation précédente. Il s'agit d'une absence dans la loi. D'une zone grise. L'action n'est donc selon eux pas illégale, mais plutôt « a-légale ». Jolie argutie rhétorique, que l'on retrouvera par la suite quand il sera question de valider a posteriori des activités illégales de la police ou du renseignement.

LA DÉMOCRATIE À L'ÉPREUVE DES LOIS SÉCURITAIRES

Demander des informations à des tiers, voyez-vous, c'est un peu long. Alors le gouvernement propose la mise en place d'une collecte « en temps réel » des données grâce à la « sollicitation » du réseau. Cette formulation est floue, très floue. Techniquement, personne ne sait vraiment à quoi elle correspond. Ce flou conduit certains observateurs[2], nous y compris, à se demander s'il s'agit d'installer des dispositifs d'interception directement sur les équipements du réseau (câbles, serveurs, équipements des FAI, antennes de téléphonie…) – comme a pu le faire la NSA dix ans auparavant en aspirant une copie des données transitant par les câbles de fibre optique sous-marins dans l'énigmatique « Room 641A ». Ces spéculations inquiétantes présagent des futurs débats sur ces dispositifs d'interception, surnommés « boîtes noires », car destinés à enregistrer tout ce qui (se) passe sur le réseau. Nous y reviendrons.

De fait, la loi permet la capture en temps réel et sur simple demande administrative, donc sans supervision ni mandat judiciaire, des informations et des documents traités dans les réseaux concernant tout un chacun, et rendant permanents des dispositifs qui n'étaient que

temporaires. Elle passe à l'Assemblée dans une relative indifférence à l'automne, puis est adoptée par le Sénat en décembre, malgré notre mobilisation, relayée dans certains médias[3].

La seule institution encore capable de s'y opposer est le Conseil constitutionnel. Alors que la Quadrature avait gagné ses lettres de noblesse du militantisme en s'immisçant dans le débat parlementaire via le lobbying citoyen, nous devons désormais lutter pour nos idées sur le plan judiciaire, en engageant des procédures. Nous appelons ainsi solennellement les parlementaires à déposer une saisine du Conseil constitutionnel pour que ce dernier se prononce sur la conformité de cette loi à la Constitution. Et nous signons trois jours plus tard une lettre ouverte avec la Fédération internationale pour les droits humains (FIDH), la Ligue des droits de l'homme (LDH) et Reporters sans frontières[4].

C'est dans la foulée de ces événements qu'est créé, le 28 janvier 2014 (journée internationale de la protection des données personnelles), l'Observatoire des libertés et du numérique (OLN). Son but ? « Sensibiliser et alerter l'opinion publique sur les dérives possibles, utiliser tous les instruments juridiques disponibles afin de défendre les droits et les libertés. […] Initier et encourager les oppositions à tout projet liberticide. […] Dénoncer, d'une part, la prolifération des moyens de surveillance dans tous les domaines de la vie privée et socio-économique et, d'autre part, la généralisation de la collecte, du stockage, de l'utilisation et de la réutilisation indus des données personnelles. [Appeler] à la mise en œuvre de dispositifs de contrôle effectifs des fichiers et des technologies de surveillance actuelles et à venir ainsi qu'au développement de protections effectives des données personnelles. » Vaste programme, qui rappelle furieusement les missions que s'est données la Quadrature. C'est donc sans surprise que nous rejoignons l'OLN (et nous en faisons toujours partie).

2014 va être une année charnière pour le paysage politique français. Alors que la LPM n'est pas encore mise en place (son décret d'application n'arrivera qu'un an plus tard), les choses s'accélèrent : le terrorisme, épouvantail rhétorique dans les discours politiques depuis des

années, devient plus tangible dans la vie des Français et des Européens. Daech proclame en juin 2014 un califat entre l'Irak et la Syrie : l'État islamique. La menace terroriste se répand avec un souffle nouveau dans le champ médiatique occidental. La France découvre l'existence de djihadistes radicalisés sur son territoire, qui partent en Syrie se former et prendre les armes.

Le même mois, Guillaume Larrivé, député UMP, propose dans un rapport une batterie de mesures pour stopper ces « loups solitaires ». Ce rapport commence par une section intitulée « Internet est devenu le premier vecteur de la propagande djihadiste et le principal moyen de recrutement de terroristes ». Cette inquiétante déclaration donne le ton des actions prescrites par le rapport, qui vont de la création d'une « liste noire » de sites à censurer (car faisant l'apologie du terrorisme), à celle d'un délit de consultation habituelle de ces sites, en passant par l'instauration d'une « cyberpatrouille ».

Certes, il serait stupide et contre-productif de nier qu'Internet est utilisé efficacement par les mouvements terroristes (de toutes sortes) pour diffuser leurs idées et recruter, mais il y a un pas certain à dire qu'il est le principal moyen de recrutement des terroristes, un pas que le rapport franchit sans hésitation sans pour autant étayer son propos par des études. À la place, de multiples témoignages, dont ceux de responsables des services de renseignement qui sont – on peut presque les comprendre – les premiers à demander plus de pouvoirs sur Internet. À la même période, on assiste à une réorganisation des services de renseignement français, la Direction centrale du renseignement intérieur (DCRI) devenant en avril la Direction générale de la sécurité intérieure (DGSI). Qui dit « direction générale » dit pouvoirs, effectifs et budgets étendus. Demander à ceux dont le rôle est de surveiller s'ils souhaitent obtenir plus de pouvoirs plutôt que de s'appuyer sur des analyses chiffrées de la situation aboutit invariablement à renforcer la mainmise des services de renseignement sur Internet.

Du côté de la Quadrature, le potentiel de détournement de ces mesures pour porter atteinte aux libertés fondamentales des citoyens

saute aux yeux. Au-delà de l'inefficacité technique des mesures de censure, inévitablement contournables par les personnes un tant soit peu motivées, l'idée d'un délit de consultation de sites terroristes pose de réelles questions politiques et éthiques : qui décide de ce qui est terroriste ? Qui en a la légitimité ? Il n'y a pas grand débat à rappeler que les terroristes des uns sont les défenseurs de la liberté des autres. En pratique, la qualification de « terroriste » n'est souvent pas évidente et elle est de plus une arme politique puissante – le traitement des Black Panthers en est un exemple. Et la censure : sur quels critères est-elle décidée ? Ceux-ci sont-ils publics ? Peut-on vérifier, liste à l'appui, qu'ils sont correctement appliqués ? Et si ce n'est pas le cas, comment croire que les décisions ne verseront pas dans l'arbitraire ? Quoi qu'il en soit, la « liste noire » ainsi compilée ne devient-elle pas un annuaire, dont l'efficacité est aussi fluctuante que les changements d'adresse des sites Web ?

En outre, ce très orwellien « délit de consultation de sites terroristes » accorde un pouvoir de conviction quasi magique à ces sites, si dangereux que le bon peuple ne devrait même pas pouvoir les voir, au risque de tomber sous leur charme. Il simplifie également de manière caricaturale les raisons de consulter un site de propagande de Daech, en les réduisant à une seule : l'« auto-radicalisation ». C'est oublier le travail des journalistes, des chercheurs, des activistes… Le temps n'est pas à la finesse ou à la pensée complexe. Et, bizarrement, personne ne parle de couper l'accès au site le plus utilisé par les terroristes pour entrer en contact : Facebook.

Porté par son rapport, le député Larrivé dépose en avril 2014 à l'Assemblée nationale avec les députés Ciotti, Goujon et Marleix une proposition de loi « renforçant la lutte contre l'apologie du terrorisme sur Internet[5] ». Bernard Cazeneuve, alors ministre de l'Intérieur, reprend dans sa proposition de loi une grande partie des préconisations des députés, mettant en place un dispositif de blocage de sites « faisant l'apologie du terrorisme ». De nouveau, choqués par la mise en place d'une infrastructure de censure qui risque d'être réutilisée à d'autres fins,

nous lançons une campagne dénonçant la manière dont les parlementaires abandonnent les libertés fondamentales au nom de l'antiterrorisme, créant un dangereux précédent et des risques inacceptables dans un État dit démocratique.

La « loi Antiterrorisme » est néanmoins votée pratiquement en l'état, et promulguée le 13 novembre 2014. En parallèle, la communauté internationale s'engage contre l'État islamique, à la suite de l'intervention militaire en août des États-Unis en Irak. À l'automne 2014, le Parlement débat d'un nouveau projet de loi, le projet de loi de Larrivé, renforçant les dispositions relatives à la lutte contre le terrorisme. Encore.

UN NOUVEL OUTIL : LES TRIBUNAUX

À la Quadrature, on ne sait plus où donner de la tête. Sur le site de l'organisation, le rythme de publication d'analyses politiques sur les mesures antiterroristes s'accélère. Les lois sécuritaires se succèdent et passent les unes après les autres, dans un sentiment de danger imminent qui vient peser sur les débats et neutraliser l'analyse rationnelle. Le lobbying parlementaire ne fonctionne plus.

Malgré tout, nous tentons une nouvelle fois de réinventer nos moyens d'action, leitmotiv de la Quadrature depuis sa naissance. Le 26 décembre 2014, lendemain de Noël, quelque part sur Internet un salon de discussion IRC s'anime. Le premier décret d'application de la LPM vient d'être publié. Les militants de la Quadrature, mais aussi de French Data Network (FDN) et de la Fédération des fournisseurs d'accès à Internet associatifs (FFDN) prennent connaissance du texte. C'est un groupe hétéroclite de geeks et de juristes, qui travaillent ensemble depuis quelques mois déjà sur les dangers que pose la LPM. Ils ont participé à l'analyse du projet de loi, aux propositions des amendements, à la rédaction des communiqués. Et surtout, ils sont prêts. Ce décret, voilà plusieurs mois qu'ils l'attendent. Ils ont deux mois à compter de sa sortie

pour l'attaquer devant le Conseil d'État et ils comptent bien ne pas manquer l'échéance.

À force de préparation, les geeks se prennent au jeu du juridique et apprennent les ressorts des différentes juridictions, les mécanismes du droit administratif et, surtout, son vocabulaire. Les juristes, eux, apprivoisent IRC et rédigent les procédures en LaTeX, cet obscur système de composition de documents, sur des *pads* auto-hébergés. L'auto-formation bat son plein avec enthousiasme et les points de vue se croisent et se complètent.

En janvier 2015, moins d'un mois plus tard, le groupe de travail publie son premier mémoire et se met à attaquer en justice les décrets du gouvernement, les uns après les autres. À peine créé, le groupe informel est déjà identifié dans les débats à l'Assemblée nationale : le député Jean-Jacques Urvoas (à l'époque pas encore condamné pour violation du secret professionnel) les qualifie avec un dédain perceptible d'« exégètes amateurs », en référence à leur travail d'analyse juridique. Être cités dans un rapport de la commission des lois[6], c'est une consécration ! Alors, après quelques mois à fonctionner sans nom pour se désigner, quand le groupe informel en vient à s'en choisir un, il fait écho à une ancienne tradition quadraturienne de réappropriation des sobriquets qui lui sont attribués. En avril 2015 naissent les Exégètes Amateurs. L'engouement dépasse le petit cercle militant, et des outils sont mis en ligne dans le même esprit de dénonciation du texte et des soutiens de la LPM[7].

Après avoir « hacké le Parlement », en permettant à tous les citoyens de participer au lobbying, voici le « hack juridique de la procédure législative ». Le combat se déplace. Au milieu de cette période éprouvante, émerge un nouveau moyen d'action crédible, pouvant potentiellement prendre le relais du plaidoyer politique et parlementaire. La Quadrature, portée par ce souffle nouveau, est en marche contre l'antiterrorisme, et la victoire semble atteignable.

2. LE TERRORISME PARTOUT

Le 7 janvier 2015, à 11 h 30, une attaque terroriste cible le journal *Charlie Hebdo* à Paris. La France s'arrête, stupéfaite, sous le choc. Quatre jours après, quatre millions de Français et quarante-quatre chefs d'États entament une marche républicaine contre le terrorisme islamiste. Au Parlement, la machine s'emballe.

Deux jours à peine après l'attentat, la Quadrature publie un communiqué alertant sur le risque d'instrumentalisation sécuritaire[1]. Nous mettons en garde le gouvernement contre une récupération de ces attentats pour faire passer de nouvelles lois d'exception. Ce communiqué parle aux gens : cinq mille personnes le lisent en une heure, vingt mille dans les premières 24 heures. Et ce d'autant plus que l'association a malheureusement vu juste : un boulevard vient de s'ouvrir pour les lois sécuritaires.

Pendant que des millions de Français défilent contre le terrorisme et pour la liberté d'expression, le gouvernement français notifie la Commission européenne qu'il compte déroger aux règles sur la censure des réseaux[2]. Il prévoit ainsi de mettre en place le blocage de sites Internet sans contrôle judiciaire et sous 24 heures, prévu par la « loi Antiterrorisme » promulguée quelques mois plus tôt, le 13 novembre 2014. Dans la foulée de l'émotion suscitée par l'attentat de *Charlie Hebdo*, des déclarations plus outrancières les unes que les autres sur la responsabilité de la Toile dans le danger terroriste se multiplient…

Alors que la Quadrature alertait depuis plus d'un an sur l'instrumentalisation de la menace terroriste pour justifier des atteintes majeures aux libertés des citoyens, ce ne sont plus quelques décrets contre lesquels les associations de défense des libertés doivent s'opposer : elles font maintenant face à une ribambelle de projets de lois, d'amendements, de déclarations, de propositions, d'accusations même. Très vite, profitant de la période, le gouvernement use abondamment d'un outil d'exception dans son passage de loi : la procédure accélérée prévue par la Constitution[3].

LA « LOI RENSEIGNEMENT »

En avril 2015, le projet de loi relatif à la prévention d'actes de terrorisme et au renseignement, surnommé « PJL renseignement », est examiné en à peine trois semaines par la Commission des lois. Une gageure pour un texte si complexe. Députés et sénateurs n'ont plus le temps de lire ou de comprendre ce qu'ils doivent voter. La riposte ne peut pas s'organiser dans ces délais qui empêchent la mobilisation citoyenne.

Nous mettons sur pied avec la LDH, le Syndicat des avocats de France et le Syndicat de la magistrature (ces derniers étant pourtant rarement d'accord) une conférence de presse commune sur le sujet. Il s'agit du premier événement organisé dans le tout nouveau « Garage » de la Quadrature, qui vient de déménager dans de plus grands locaux, dans le XX^{e} arrondissement de Paris. Nous y dénonçons le fait que le gouvernement s'apprête à utiliser le Big Data pour « révéler la menace terroriste ». En clair, il s'agit de la captation massive des données informatiques et de l'installation au cœur des équipements du réseau d'un algorithme permettant de les analyser. Cet algorithme, nul ne sait comment il fonctionnera exactement : il est classé *secret-défense*. Les « boîtes noires » du gouvernement sont de retour.

Elles ne sont pas les seules mesures que le gouvernement souhaite déployer pour surveiller la population : *IMSI catchers* (permettant de

repérer les téléphones mobiles et d'intercepter leurs communications), utilisation de logiciels espions, pose de micros et de caméras dans les domiciles et les véhicules, extension de l'accès aux données « en temps réel » prévu par la LPM 2013 dont la Commission nationale de l'informatique et des libertés (CNIL) s'inquiète qu'elle pourrait permettre une « aspiration massive et directe des données par les agents des services concernés »… De nouveau, des pratiques illégales (« a-légales », souvenez-vous), des mesures mises en œuvre en dehors de tout cadre juridique, sont légalisées a posteriori, en tirant avantage de la sidération.

La « loi Rens » (oui, c'est un jeu de mots), poussée par le Premier ministre Manuel Valls qui veut « conférer aux services de renseignement des moyens à la hauteur de la menace terroriste » en profite pour étendre les missions des services de renseignement. Les différentes mesures pourront être mises en place pour des buts aussi variés que « l'indépendance nationale », la « prévention des violences collectives » ou la défense des « intérêts économiques, industriels et scientifiques majeurs de la France ». La « raison d'État » débridée…

La liste complète de ces buts, qui compte dix éléments, laisse une grande latitude aux services de renseignement, permettant d'interpréter par exemple les manifestations contre le nucléaire comme allant à l'encontre de la protection des « intérêts économiques essentiels ». Cela n'est évidemment pas un hasard et on est bien loin de la « simple » prévention du terrorisme, et ce malgré des mesures drastiquement attentatoires aux libertés individuelles, doublée de l'utilisation de la procédure accélérée au titre de « l'urgence ». On pourrait même croire que le terrorisme sert de prétexte pour faire passer une réforme des pouvoirs du renseignement et de leur encadrement, si on avait l'esprit un peu cynique (ou simplement, l'habitude)…

Presque comme une réponse préemptive à ces critiques, pour toutes ces mesures, la loi propose néanmoins un contrôle. Une autorité administrative indépendante : la Commission nationale de contrôle des techniques de renseignement (CNCTR) est créée. Elle est composée pour moitié de parlementaires – plutôt que d'une majorité de magistrats – et

dispose de 24 heures pour rendre ses avis, son silence valant évidemment acceptation des mesures de renseignement. Si jamais ce maigre contrôle venait malgré tout à être trop inconvenant, il pourrait être contourné grâce à une procédure dite d'« urgence absolue », qui permet tout bonnement de s'en passer, sur simple appréciation du seul Premier ministre.

Dans l'ensemble, c'est un incroyable passage en force politique.

Commence une bataille législative. L'UMP trouve le texte insuffisant, mais nécessaire. Le Parti de gauche s'oppose. Les Verts aussi, sans savoir que ces dispositions vont être utilisées contre eux quelques mois plus tard. En revanche, aucun député socialiste ne s'élève contre le texte. Dans les médias, comme auprès des députés de tout bord, contactés un à un, nous démontrons notre capacité à avoir une bonne lecture politique des textes, et à être une sérieuse source d'analyse. Mais de la part du gouvernement, et de Bernard Cazeneuve en particulier, ce n'est que mépris et hostilité. Selon ce dernier, l'association n'aurait rien compris à la qualité et à la nécessité de son texte.

Quelques jours après notre conférence de presse commune, le débat sur la surveillance prend de l'ampleur. Une soirée débat est organisée au Numa, espace parisien dédié aux start-up. Côté invités, rien de bien surprenant : quelques personnalités du PS, bons soldats du gouvernement, et des *usual suspects* des droits humains comme Amnesty, le Syndicat de la magistrature, la Quadrature, et des journalistes comme Marc Rees de *Next INpact*. Par contre, bien plus étonnante est la présence de membres des services de renseignement venus (c'est rare) au contact du public pour expliquer que « les boîtes noires, chers jeunes geeks naïfs, ça n'est pas ce que vous croyez ». Un moment ambigu par excellence, considéré par eux comme une main tendue et perçu par nous, qui sommes habitués à discuter avec des parlementaires et des journalistes, comme un coup de pression surréaliste. Le contexte de la chasse aux sorcières contre les hackers et les lanceurs d'alerte n'aide pas… La Quadrature évolue désormais dans une sphère bien différente de celle de ses débuts, qui avec le recul semble insouciante.

Devant l'inefficacité de leurs interventions dans le débat parlementaire, les associations se replient sur le volet juridique. Sous la pression médiatique et pour couper l'herbe sous le pied des détracteurs de la loi Renseignement, le président de la République François Hollande saisit lui-même le Conseil constitutionnel. Les Exégètes envoient, par le biais de FDN, la Quadrature et la FFDN, un *Amicus Curiae*[4] aux sages du Conseil constitutionnel, un document littéralement d'« ami de la cour », présentant des informations pour aider le Conseil à trancher sur un sujet. Le Conseil constitutionnel valide la quasi-totalité des mesures de surveillance prévues, le 23 juillet 2015, légalisant la surveillance de masse et avalisant un recul historique des droits fondamentaux[5]. Les boîtes noires algorithmiques sont entérinées. Seule la surveillance internationale est jugée non conforme à la Constitution. Malgré la médiatisation du débat, le « PJL renseignement » est adopté et devient la loi n° 2015-912 du 24 juillet 2015 relative au renseignement.

LES EXÉGÈTES AMATEURS PASSENT À LA VITESSE DE CROISIÈRE

Le petit groupe des Exégètes Amateurs se solidifie. Ils ont attaqué un à un les décrets de la loi de programmation militaire (LPM) pour s'opposer aux dispositions d'accès aux données de connexion. Ils viennent d'attaquer le décret de la LPM par un recours en excès de pouvoir devant le Conseil d'État, et de demander le renvoi au Conseil constitutionnel d'une question prioritaire de constitutionnalité (ou QPC). Cette QPC est un mécanisme qui permet à tout justiciable, dans le cadre d'un procès, de saisir le Conseil constitutionnel afin que celui-ci s'assure que la disposition législative applicable à son affaire ne porte pas atteinte aux droits et libertés garantis par la Constitution. Grâce à cette procédure, qui existe en France depuis 2010, les Exégètes Amateurs espèrent faire annuler d'un coup tous les décrets.

Après le dépôt de cette QPC en avril, les Exégètes continuent de s'attaquer au sujet des données de connexion. En effet, l'accès à ces

données ne peut avoir lieu que si elles existent et ont été conservées. C'est la loi pour la confiance dans l'économie numérique (LCEN) de 2004 qui encadre la rétention des données de connexion, et le décret d'application de 2011 de la même loi qui fixe le délai de cette rétention à un an. Autrement dit : tous les fournisseurs d'accès et d'hébergement doivent conserver les données permettant l'identification de leurs utilisateurs pendant un an.

Ces dispositions vont à l'encontre de la jurisprudence de la Cour de justice de l'Union européenne (CJUE) d'avril 2014, dite « Digital Rights Ireland ». L'arrêt Digital Rights invalide le principe de conservation généralisée des données de connexion, que la Cour considère comme contraire à la Charte des droits fondamentaux de l'Union européenne[6]. Oui mais voilà : on ne peut faire de recours que contre les décisions administratives récentes. Or, nous sommes en 2015 et les décrets d'application de la LCEN, qui doivent être attaqués comme toute décision administrative dans les deux mois suivant leur parution, sont déjà bien anciens. Comment faire appliquer une jurisprudence nouvelle à des lois anciennes ?

Les Exégètes trouvent alors une faille. S'appuyant sur l'arrêt Digital Rights, ils demandent au gouvernement l'abrogation du décret, rendu illégal par la décision de la CJUE. L'administration a ensuite deux mois pour répondre, l'absence de réponse valant refus. C'était attendu, l'administration ne daigne pas répondre à la demande des Exégètes Amateurs. Mais voilà : un refus est bien une décision administrative… que les Exégètes ont donc deux mois pour attaquer devant le Conseil d'État[7] !

Ils déposent leur demande d'abrogation le 6 mai 2015 et attendent patiemment le 6 juillet pour constater l'absence de réponse du gouvernement. Pendant ce temps, le Conseil constitutionnel transmet au mois de juin la QPC portant sur la LPM[8]. La loi Renseignement qui est alors en discussion au Parlement vient étendre les dispositions contestées sur l'accès aux données de connexion. Et le lendemain du vote de la « loi

Rens », le 24 juillet, le Conseil constitutionnel rejette la QPC des associations. Le groupe de juristes bénévoles ne se laisse pas abattre.

La procédure contre le décret de la LPM continue devant le Conseil d'État (qui rejettera le recours en février 2016), et les Exégètes commencent à attaquer les décrets de la loi Renseignement[9] qui paraissent à l'automne, tout en attaquant le refus d'abrogation du décret de la LCEN. Ils publient de nouveaux recours chaque mois, chacun plus dense que le précédent. En un an, ils vont attaquer une douzaine de décrets, poser quelques QPC, permettant la censure de lois parlementaires par le Conseil constitutionnel, et entamer des dossiers qui feront plus tard jurisprudence. Bien plus tard. La justice est lente, d'autant plus lente lorsqu'elle doit remonter d'institution en institution jusqu'à la Cour européenne. C'est un long combat qui commence pour les juristes, qui les mènera jusque devant la Cour européenne des droits de l'homme et, à nouveau, de nombreuses fois, devant le Conseil d'État et le Conseil constitutionnel.

Mais alors que les Exégètes entament leurs démarches les unes après les autres, pleins d'espoir dans leurs futures retombées, un autre événement vient encore accentuer la pression de l'agenda parlementaire antiterroriste.

LES ATTENTATS DU 13 NOVEMBRE 2015

Le soir du 13 novembre 2015, une série de fusillades et d'attaques-suicides sont perpétrées au Stade de France à Saint-Denis et dans de multiples lieux à Paris : la salle de spectacle du Bataclan et plusieurs terrasses des X^{e} et XI^{e} arrondissements. Les attentats font 130 morts et 413 blessés hospitalisés, dont 99 en situation d'urgence absolue. Dans la panique, devant la multiplicité des points d'attaque et l'incertitude des informations qui arrivent de toutes parts, les Parisiens se précipitent dans les commerces et immeubles les plus proches. En quelques dizaines de minutes, les rues de Paris se sont vidées et les rideaux de fer ont été tirés

devant les boutiques. À 23 h 53, le président de la République François Hollande décrète l'état d'urgence sur tout le territoire.

L'horreur de cette soirée, la panique qu'elle a engendrée, nous l'avons vécue de près, comme de nombreux Parisiens. Ce sentiment que quelque chose de différent vient de se produire, que quelque chose vient de rompre. L'inquiétude pour les proches, les connaissances… Sans surprise, comme beaucoup de gens, nous apprendrons au cours des jours suivants qu'un proche, une amie d'amie, un cousin, un collègue… a vécu les attaques directement. Certains y ayant perdu la vie.

Le lundi matin, à peine remis, nous publions un communiqué : « S'associer à la douleur, penser l'avenir ». Et pour penser l'avenir, nous, militants des libertés, repensons au passé. En 2001, les attentats du 11 septembre ont ouvert la voie au Patriot Act, une loi antiterroriste américaine attaquant les libertés individuelles comme le droit à un procès équitable, le droit à la vie privée ou le droit à la liberté d'expression. Ce long texte réunissait pêle-mêle des mesures pour la plupart déjà rédigées en amont qui n'attendaient que le bon moment pour être votées. C'est ce que la journaliste Naomi Klein a nommé la « stratégie du choc » : l'utilisation par les personnes au pouvoir d'un « choc psychologique » pour renverser la situation à leur avantage. Quatorze ans plus tard, nous le savons, la suite de lois sécuritaires qu'elle a combattue depuis sept ans en est l'amorce : c'est le même destin qui attend la France. « Face à la déclaration de l'état d'urgence et aux annonces faites au cours du week-end, La Quadrature du Net demande aux responsables politiques de prendre le temps de la réflexion. »

Mais au lendemain de cet « acte de guerre commis par une armée terroriste », comme le qualifie François Hollande, personne n'ose rompre les rangs de la solidarité nationale. Depuis un an et demi, soit depuis le début de l'été 2014, la Quadrature ne fait pratiquement que de l'anti-antiterrorisme. Depuis un an, l'hystérie collective a monté en épingle des faits divers d'enfants qui « ne sont pas Charlie », a jeté une suspicion de sédition sur tous les musulmans, a cloué au pilori tous ceux qui ne

faisaient pas le jeu de l'unité nationale. Le 16 novembre, la Quadrature se sent seule.

La campagne sur la « directive Copyright », qui démarre au même moment, est complètement éclipsée par l'actualité médiatique. L'antiterrorisme est partout. Nous sommes épuisés et, devant nous, les menaces contre les libertés sont plus grandes que jamais.

3. EXTENSION DES OUTILS ANTITERRORISTES

S'il y a une idée qui revient souvent dans les analyses de la Quadrature, c'est celle du danger de mettre en place une infrastructure, qu'elle soit technique ou légale, en jurant qu'elle ne servira que dans un but précis, et noble, bien évidemment. Certains esprits chagrins diraient que c'est une marotte, mais l'histoire nous a donné un nombre déprimant d'exemples de détournement de ce type. Ainsi, la collecte de données dans un but parfois justifié à l'origine peut dériver trois, cinq, dix, vingt ans plus tard. De manière complètement légale.

Le Fichier national automatisé des empreintes génétiques (FNAEG) en est un exemple incroyable (et révoltant). Ce fichier, créé en 1998 et censé servir à la lutte contre les délinquants sexuels, comptait moins de 5 000 personnes en 2002. En 2020, il en compte plus de 4,8 millions, soit environ 8 % de la population française ! Cette augmentation presque exponentielle s'explique par l'extension continue du périmètre du fichage génétique en France, dû à de multiples lois successives. C'est ce qui conduit à des situations ubuesques, comme celle de 2006, quand des lycéens mis en garde à vue après avoir participé aux manifestations contre le contrat première embauche (CPE) ont été obligés de se soumettre à des prélèvements ADN[1]… De même que des enfants à la suite d'un vol de tamagotchis[2] ! On est loin du but originel du fichier.

En 2021, le FNAEG contient plus d'un tiers des Français[3] si l'on compte les personnes directement identifiées et les parentèles (parents, frères et sœurs) indirectement identifiables (les parentèles multiplient le

nombre de personnes identifiables par cinq). Bien que plus de 80 % des personnes y soient enregistrées en tant que simples « mis en cause » (donc présumés innocents), leurs empreintes sont conservées pendant quarante ans. Un véritable « fichier des honnêtes gens ».

Ce phénomène est connu et étudié. En anglais, il a un nom descriptif : on parle de « *mission creep* » (ou « *scope creep* »), cette idée que la mission (ou le périmètre) d'origine s'étire jusqu'à couvrir des zones bien plus larges que celles initialement prévues. Au niveau européen, l'expression est régulièrement employée pour décrire des lois qui commencent par un cadre donné et l'étendent, l'étendent, jusqu'à englober des choses qui n'ont aucun rapport avec le premier cadre, que ce soit par tactique, par bêtise ou par hubris.

Cette « dérive des missions », en bon français, se combine souvent avec un autre phénomène que l'on redoute à la Quadrature : *l'effet cliquet*. L'effet cliquet, c'est cette (quasi-)impossibilité de retour en arrière, une fois un certain stade passé. En 2015, un nouvel exemple de ces phénomènes va nous être donné en France.

L'ÉTAT D'URGENCE, C'EST MAINTENANT

Le 13 novembre 2015, au soir des attaques-suicides et de la prise d'otage du Bataclan, et alors que celle-ci est encore en cours, François Hollande décrète l'état d'urgence, pour une durée déterminée de douze jours[4]. Trois jours plus tard, le président de la République annonce devant le Congrès une ribambelle de mesures qu'il souhaite dérouler dans les prochains mois : prolongation de l'état d'urgence, intensification des opérations françaises en Syrie, révision de la Constitution pour « agir contre le terrorisme de guerre », création de postes supplémentaires dans les forces de sécurité…

La Conférence de Paris sur le climat doit avoir lieu quelques semaines plus tard, du 30 novembre au 12 décembre 2015 au Bourget, et à cette occasion de nombreux militants écologistes ont prévu des actions à Paris,

en France et en Europe pour porter leurs revendications. Dès le 18 novembre, au prétexte de la nécessité de renforcer la sécurité sur la voie publique, le gouvernement annonce l'interdiction de la Marche mondiale pour le climat prévue pour le 29 novembre.

Quelques jours après, l'état d'urgence est consacré et étendu pour trois mois par la loi du 20 novembre[5], qui autorise notamment l'assignation à résidence des personnes dont le « comportement constitue une menace pour la sécurité et l'ordre publics ». Il sera renouvelé six fois !

Très vite, cette loi d'exception censée protéger la France des attentats terroristes est mise en application pour freiner les militants écologistes. Dans la semaine qui suit, des activistes, impliqués dans les mouvements de contestation autour du projet d'aéroport de Notre-Dame-des-Landes, font l'objet de violentes perquisitions en Dordogne, à Ivry-sur-Seine, à Rennes, à Rouen, à Lyon, parfois sous des prétextes flous, voire franchement fallacieux. Le 28 novembre, le ministre de l'Intérieur Bernard Cazeneuve annonce l'assignation à résidence de vingt-quatre militants, jusqu'au 12 décembre, date de fin de la COP21[6].

Malgré les interdictions, les perquisitions, les assignations, plusieurs milliers de manifestants se réunissent le 29 novembre sur la place de la République à Paris, où devait initialement avoir lieu la Marche mondiale pour le climat[7]. Certains sont venus de loin. Un groupe de zadistes de Notre-Dame-des-Landes est présent, tout comme des militants du NPA ou des membres de la Brigade activiste des clowns. On compte aussi de nombreuses personnes simplement concernées par le sujet – enfants, adolescents, personnes âgées… Le rassemblement démarre dans une bonne ambiance. Mais toutes les artères autour de la place de la République sont bloquées par la police, à une exception près. La manifestation ne peut que faire le tour de la place. La tension monte très vite. Les policiers qui encadrent la place font, aléatoirement, quelques pas en avant, créant confusion et inquiétude chez les manifestants qui, pour la plupart, discutent climat et état d'urgence en petits groupes. Rapidement, la place se recouvre d'un épais nuage de gaz lacrymogène. Les gens,

parfois des personnes âgées ou des parents avec leurs enfants, que la police a laissés entrer sans sourciller sur la place, courent d'un côté à l'autre entraînant des mouvements de foule. La police charge une fois, deux fois, trois fois. Les manifestants et les policiers piétinent les bougies et les fleurs qui avaient été rassemblées en un mémorial aux victimes des attentats. À l'issue de cette journée mouvementée, la préfecture de police aura procédé à 341 interpellations et 316 mises en garde à vue, dont seules deux aboutiront à une condamnation, dont une pour refus de donner ses empreintes digitales.

La première manifestation sous le régime de l'état d'urgence donne le ton de la montée de la répression policière permise par l'arsenal antiterroriste. Désormais, les manifestations seront des confrontations. Et concernant le niveau de violence, c'est encore ce qu'un haut responsable des forces de l'ordre confiait au *Monde diplomatique* il y a quelques années qui l'explique le mieux : « C'est nous, l'institution, qui fixons le niveau de violence de départ. Plus la nôtre est haute, plus celle des manifestants l'est aussi[8]. »

Celle-ci existe dans un cadre, et le cadre ne cesse de s'étendre. François Hollande le confirmera d'ailleurs dans une série d'entretiens publiés l'année suivante dans le livre *Un président ne devrait pas dire ça* : « C'est vrai, l'état d'urgence a servi à sécuriser la COP21, ce qu'on n'aurait pas pu faire autrement […]. Imaginons qu'il n'y ait pas eu les attentats, on n'aurait pas pu interpeller les zadistes pour les empêcher de venir manifester. »

Pour réagir à la mise en place et à l'utilisation abusive de l'état d'urgence, de manière presque réflexe, nous ouvrons un *pad*, un document collaboratif en ligne accessible à toutes et à tous, puis une page sur le wiki de l'association, pour recenser les atteintes aux libertés liées à des dérapages. Ne serait-ce que dans les quinze premiers jours de l'état d'urgence, entre le 14 et le 30 novembre 2015, près de 150 abus sont documentés et sourcés sur la page. Au total, l'état d'urgence donne lieu à plus de 7 000 mesures administratives : perquisitions, assignations à

résidence, interdictions de séjour ou de manifestation. Une majorité d'entre elles ne feront l'objet d'aucune suite judiciaire[9].

Comme la Quadrature et ses alliés l'avaient prévu, l'État utilise les largesses permises par la mesure d'exception pour s'attaquer à d'autres cibles, en particulier aux opposants politiques[10]. Sur le wiki, les contributeurs inexpérimentés ajoutent tant bien que mal leurs pierres à l'édifice, tandis que des wikipédiens chevronnés viennent régulièrement « jardiner » la page pour organiser, ranger et mettre en forme les contributions. L'outil tourne finalement sans la Quadrature, dans un enthousiasme collaboratif et décentralisé.

LA MACHINE À FANTASMES TECHNOLOGIQUE

La Quadrature n'est pas la seule à vouloir mettre en place des outils, mais tous n'auront pas la même vocation. Après les attentats du 13 novembre 2015, les politiques tentent une fois de plus de jouer la carte de la solidarité nationale, du « tous ensemble », comme l'avait déjà été la marche du 11 janvier faisant suite aux attentats de *Charlie Hebdo*. Anne Hidalgo, maire de Paris, lance une grande campagne d'affichage « *Fluctuat nec mergitur* ». Sur les systèmes d'affichage de publicité JC Decaux, sur la tour Eiffel, en *street art*, sur le mémorial de la place de la République, la devise est partout. Cette campagne est accompagnée d'initiatives comme cette « carte citoyenne » qui permettrait aux Parisiens de participer à la vie de leur cité. La devise se décline encore avec l'organisation d'un hackathon « *Nec mergitur* » en janvier 2016, en partenariat avec la mairie, la préfecture de police de Paris, le ministère de l'Intérieur et d'autres services de l'État. L'événement a pour objectif d'« accompagner la police et les services de l'État dans leur mission de prévention, d'alerte et de gestion des crises, en leur proposant des outils innovants et nouveaux ». Les promoteurs de l'événement avaient, à l'époque, déjà proposé des idées d'applications à l'idéologie pour le moins orientée. Par exemple, une application permettant de détecter si

votre voisin est radicalisé. Le temps est à la suspicion et à la délation automatisée. Charmant.

Voyant cela, nous contactons les organisateurs en amont de l'événement, pour leur rappeler que le développement d'outils numériques peut être positif, et non effectué uniquement dans l'objectif de désigner des boucs émissaires. On nous suggère de participer au débat, et même de faire partie du comité de déontologie de l'événement, qui n'a pas de pouvoir de contrainte. Ce qu'après discussions nous refusons. Une sage décision…

Des journaux titrent sur une mobilisation du monde de l'innovation « contre le terrorisme », ou « pour la sécurité ». Le résultat est à l'avenant : le premier groupe de travail du hackathon a pour thème « Prévenir la radicalisation, concevoir et diffuser les contre-discours » et le prix spécial du jury est décerné à un « outil d'identification de niveau du risque de radicalisation d'un individu à travers ses différents profils sur les réseaux sociaux et l'analyse du contenu de ses messages ». Du monde de la tech au gouvernement, on est en pleine période de fantasme de détection des « terroristes » par des algorithmes et « signaux faibles » ! Une autre application propose la « détection automatisée de rumeurs sur les réseaux sociaux et diffusion de contre-discours ». Heureusement, des outils plus positifs voient le jour, comme des systèmes d'amélioration de l'organisation des secours, ou la mise en contact par appli entre une victime et des secouristes dans une zone déterminée[11].

Participer à des événements de ce type est-il la mission de la Quadrature ? Sert-elle alors de faire-valoir ou permet-elle d'infléchir une politique ? Cette question est récurrente dans les décisions que doit prendre l'organisation. La tactique des décideurs est toujours la même : donner à leurs opposants un comité soigneusement étudié sans aucun pouvoir réel. Aujourd'hui, nous en sommes convaincus. En 2015, dans ces circonstances si particulières, alors que notre positionnement se fondait sur le respect des libertés fondamentales – même en temps d'attaques terroristes –, nous avions un temps espéré pouvoir infléchir la ligne sécuritaire, mais toute confiance a depuis été rompue.

Pendant ce temps, le gouvernement continue ses propositions de lois[12]. La Quadrature alerte sur la banalisation des mesures d'exception, qui viennent entériner dans le droit commun les restrictions de l'état d'urgence[13]. Mais rien n'arrête la course folle à l'antiterrorisme ! La loi relative à la lutte contre les incivilités et les actes terroristes (c'est large, n'est-ce pas ?), passée en procédure accélérée, est promulguée le 22 mars 2016. Elle autorise notamment les agents des réseaux de transports publics (RATP et SNCF) à procéder à des palpations de sécurité et à des fouilles de bagages. Cette loi débattue au Parlement à partir de décembre a été déposée par le gouvernement en octobre 2015[14]. Un mois avant les attentats de novembre ! Le 3 juin 2016 est promulguée la loi relative à la lutte contre le crime organisé et le terrorisme, déposée en février, toujours en procédure accélérée[15]. Elle autorise les perquisitions de domiciles de nuit, l'utilisation élargie des *IMSI catcher* et le renforcement des contrôles d'accès aux lieux accueillant de grands événements. Petit à petit, l'une après l'autre, les lois adaptent dans le droit commun des mesures jusque-là réservées à l'état d'urgence. Cet état exceptionnel, et surtout temporaire, qui vient d'être renouvelé pour la troisième fois, afin de sécuriser les manifestations sportives de l'été (l'Euro de football et le Tour de France).

Le gouvernement continue également ses initiatives de « solutionnisme technologique[16] ». À la veille de l'Euro, une nouvelle application est créée : « Alerte attentat ». Elle vient renforcer le dispositif SAIP (pour « système d'alerte et d'information des populations »), qui rassemble différentes méthodes d'alerte, comme le Signal national d'alerte[17] (la sirène à midi le premier mercredi du mois) ou la diffusion cellulaire (l'envoi d'un message à l'ensemble des téléphones portables présents sur une zone, utilisé depuis longtemps aux États-Unis pour les alertes météorologiques, et qui servira en France pour annoncer le confinement de mars 2020). Cette nouvelle méthode d'alerte nécessite de posséder un smartphone, d'installer l'application « Alerte attentat » et, surtout, d'être connecté à un réseau mobile non saturé. Le 14 juillet 2016, à Nice, alors qu'un attentat terroriste fait plus de 80 victimes aux

alentours de 23 heures, l'application ne donnera l'alerte qu'à 1 h 34. Lors des attentats du 20 avril 2017 sur l'avenue des Champs-Élysées, et du 23 mars 2018 à Carcassonne et Trèbes, l'application n'enverra tout simplement aucun message. Elle sera abandonnée en 2018, après avoir coûté 300 000 euros pour 900 000 téléchargements (sur une population de 67 millions de personnes), puis remplacée par un accord avec Google, Twitter et Facebook pour que ces plateformes relaient les messages du gouvernement.

L'attentat du 14 juillet à Nice est une bonne occasion pour un nouveau projet de loi, que l'on appellera loi relative à l'état d'urgence et portant des mesures de renforcement de la lutte antiterroriste. Déposée par le Premier ministre le 19 juillet 2016 en procédure accélérée, elle est adoptée le 21 juillet 2016[18]. Trois jours : c'est le temps donné aux débats des deux chambres parlementaires et aux réunions de la commission mixte paritaire. Trois jours pour prolonger l'état d'urgence et suspendre le droit commun pour six mois de plus. Trois jours pour voter le durcissement des peines liées au terrorisme et exclure les personnes condamnées du régime de réduction de peine. Trois jours pour autoriser la fermeture des lieux de culte sur simple décision administrative. Trois jours pour permettre l'interdiction par l'autorité administrative des cortèges, défilés et rassemblements de personnes sur la voie publique. Trois jours.

Cette interdiction des manifestations sur la voie publique tombe à pic. Depuis février, la loi relative au travail, à la modernisation du dialogue social et à la sécurisation des parcours professionnels, dite « loi Travail » ou « loi El Khomri », fait l'objet d'un important mouvement de contestation. Alors que l'on constate une augmentation générale des violences policières (pour la première fois en 2016, plus de mille plaintes sont déposées devant le Défenseur des droits) dans ces manifestations, voilà que sont donnés encore plus de moyens de répression à la police.

Alors que ces violences sont au cœur d'une médiatisation intense, le 19 juillet 2016, Adama Traoré meurt à la gendarmerie de Persan (Val-d'Oise), à la suite de son interpellation à Beaumont-sur-Oise. Les

expertises se multiplient pour déterminer les causes du décès et la responsabilité des gendarmes, mais aboutissent à des conclusions diverses, faisant planer la suspicion sur l'objectivité du système juridique lorsqu'il s'agit de la mise en cause de la gendarmerie. Malgré les répressions, le Comité vérité et justice pour Adama organisera des manifestations locales. Encore une fois, l'argument antiterroriste a bon dos lorsqu'il s'agit de réprimer un mouvement social qui n'a pourtant rien à voir avec les attentats.

Du côté de la Quadrature, nous n'avons plus beaucoup d'espoir d'influer sur le débat parlementaire. Les militants se concentrent donc sur des actions a posteriori et se remettent à travailler sur les anciennes lois, à commencer par la loi Renseignement, dans leur viseur depuis 2015.

En avril 2016, *Le Monde* révèle la surveillance par la Direction générale de la sécurité extérieure (DGSE) de Thierry Solère[19]. Le téléphone et les e-mails du candidat aux législatives de 2012, face à l'ancien ministre de l'Intérieur Claude Guéant, ont été espionnés. En creusant, les Exégètes comprennent que les autorités se sont appuyées sur l'article 20 de la loi de 1991, dépoussiéré et renuméroté par la loi Rens, qui prévoit que « les mesures prises par les pouvoirs publics pour assurer […] la surveillance et le contrôle des transmissions empruntant la voie hertzienne ne sont pas soumises aux dispositions du présent livre ». La « voie hertzienne », c'est-à-dire toutes les transmissions sans fil. Alors que nous sommes entourés de wifi, de 3G/4G, de Bluetooth, de GSM, de RFID et NFC[20], la loi Rens a, en laissant cet article inchangé, exclut toutes les communications sans fil du champ des (toujours insuffisantes) procédures de contrôle instituées pour les techniques de renseignement.

Ni une ni deux, en mai 2016, les associations déposent une nouvelle demande de QPC, transmise par le Conseil d'État au Conseil constitutionnel en juillet, et qui aboutira en octobre à la censure de ces dispositions[21]. Mais l'accès aux données de connexion est dans tous les textes de lois du gouvernement. Et la loi de juillet 2016 sur la prorogation de l'état d'urgence (celle débattue en trois jours) vient d'élargir encore ces accès en autorisant la collecte en temps réel des données de «

l'entourage » des personnes surveillées[22] ! Cet élargissement se fonde sur le dernier décret de la loi Rens paru en janvier, que les Exégètes n'avaient pas encore pu attaquer. Le délai pour le faire étant passé, ils reproduisent la technique qu'ils avaient établie en 2015 : ils demandent l'abrogation du décret au gouvernement en août 2016, attendent pendant deux mois l'absence de réponse valant refus, pour ensuite attaquer, en décembre 2016, le refus d'abrogation devant le Conseil d'État. Ils demanderont le transfert d'une QPC en 2017 au Conseil constitutionnel qui censurera le décret au mois d'août 2017.

La machine parlementaire ne s'arrête pas. En décembre 2016, plus d'un an après les attentats du Bataclan, l'état d'urgence est prolongé pour la cinquième fois.

4. PROTÉGER NOS DONNÉES : LE RGPD EN RENFORT

Début 2016, la Quadrature cherche comment reprendre la main sur le calendrier. Mais il faut se rendre à l'évidence : le débat parlementaire est de plus en plus verrouillé. Les appels aux députés ont toujours moins d'impact, les échanges avec eux sont plus policés et relèvent davantage de la stratégie de communication que de l'intérêt véritable envers des positions différentes.

Dans le contexte de l'opposition populaire à la loi Travail, le gouvernement se tend, les négociations sont de plus en plus compliquées. Le 31 mars, une nouvelle manifestation se termine place de la République, où est projeté le film de François Ruffin, *Merci Patron*. Les manifestants refusent ensuite de partir. Ils refusent même de quitter le mois de mars pour passer en avril. 32 mars, 33 mars : c'est le début de Nuit debout, expérience revendicative et convergente des luttes sociales. Nous participons à ce mouvement optimiste en organisant une partie de l'infrastructure numérique, en proposant des conférences ou en ouvrant, sur la place « biblio debout », une bibliothèque ouverte et participative. Le lieu se transforme en forum permanent, où les assemblées générales sont ouvertes à toutes et à tous et où des débats ont lieu à tout moment du jour et de la nuit. Nuit debout perdure jusqu'au début de l'été.

À force de se positionner sur tous les sujets, la Quadrature devient incontournable dès que le numérique est en jeu, une position utile mais qui a un coût : il faut toujours plus d'expertise dans des domaines différents et toujours plus d'énergie pour suivre, dans toutes les

directions. Au premier semestre 2016, lors d'un apéro proposé aux bénévoles, puis dans un communiqué de presse[1], est présentée la nouvelle position de l'association : « Face à une représentation politique dont la seule logique est sécuritaire, La Quadrature du Net refuse de perdre davantage de temps à tenter d'influencer rationnellement ceux qui ne veulent rien entendre et choisit de réorienter ses actions. » L'urgence permanente, les propositions irresponsables, relayées par des parlementaires dociles au gouvernement, nous conduisent à vouloir réorganiser notre action pour moins de suivi législatif français, davantage d'actions avec des partenaires européens et plus de réflexions, ouvertes à des interventions externes et des compétences que nous n'avons pas dans nos équipes. Moins de temps avec le monde politique et davantage avec les gens, via plus de sensibilisation de fond, plus de participation, de décentralisation de nos actions. D'un côté fatigués mais de l'autre portés par ce moment d'engouement populaire, nous voulons faire de l'éducation populaire (à l'aide d'ateliers, de conférences), pour armer intellectuellement la population sur ces sujets. Bref, nous souhaitons tous plus d'indépendance face aux agendas imposés : sortir de l'état d'urgence.

Si cette nouvelle posture nous permet de respirer et de reprendre la main sur un certain nombre de dossiers, elle va se révéler difficile à tenir. Les ateliers s'essoufflent courant 2017 et disparaissent par manque d'investissement de l'équipe, malgré une participation souvent importante. Très vite le naturel revient au galop : nous n'arrivons pas à lâcher le débat législatif. Et pour cause, un texte qui va se révéler majeur est en train de se mettre en place. Mais notre approche envers celui-ci sera cette fois-ci un peu différente.

UNE RÉVOLUTION SANS TROP RÉVOLUTIONNER

En mai 2016 est voté l'un des textes européens les plus marquants et les plus positifs de ces dernières années : le RGPD, pour « règlement général

sur la protection des données ». Lors de la négociation du texte au Parlement européen, les parlementaires en charge de le porter ont pourtant subi une campagne de lobbying de la part des GAFAM d'une intensité encore jamais vue à l'époque.

Alors que le développement d'un Internet à vocation de plus en plus commerciale a pour corollaire la perte progressive de contrôle sur la destination de nos données personnelles, la réglementation existante n'est que très peu respectée – même en France, où la Commission nationale de l'informatique et des libertés (CNIL) existe pourtant depuis 1978. La faute à une institution qui n'a que peu de pouvoir sur les entreprises, et de moins en moins sur l'État.

Le RGPD prend la relève d'une directive pré-Internet grand public, votée en 1995, et vise alors à donner un coup de fouet aux autorités de contrôle (nom générique des « CNIL » européennes dans le règlement) en leur donnant des pouvoirs de sanction supplémentaires, allant jusqu'à 20 millions d'euros ou 4 % du chiffre d'affaires mondial de l'entreprise visée, ce qui peut revenir à plusieurs milliards d'euros pour les géants du numérique. C'est pratiquement la seule grande nouveauté du texte.

La campagne de lobbying réussit dans un premier temps à rendre encore plus mou le texte initialement proposé par la Commission européenne. Mais l'onde de choc politico-médiatique des révélations Snowden modifie le contexte des négociations et ramène finalement le texte plus près de sa version initiale : peu de grandes nouveautés, mais quelques avancées considérables. Y figure le « consentement explicite », pour lequel nous nous battons depuis de nombreuses années et la possibilité de saisir les autorités de contrôle par des plaintes collectives. Mais en dehors de cela, tous les grands principes de la protection des données (définition des données « sensibles », conditions de licéité de leur collecte et de leur utilisation, loyauté envers le consentement, etc.) ainsi que la majorité de nos « droits » (accès à nos données, possibilités de rectification, etc.) ont été repris presque à l'identique de la directive européenne initiale de 1995. Le règlement crée bien aussi un nouveau droit à la portabilité, mais son intérêt pratique reste encore à trouver.

Malheureusement, le RGPD ne se contente pas d'hériter des forces de la directive de 1995, il hérite aussi de sa faille principale : il autorise toute entreprise à collecter et à utiliser des données personnelles si elle y trouve un « intérêt légitime » (économique, structurel…) et que la poursuite de cet intérêt ne porte pas une « atteinte disproportionnée » aux intérêts des personnes concernées. Oui, ce « critère » est particulièrement flou et tordu, et c'est hélas bien son but : « Pour l'instant, vous avez le droit de faire ce que vous voulez, et on viendra vérifier plus tard, si on a le temps, que vous n'avez pas trop dépassé les bornes. »

Mais alors, si le RGPD apporte si peu de nouveautés, pourquoi y trouver l'espoir de changements majeurs ? Son principal effet, en vérité, n'est pas tant d'avoir modifié le droit que d'en permettre enfin l'application. Et c'est sur cette partie que cette fois nous allons concentrer nos efforts.

En théorie, depuis longtemps, le droit des données personnelles pourrait être une arme puissante pour nous protéger : l'analyse comportementale n'est possible qu'avec notre consentement (qui doit désormais être explicite) et, surtout, ce consentement doit être libre. C'est ce format de consentement qui est important : le droit des données personnelles prévoit, depuis plusieurs années, que notre consentement n'est pas « valide » s'il est une condition pour accéder à un service. Qu'il n'est pas « libre » s'il est donné sous la menace de subir une conséquence négative. Qu'il n'est pas « valable » s'il est assimilé à la contrepartie d'un contrat ou à un prix.

Ce principe est simple : céder ses données, c'est renoncer à son droit fondamental à la protection de la vie privée, à la liberté de conscience, à l'intégrité. Or, heureusement, nos principes démocratiques s'opposent à la marchandisation de nos libertés fondamentales (sans quoi la moindre « égalité des droits » ne bénéficierait qu'à ceux pouvant se l'acheter).

Pour résumer, depuis plusieurs années, les modèles économiques de Facebook ou Google n'ont, juridiquement, aucune raison d'exister : ils se financent grâce à une analyse comportementale de masse à des fins publicitaires. Or cette analyse n'est possible qu'avec notre consentement.

Nous devrions pouvoir accéder à leur service tout en refusant de donner ce consentement, sinon ce consentement n'est pas libre : mais si nous avions véritablement cette possibilité, la très grande majorité d'entre nous refuserait cette surveillance.

Leur modèle est illégal et juridiquement absurde depuis longtemps. Le seul problème, en vérité, c'est que personne n'avait le pouvoir, ou la volonté, de les arrêter. Nous en avons la volonté, et désormais des moyens, avec le RGPD. C'est cela, et surtout cela, qui change avec le RGPD.

Au lieu du consentement explicite, les GAFAM veulent absolument un vague « consentement indubitablement donné ». Pour contrer l'influence de ce lobbying néfaste, nous rencontrons des eurodéputés pour les mettre en garde de ne pas voter « en faveur de l'intérêt des États-Unis », travaillant de concert avec les autres organisations européennes, s'inspirant de l'époque de l'ACTA.

Le RGPD est adopté le 14 avril 2016. Sa mise en application est prévue pour le 25 mai 2018. Ce sont deux longues années que le législateur laisse aux entreprises et aux États pour se préparer. Dans l'entre-deux, comme pour couronner un texte déjà inattendu, certaines décisions de la CNIL semblent montrer qu'une nouvelle ère s'ouvre enfin. Les possibilités de sanction ne sont pas encore aussi importantes qu'une fois que le RGPD sera entré en vigueur, mais fin 2017 l'autorité française met en demeure[2] WhatsApp de corriger son système de transfert de données personnelles à Facebook. La CNIL considère ce transfert illicite car se fondant sur le consentement forcé des utilisateurs, ceux-ci ne pouvant s'y opposer qu'en renonçant au service. Le message est fort, et se fonde sur les lignes directrices du G29, groupement des CNIL européennes[3], en prévision de la sortie prochaine du règlement. Nous nous réjouissons de l'analyse faite par la CNIL, car c'est exactement celle que la Quadrature défend depuis des années.

Néanmoins, dans un profond déni de réalité, États et entreprises attendront le dernier moment pour prendre le texte en compte. L'adaptation en droit français n'est votée qu'en juin 2018, après six mois

de négociation. Juste après, fin juillet, la CNIL déclare illicites[4] les activités de deux start-up françaises, Teemo et Fidzup, qui géolocalisent des millions de personnes à des fins publicitaires et sans leur consentement. Elles ont trois mois pour cesser ces activités. De nouveau un bon signal pour la mise en place effective des principes fondateurs du RGPD, et de l'interprétation qui en est faite par la Quadrature, et sur le moment nous en venons à voir ces deux années comme une période d'accélération prometteuse pour la CNIL.

Toutefois, en arrière-plan se profile déjà un autre texte qui pourrait venir désarmer le RGPD : le règlement ePrivacy.

LE RGPD MIS À MAL : LA DIRECTIVE EPRIVACY

Alors que l'Union européenne négocie encore le RGPD, en avril 2016, le Parlement européen lance une consultation pour mettre à jour une directive de 2002 largement moins médiatisée : ePrivacy.

Les deux textes sont très liés : le RGPD réglemente l'usage des données personnelles de manière générale, quand ePrivacy précise cet usage pour les services de communication. Cela inclut, par exemple, le spam ou la gestion des cookies, ces petits fichiers déposés sur votre machine qui permettent de conserver des informations sur vous d'une visite à l'autre. Le traitement de ces derniers est précisé par la directive bien avant l'entrée en application du RGPD : leur dépôt est soumis à un « consentement valide » de l'utilisateur, tel que défini par le droit supérieur. Lorsque le RGPD entre en vigueur, il devient ce « droit supérieur », et la définition du « consentement valide » change : celui-ci ne peut plus être « déduit » du simple fait que nous sommes informés par un vulgaire « bandeau cookie ». Notre silence ne vaut plus accord, enfin ! Tant que nous ne cliquons pas explicitement sur un bouton « j'accepte », il est strictement interdit de nous pister et de réaliser des profits sur nos données personnelles[5]. Mais encore faut-il que l'autorité de protection des données (APD) de chaque État membre prenne la mesure du

changement – ce qu'elle mettra beaucoup de mauvaise volonté à faire en France…

Malgré l'aspect très technique de cette consultation, la Quadrature appelle le public à s'investir dans le débat et publie son analyse[6]. Elle y explique que le RGPD contient des failles et, les technologies de surveillance capitaliste de la population continuant à s'améliorer, que cette nouvelle négociation est une occasion pour faire une fois de plus reculer les velléités des GAFAM (et des États).

En octobre 2017, deux commissions du Parlement européen publient leurs « opinions », des recommandations qui visent curieusement à faire d'ePrivacy un texte qui autorise l'analyse de nos messages, de nos appels et des sites que nous visitons, et même notre géolocalisation, sans notre consentement et à visée commerciale. Cela revient ni plus ni moins à vider de son sens le principe de consentement explicite pourtant tout juste mis en place par le RGPD ! Nous publions un site de campagne pour faire parler du texte[7]. La commission LIBE (« libertés civiles ») du Parlement européen, présidée par une eurodéputée de centre gauche proche des idées de la Quadrature, est mandatée pour avoir le dernier mot et arrêter la position du Parlement.

Pour mieux comprendre l'état de ce texte qui pourrait défaire des pans entiers du RGPD, nous devons plonger un instant dans les méandres des mécanismes de l'Union européenne. En principe, toute nouvelle norme créée par l'UE ne peut être adoptée que si le Parlement européen et les gouvernements des États membres (qui négocient au sein du Conseil de l'UE) se mettent d'accord sur un texte identique – ce qui peut prendre des mois et plusieurs lectures par institution. Pour gagner du temps, les règles de procédure du Parlement prévoient ce qui suit : une commission d'examen (constituée d'une soixantaine de députés sur les 751) arrête, seule, la position du Parlement et dispose d'un mandat pour négocier avec le Conseil de l'UE, au nom de l'ensemble du Parlement, afin de trouver un texte commun. Cette négociation, sous la supervision de la Commission européenne, est appelée « trilogue ». Elle brille par son absence totale de transparence. Lorsque le trilogue aboutit à un

consensus, il ne reste plus au Parlement et au Conseil qu'à adopter le texte de compromis par un vote formel.

Pour maintenir son mandat de négociation et arriver à un texte commun, la présidente de la commission LIBE se retrouve prête à accepter des compromis importants, tels que l'exploitation des métadonnées de nos communications sans notre consentement. Mais mis sous pression par le public et les organisations de la société civile affirmant que le résultat de cette négociation serait rejeté en bloc, les députés retirent finalement les compromis les plus graves. En fin de compte, la commission LIBE finit par voter un texte érodant moins nos libertés que prévu, mais qui reste tout de même largement problématique.

Et ce n'est que le début : le fameux trilogue doit maintenant avoir lieu. Mais une autre pièce se joue, du côté des gouvernements. La mise à jour d'ePrivacy contient en effet une partie sur l'obligation de conservation généralisée des données de connexion. Or plusieurs associations attaquent justement la France sur la surveillance de masse induite par une conservation démesurée des données de connexion. Les différents membres de l'UE n'étant pas d'accord sur la réponse à donner à cette question (l'Italie et la France demandant un *open bar* sur nos données, l'Allemagne étant largement plus réservée, et la CJUE souhaitant calmer les velléités de surveillance de masse), difficile de trouver une position commune et d'aller négocier avec le Parlement.

Pour compliquer le tout, de nombreuses plaintes étant en cours contre les GAFAM (entre autres sur des points gérés par ePrivacy), de multiples appels sont lancés pour éviter de modifier la législation alors même que les APD n'arrivent pas à appliquer celle déjà en vigueur.

Résultat ? Nous en sommes restés là, et ça n'est pas un mal[8]. Les gouvernements doivent entériner une position commune avant de pouvoir démarrer les négociations en trilogue. Mais les discussions sont toujours engluées en 2022. Ce statu quo nous semble être plutôt une bonne situation : les textes actuels sont relativement corrects et, à l'inverse, rien ne nous garantit qu'un futur texte permettrait d'améliorer les choses.

Tout ça pour ça. Parfois, la victoire ressemble plus à un marécage qu'à autre chose.

Traduire le droit européen en droit français : la « loi protection des données personnelles »

Dès 2016, mais surtout à partir de 2018, les pays de l'Union européenne se lancent dans l'adaptation en droit national de deux textes : le RGPD et la directive 2016/680 (aussi appelée « directive Police-Justice »)[9]. Le premier impose des obligations à toute personne qui exploite les données personnelles d'Européens, sauf si elle le fait dans le cadre de la lutte contre les infractions et les menaces à la sécurité publique, donc pour le compte de l'État. Le second texte encadre, justement, cette lutte contre les infractions, en fixant des principes généraux que les États membres doivent traduire dans leur droit national en règles précises[10]. Les États membres ont jusqu'au 6 mai 2018 pour en faire la transposition.

En France, c'est le projet de loi Protection des données personnelles qui doit adapter ces deux textes. La Quadrature rencontre la rapporteure du projet de loi, Paula Forteza, alors encore membre de LREM, et propose en janvier 2018 six amendements[11] aux parlementaires :

- Faciliter les actions de groupe, en prévoyant que les personnes (notamment les entreprises) sanctionnées remboursent à l'association les frais engagés pour porter l'action.
- Exiger que les données soient chiffrées de bout en bout chaque fois que cela est possible.
- Préciser dans la loi le caractère libre du consentement.
- Concilier de façon cohérente la liberté d'expression et la protection des données personnelles, notamment en intégrant la jurisprudence de la Cour européenne des droits de l'homme

(CEDH) qui instaure le critère de « contribution à un débat d'intérêt général » pour autoriser la publication de données.
- Renforcer la protection des données sensibles, en corrigeant des imprécisions du RGPD, en intégrant des positions de la CNIL.
- Corriger la loi Renseignement de 2015.

En effet, la directive réglemente aussi des sujets portés par la fameuse loi Renseignement, qui doit donc être modifiée pour être rendue conforme. Une occasion en or pour nous ! Nous proposons alors quatre axes d'amélioration, qui sont d'ailleurs tous exigés par la directive.

Premièrement, que les personnes qui font l'objet d'une mesure de surveillance en soient informées dès que cette mesure prend fin, ou ultérieurement si cela met en péril l'objectif qui a initialement motivé la mesure (actuellement, ces personnes n'ont absolument aucune façon d'être informées des mesures subies). Deuxièmement, que la Commission nationale de contrôle des techniques de renseignement (CNCTR) ait accès aux renseignements transmis aux services français par des services étrangers, afin de vérifier que ceux-ci sont légalement exploités (ce que la CNCTR ne peut pas faire aujourd'hui). Troisièmement, que toute personne puisse saisir une juridiction pour contester la légalité d'une mesure de surveillance dont elle pense faire l'objet (ce que le droit français ne prévoit pas s'agissant des mesures de surveillance internationale, menée en particulier par la DGSE). Enfin, quatrièmement, que les services français ne puissent échanger des renseignements avec d'autres services, français ou étrangers, qu'en respectant les mêmes conditions que pour la mise en œuvre d'une technique de recueil de renseignement, et sous le contrôle de la CNCTR.

Mais députés et sénateurs ne l'entendent pas de cette oreille et refusent de légiférer pour adapter la sacro-sainte loi Renseignement à la directive. Incroyablement, cela revient, ni plus ni moins, à refuser d'appliquer le

droit européen en droit français. Les parlementaires seraient-ils partisans du Frexit ?

Dans les amendements au projet de loi déposés par des députés s'en trouve un qui démontre une certaine tentation néolibérale : celui de Bruno Bonnell (LREM) qui souhaite transformer nos données personnelles en de simples marchandises[12], qu'il nous serait possible de céder pour accéder à un service sans avoir à payer en monnaie. Heureusement, ni le Parlement européen, ni la CNIL, ni l'ensemble des CNIL européennes ne sont dupes, et s'opposent clairement à ce que l'accès à des biens ou services puisse être conditionné à la cession de données personnelles. Il faut donc y voir une tentative désespérée de semer la confusion avant l'arrivée prochaine des changements majeurs que laisse espérer le règlement européen sur la protection des données. Mais cette idée revenant régulièrement, elle mérite qu'on s'y arrête.

LA PATRIMONIALISATION DES DONNÉES, FAUSSE BONNE IDÉE

Au printemps 2019, l'un de nous est invité au Luxembourg pour participer à un grand débat public, un show politique animé par Audrey Pulvar. L'enjeu du débat ? La « patrimonialisation des données ». Face à notre juriste de choc, l'autre débatteur est Gaspard Koenig, président du *think tank* Génération libre, qui tente depuis plusieurs années de populariser l'idée que chaque individu doit être propriétaire de ses données personnelles, au même titre qu'il l'est d'un capital ou d'un bien.

On voit l'intérêt immédiat de la proposition : utiliser des données personnelles sans consentement, ce serait du vol. Le droit de la propriété privée est suffisamment ancien et établi pour que nos données personnelles, si elles sont un bien que nous possédons, soient dès lors protégées contre les utilisations abusives qui en sont faites. Mieux encore : ce qu'on possède, on peut le vendre avec profit. Puisque Google s'enrichit en vendant nos données, on doit pouvoir gagner de l'argent en

vendant ses données à Google ! Hélas, ce rêve ultralibéral brille comme la pyrite : on dirait de l'or, mais c'est un simple caillou.

Les institutions juridiques en France et en Europe ont toujours refusé cette propriété des données personnelles. Elles estiment que la propriété privée n'est pas le seul moyen de définir un droit. Quand un État prélève un impôt ou assujettit un citoyen à une obligation militaire, ce n'est pas au nom d'un droit de propriété. Le fait que les parents aient des devoirs et des droits sur l'éducation de leurs enfants ne découle pas non plus d'un droit de propriété. On pourrait par exemple envisager les données comme une « production incorporelle » de la personne, au même titre qu'une idée ou qu'une œuvre, protégée par le droit d'auteur. Mais le droit européen affirme plutôt que les données personnelles sont un *prolongement*, une *partie* de la personne : elles constituent un attribut de la personnalité, une émanation immatérielle de l'individu, un prolongement incorporel de soi-même. La « personnalisation », donc, plutôt que la « patrimonialisation ».

C'est ce qui fonde l'efficacité du RGPD : même si vous consentez au traitement de vos données personnelles par un site Web pour une finalité définie, vous gardez un certain nombre de droits sur ces données (accès, rectification, opposition, effacement, etc.), ainsi que la possibilité de révoquer à tout moment votre consentement. En revanche si vous les aviez vendues, vous auriez perdu tous ces droits.

Par ailleurs, l'approche individualiste de la logique « patrimoniale » lui fait manquer le véritable enjeu de l'exploitation des données, qui est collectif, à l'échelle de la société tout entière. D'abord une mise au point : nous ne devons pas protéger nos données personnelles sous prétexte que les sites Web nous espionneraient ou nous surveilleraient – l'enjeu n'est pas là. Mais nous devons les protéger parce que les sites Web les utilisent pour nous transformer en cibles publicitaires : les traces que nous laissons en naviguant sur le Web permettent aux publicitaires de nous inscrire dans une multitude de profils dont nous sommes l'intersection unique. Ces pratiques ont transformé le Web en vaste espace publicitaire et marchand.

Que je m'appelle Gérard Martin, cadre dans l'industrie alimentaire vivant dans un pavillon au 37 de la rue des Bégonias, n'intéresse pas directement les publicitaires en ligne (ils ne sont pas policiers). Ce qui les intéresse est anonyme et me relie à mes proches : si je suis célibataire (restaurant, parfum, livraison à domicile) ou en couple (voyage, voiture, immobilier), si j'ai des enfants en bas âge (couches) ou plus grands (vélo, jeux vidéo), etc.

Les données personnelles valorisées par les publicitaires m'impliquent en tant qu'élément d'un ensemble familial, professionnel ou social qui me dépasse. Google ne vend pas aux publicitaires des données individuelles, mais des données « agrégées ». Vous n'êtes une personne intéressante que parce que vous êtes à l'intersection d'un réseau familial qui lit des mangas, aime tricoter, et vit dans telle région avec tel pouvoir d'achat, d'un réseau professionnel qui achète des services informatiques ou des grues de chantier, d'un réseau social qui vote et revendique des droits. Ce sont des données collectives, et la voie de la patrimonialisation des données personnelles revient à reconnaître un droit de propriété sur une chose qui ne vous appartient pas en propre. C'est d'ailleurs pour avoir compris l'importance de cette dimension réticulaire des données personnelles que des entreprises comme Google ou Facebook ont construit leurs empires sur la publicité ciblée.

Cette approche permet aux régies publicitaires de modéliser des comportements et d'essayer de les influencer grâce à des messages publicitaires, qu'il s'agisse d'engendrer un acte économique (l'achat), un acte social (prévention médicale, par exemple) ou un acte politique : le vote. On se souvient par exemple de l'affaire Cambridge Analytica, qui a mis au jour l'utilisation des données fournies par Facebook pour influencer les électeurs lors du référendum britannique sur le Brexit (juin 2016) et lors de la présidentielle américaine de novembre 2016 (élection de Trump). L'exploitation des données personnelles a des conséquences sociales. La vie privée est un droit collectif.

Malheureusement, la CNIL semble avoir assoupli sa position sur la patrimonialisation des données. Elle considère aujourd'hui qu'un service

en ligne peut conditionner son accès soit au paiement d'un abonnement, soit au traitement des données personnelles des internautes à des fins publicitaires. Autrement dit, la CNIL autorise, sous certaines conditions[13], les services en ligne, notamment le monde de la presse en ligne, à considérer que les données de ses utilisateurs valent quelques euros.

5. MULTIPLICATION DES FRONTS : L'HEURE DES CHOIX

La multiplication des chantiers législatifs au sein de l'Union européenne entraîne une surchauffe. La Quadrature, avec ses petits moyens, n'est pas capable de suivre tous les dossiers avec efficacité. Cette saturation oblige l'association à faire des choix qui ont des conséquences sur son audience et sa popularité.

Pourtant, plusieurs décisions européennes sont d'abord reçues comme de bonnes nouvelles, porteuses d'espoir. D'abord, en octobre 2015, la Cour de justice de l'Union européenne (CJUE) invalide le « Safe Harbor », un accord passé en juillet 2000 entre l'Union européenne et les États-Unis pour réglementer le transfert des données personnelles des Européens vers le territoire américain. Le droit des États-Unis est beaucoup moins protecteur que le droit européen (le RGPD notamment), et un jeune Autrichien de 28 ans, Max Schrems, a invoqué cette incohérence pour attaquer l'exploitation par Facebook de ses données personnelles. À nos yeux, cette décision de la CJUE est évidemment une victoire. Dans un contexte où les géants du Web semblent imbattables, ces victoires rebattent les cartes en faveur des activistes, au moins ponctuellement. Difficile de ne pas espérer de nouveau.

Autre motif de satisfaction : au printemps 2016, le BEREC, qui est le coordonnateur européen des autorités nationales de régulation des télécoms (l'ARCEP en France), présente ses lignes directrices sur la neutralité du Net au sein de l'Union européenne et les soumet à une consultation publique. L'organe de régulation reçoit en quelques semaines

480 000 commentaires, qui plébiscitent le respect de la neutralité du réseau. Les opérateurs de réseaux (téléphone et Internet), qui avaient mis en avant l'arrivée prochaine de la technologie 5G pour justifier l'abandon de la neutralité, en sont pour leurs frais. Les organisations de défense des droits dans l'espace numérique sont soulagées : les pires menaces ont été repoussées et les mauvaises pratiques de gestion du réseau sont de plus en plus rares.

Mais voici qu'arrivent en même temps deux grands textes européens : la « directive Copyright » et le « règlement Terro ». La Quadrature doit choisir dans lequel des deux chantiers jeter ses forces.

L'EUROPE ET LE DROIT D'AUTEUR : LA DIRECTIVE COPYRIGHT

Le 14 septembre 2016, est présentée par la Commission européenne la directive sur le droit d'auteur dans le marché unique numérique, rapidement surnommée « directive Copyright », chargée de mettre à jour la législation autour du droit d'auteur dans un monde toujours plus connecté et numérisé.

Cette mise à jour, nous l'appelons de nos vœux depuis longtemps, en espérant qu'elle prenne en compte les évolutions de notre rapport et de notre accès à la culture : en particulier, légaliser le partage non marchand et autoriser la pratique du remix, voire lui donner une légitimité en tant qu'acte créatif. En 2012, déjà, nous participions à l'échelle européenne à la bataille du copyright (souvenez-vous de l'opération Datalove !). Nous avions rédigé avec Philippe Aigrain, auteur de *Sharing*, un article intitulé « Éléments pour la réforme du droit d'auteur et des politiques culturelles liées », qui comprenait quatorze points essentiels[1] :

1. Reconnaître le partage non marchand des œuvres numériques entre individus par l'épuisement des droits.

2. Reconnaître la légitimité de la référence.

3. Mettre en œuvre des exceptions solides et obligatoires pour les pratiques éducatives et de recherche.

4. Mettre à disposition sans frais les œuvres orphelines (sans ayant droit) par les bibliothèques et les archives et autoriser leurs usages larges.

5. Instaurer la liberté des usages collectifs non marchands.

6. Mettre en place de nouveaux financements mutualisés pour un financement large (réparti sur de nombreux contributeurs et projets) de la culture numérique (la « contribution créative »).

7. Créer une législation imposant des termes équitables dans les contrats d'édition et de distribution.

8. Promouvoir une politique préventive de concurrence pour prévenir les monopoles de distribution et leurs abus.

9. Réformer la gestion collective.

10. Maîtriser la pollution publicitaire.

11. Fixer des normes effectives pour la neutralité du Net et l'ouverture des appareils.

12. Rendre obligatoire l'enregistrement ou copyright 2.0.

13. Réfléchir aux financements publics culturels et à une réforme fiscale.

14. Créer un statut positif protégeant le domaine public et les communs volontaires.

En mai 2014, dans le prolongement de cette montée en puissance des partisans du libre partage, Julia Reda, membre du Parti pirate allemand, est élue députée européenne. Probablement dans l'objectif de tester le sérieux du Parti pirate, le Parlement européen lui confie la préparation d'un rapport sur la mise en œuvre de la directive 2001/29/CE concernant l'harmonisation du droit d'auteur en Europe. Elle rend son rapport en janvier 2015 et celui-ci est salué par la Quadrature[2] car, bien qu'il conserve le principe général du droit d'auteur (on aurait pu s'attendre à une position plus radicale de la part du Parti pirate, dont le fondateur a pu dire que le copyright était un monopole ou encore une religion intégriste), il reprend un certain nombre de nos propositions. Toutefois, la « pirate »

a laissé de côté une part importante de notre vision : la légalisation du partage non-marchand des œuvres entre individus.

Or s'il est bien une chose que la Quadrature a intégrée depuis longtemps, c'est qu'il n'y a aucun avantage à faire des propositions molles, voire consensuelles, au pouvoir. Avoir des exigences radicales permet de garantir un débat sur notre terrain. Si le point de départ est déjà un consensus, alors on est certain de perdre sur tous les tableaux. Le consensus ne doit être que le résultat obtenu *après* une lutte farouche pour défendre nos positions. Voire, pour une organisation comme la nôtre, il peut ne jamais être atteint : sans carrière politique, sans objectif électoral, ni même questions de popularité, la Quadrature n'a pas besoin d'être dans le consensus.

Refuser de se battre sur la légalisation du partage, c'est accepter de débattre sur des sujets peut-être intéressants, malheureusement nécessaires, mais in fine accessoires. Depuis Hadopi, l'audience de la Quadrature est en partie construite autour de gens attachés au partage, en particulier via le *peer-to-peer*. Reculer sur ce point signifie en France reculer sur un texte qui aurait rendu Hadopi caduque. Avec le rapport Reda, finalement, c'est malheureusement un symbole qui disparaît.

Mais en 2015, puisque le « gros morceau » est absent du rapport, les militants doivent se rabattre sur quelques luttes annexes. Parmi elles, l'obligation dite de « filtrage a priori » (les « *upload filters* »), qui consiste à obliger les plateformes à rendre impossible l'envoi (*upload*) d'œuvres protégées par le copyright, sur la base d'une liste d'œuvres établie par des filtres automatiques. C'est l'article 13 du texte, qui focalise dès lors les débats.

Il pose un nombre important de problèmes graves :

- L'inversion de la charge de la preuve : au lieu d'exiger que l'ayant droit prouve l'utilisation illicite de son œuvre, c'est à chaque personne qui met en ligne un contenu de prouver, après suppression automatique, que son contenu ne violait pas les droits d'autrui.

- La rupture d'égalité devant la loi : alors que les ayants droit n'ont pas à intenter d'action judiciaire pour faire supprimer des contenus, les éditeurs dont les contenus ont été abusivement supprimés doivent, eux, supporter la charge d'une action judiciaire pour faire valoir leurs droits a posteriori.
- Le contrôle des outils de détection : qui contrôlera les programmes de filtrage, les « robocopyright », qui vérifiera leurs paramétrages ? Ceux-ci seront-ils publics ? Qui pourra certifier que ces programmes auront la finesse d'analyse nécessaire pour distinguer la reprise illicite d'une œuvre et son détournement en parodie ? Qui pourra valider qu'il n'y aura pas d'interprétation abusive du droit d'auteur ? Au vu du fonctionnement arbitraire et approximatif de ces robots sur des plateformes de vidéo, comme le Content ID de YouTube (qui a pourtant coûté une centaine de millions de dollars en développement), il est d'ores et déjà prouvé qu'ils commettent de nombreuses erreurs. Quant à la liste d'œuvres protégées, que contient-elle ? Qui a la possibilité d'y ajouter des œuvres ? Les œuvres peuvent-elles en être retirées ? Sous quelle autorité ?

Un autre article, l'article 11, est lui aussi repéré comme dangereux. Il prévoit la création d'un « droit voisin » pour les éditeurs de presse : de nombreux acteurs du Web, dont Google, agrègent des articles de presse et profitent de ces « contenus » pour attirer des visiteurs sans jamais reverser de revenus aux journaux (bien que cette agrégation soit aussi cause de visites supplémentaires sur les sites de presse). Ce qui semble bénin, comme souvent, ne l'est pas : en souhaitant instaurer de nouveaux droits pour les éditeurs de presse et de nouvelles contraintes pour les grands agrégateurs comme Google, le texte restreint l'usage de ces contenus bien au-delà, en affectant aussi potentiellement des acteurs non lucratifs et tout l'écosystème de l'accès à l'information.

Ces deux articles entraînent une mobilisation massive de la société civile, qui répond en miroir à l'énorme campagne de lobbying des plateformes auprès des eurodéputés, décrite par certains anciens des couloirs de Bruxelles comme la plus intense et onéreuse jamais vue. La directive Copyright est dans tous les journaux qui, pensant nécessairement bénéficier de l'article 11, se positionnent généralement en sa faveur. La situation est complexe et rien n'est gagné.

Cette période est aussi celle où certains youtubeurs commencent à plus largement s'apercevoir que cette lutte contre la contrefaçon va les attaquer de plein fouet. Le filtrage automatique qui arrive par la directive Copyright va en effet empêcher par défaut toute réutilisation d'œuvres dans leurs vidéos, même pour quelques secondes, alors que la loi les y autoriserait. Le pouvoir des ayants droit sur la diffusion des œuvres via les grandes plateformes grandit encore. Le fait que la directrice générale de YouTube, Susan Wojcicki, prenne la plume pour prévenir ses ouailles, dans un magnifique moment de communion, que l'article 13 « pose un danger autant à votre gagne-pain qu'à votre capacité à partager votre voix avec le monde » n'y est peut-être pas étranger.

Le pouvoir du copyright est tellement important que les effets de bord sont déjà quasi quotidiens. Par exemple ? L'éditeur du jeu vidéo Fortnite se retrouve obligé de développer une fonctionnalité supprimant certains titres musicaux lors de la diffusion des parties en direct, les droits de ces titres étant couverts dans le jeu mais pas sur YouTube. Ou encore la suppression abusive de la vidéo d'un professeur à la suite d'une plainte de TF1, car elle contenait un extrait d'une série dans laquelle il souhaitait montrer une erreur à ses élèves.

UNE POSITION CONTROVERSÉE

Même si tout ce qui pouvait être dit a été dit sur la directive Copyright, les dernières évolutions de l'article 13 sur le filtrage automatique des plateformes nous inquiètent. Des critères sur les plateformes concernées

ont été ajoutés : la lucrativité, la taille, ainsi que la présence d'une recommandation algorithmique… Voilà qui réduit par la même occasion la liste des cibles aux seuls acteurs de la taille des GAFAM. Et c'est là que commence la discussion interne : finalement, est-ce bien le rôle de la Quadrature d'aller défendre YouTube et consorts ? Le soutien à la diffusion de contenus sur ces grandes plateformes est de plus en plus intenable, ou du moins incohérent, tout comme aller militer contre un texte pour l'« internet libre et ouvert » main dans la main avec Facebook et Google.

Parallèlement, alors que la bataille du copyright n'est pas encore terminée, le terrorisme et la surveillance de masse sont sur toutes les lèvres. Et des lois toujours plus sécuritaires débordent des tiroirs. La directive Copyright occupe une si grande place dans l'esprit des communautés activistes que personne, parmi nos alliés, ne fait le choix de se lancer pour faire campagne contre les risques du règlement Terroriste. Et sans aller jusqu'à prétendre que les risques posés par la directive Copyright semblent légers, disons que la brutalité des mesures du règlement Terro le font monter comparativement plus haut dans l'échelle de nos priorités.

La Quadrature, ça n'est pas une armée d'analystes, d'avocats, de juristes, d'administrateurs systèmes, de chercheurs et de chargés de campagne. C'est, au mieux, trois ou quatre de chaque, dont seulement six salariés à plein temps. Attaquer la directive Copyright et le règlement Terro en même temps est matériellement impossible. Et, dans un contexte où la levée de boucliers contre la directive Copyright est déjà massive et bien organisée au niveau européen (heureusement !), nous décidons de concentrer nos efforts sur le règlement Terroriste, auquel personne ne s'attaque frontalement. Résultat immédiat, la campagne contre l'article 13 de la directive Copyright passe de facto en « priorité basse ». Cette décision nous sera durement reprochée par certains alliés, qui considèrent que nous abandonnons le navire au moment le plus crucial. Avec la distance vient le bénéfice du recul, et nous aurions peut-être pu et dû mieux expliquer notre raisonnement sur ce choix stratégique, mais après

le vote qui entérine l'article 13 de la directive Copyright le 12 septembre 2018, la communauté est sous le choc. Les membres et l'équipe salariée se retrouvent mis en cause par celles et ceux qu'ils estiment pourtant être des alliés historiques. Pour preuve, Jérémie Zimmermann, éloigné depuis plusieurs années de l'association, demande à faire publier un texte dans lequel il démissionne officiellement de son statut de membre de la Quadrature[3]. Cet épisode restera un point de rupture de l'histoire de l'association pour de nombreuses personnes. Au cœur de ces débats, quelqu'un nous confirmera malgré tout que notre action contre le règlement Terroriste est cruciale : il s'agit de Julia Reda.

RÈGLEMENT EUROPÉEN CONTRE LA DIFFUSION DU TERRORISME EN LIGNE

Revenons un instant en 2014 : un dîner privé réunit les représentants de Google, Facebook, Microsoft, Twitter et des gouvernements européens. Le thème : comment s'attaquer à l'extrémisme et à la radicalisation en ligne et créer une meilleure coopération entre l'Union européenne et leurs sites à très fort trafic ? Le cœur de l'approche : la coopération volontaire.

Cette rencontre marque un changement de stratégie. Se rendant compte de la difficulté, tant humaine que technique, de censurer, surveiller et finalement contrôler Internet, les États tentent une nouvelle approche : travailler *avec* les géants de la tech. Les traiter en copains, ou en exécutants, plutôt qu'en adversaires. Après tout, quand, en France, 43 % des gens utilisent Facebook quotidiennement (en décembre 2013), le plus simple pour suivre ce qu'ils y font est de passer un accord avec Facebook.

Les GAFAM, surtout les plus jeunes, sont en quête de reconnaissance. Les États courtisent de plus en plus les géants de la tech, en témoignent les idées de « techplomacie » et l'« ambassadeur auprès de

Facebook », missionné par le Danemark. « D'abord ils vous ignorent, ensuite ils vous ridiculisent, ensuite ils vous combattent, puis vous gagnez », disait Gandhi. Et si, plutôt, ils vous transformaient en collaborateur, dissolvant les deux dernières étapes en un partenariat public-privé aux contours flous ? L'État, après avoir d'abord ignoré, puis regardé mi-circonspect, mi-amusé les sites Web devenir des services incontournables du quotidien, a observé avec inquiétude le réseau Internet mondial donner corps à de multiples droits (telle la liberté d'expression) jusqu'alors assez théoriques. Il voit désormais s'enrichir des entreprises privées à l'appétit insatiable. Jusque-là adversaire des champions de la liberté sur Internet que s'imaginent être Google ou Facebook, l'État décide habilement de faire disparaître cette hostilité contre-productive. Et les deux camps – public et privé – de s'allier : plutôt que de combattre, centralisons donc Internet ensemble, à notre bénéfice mutuel !

Car à y réfléchir un instant, dans sa vision décentralisée originale, Internet est, du fait de sa conception, impossible à censurer et à contrôler. « Le Net interprète la censure comme un dégât et contourne celle-ci », explique dès 1993 un des fondateurs de l'Electronic Frontier Foundation (EFF), John Gilmore. En effet, si 500 millions de personnes utilisent 150 000 sites, forums, fournisseurs d'adresses e-mail et applications de chat différents pour discuter et échanger, comment contrôler ce désordre ? Mais, si on peut écrire une loi pour obtenir ce qu'on veut de 5, 10 ou 100 sites, et créer un goulot d'étranglement pour que les gens passent par ces sites, on peut commencer à aboutir à quelque chose. En tout cas, c'est plus réaliste que d'essayer de contrôler tout l'internet, qui refuse d'être une entité unique et s'obstine à être un ensemble de réseaux mouvants et d'utilisateurs associés.

Du côté des GAFAM, un texte qui inscrit dans la loi leur manière de faire, leur capacité technique, comme seul horizon possible de la mise sous contrôle du désordre d'Internet, c'est un texte positif : quel nouvel entrant aurait les moyens de les rattraper, techniquement ou en matière d'investissements ? Une loi qui dirait, en substance, « il faut contrôler les

publications de public sur Internet par des systèmes automatisés complexes et coûteux, comme le font Google et Facebook » garantit à Google et Facebook d'être, si ce n'est les seuls à disposer de ces systèmes, du moins les uniques fournisseurs de ces systèmes pour tous les autres acteurs (ce qui revient presque au même). Le genre de barrière à l'entrée dont rêve tout monopoliste.

Cette coopération volontaire étant engagée au niveau européen, on commence à voir fleurir différents éléments qui la formalisent de plus en plus. En juin 2017, le Conseil européen explique qu'il attend des entreprises du secteur qu'elles « mettent au point de nouvelles technologies et de nouveaux outils en vue d'améliorer la détection automatique et la suppression des contenus qui incitent à la commission d'actes terroristes. Cela devrait être complété par les mesures législatives appropriées au niveau de l'Union européenne, si nécessaire[4]. » En mars 2018, c'est la Commission européenne qui adopte une série de « recommandations pour lutter efficacement contre le contenu illégal en ligne ».

C'est finalement en septembre 2018 que nous voyons apparaître sur notre radar un nouveau texte qui porte en son sein de graves dangers pour nos libertés. C'est un règlement sur des mesures antiterroristes (évidemment), qui porte le doux nom de « règlement européen contre la diffusion du terrorisme en ligne » et qui, en tant que règlement, une fois voté, s'applique directement dans chaque État membre, sans passer par la case du législateur local (le Parlement, en France).

Pourquoi nous alarmons-nous ? Car ce nouveau règlement imposera deux obligations à tout acteur du Web (hébergeurs de blogs ou de vidéos, sites de presse, petits forums ou grands réseaux sociaux) : premièrement, bloquer en une heure n'importe quel contenu signalé comme « terroriste » par la police (sans qualification préalable d'un juge) et ce, 24 heures sur 24 et 7 jours sur 7 ; et deuxièmement, devancer les demandes de la police en détectant lui-même les contenus illicites à l'aide d'outils de filtrage automatisés.

L'obligation de blocage en une heure est délirante. Elle est intenable pour la majorité des acteurs du Net. Ou, plus spécifiquement, elle est étudiée pour n'être tenable que par une très petite minorité d'entre eux. Celle qui était a priori présente au dîner en 2014… C'est une manière d'obtenir le goulot d'étranglement qui cherche à concentrer le trafic par un nombre restreint d'acteurs. Et c'est la délégation de la censure aux géants du Web qui s'accomplit.

Par ailleurs, le fait que la qualification de terroriste vienne de la seule police est également inacceptable. Nous défendons depuis des années la nécessité absolue dans tout cas de censure de la qualification par un juge, seul capable de mettre en balance le difficile équilibre entre les différentes libertés. Voir ce pouvoir confié à l'exécutif seul est aberrant.

Quant au filtrage automatisé, en revoici un énième avatar, cette fois-ci au nom de la lutte contre le terrorisme. Sans surprise, il ne répond toujours pas aux sempiternels problèmes : aucune liste de « contenus terroristes » ne permet de bloquer une vidéo, un article ou une photo a priori… Pire, après avoir fièrement annoncé être capable de faire de la modération en direct, Facebook est violemment désavoué par la réalité : en mars 2019, le suprémaciste blanc à l'origine du massacre dans deux mosquées de Christchurch en Nouvelle-Zélande diffuse en temps réel les images de ses crimes via le réseau social. La vidéo se répand et le flux est immédiatement repris et décuplé. Malgré ses annonces, Facebook échoue à modérer. De toute évidence, l'état de l'art technique des capacités de Facebook et des autres est largement en dessous de ce qu'ils ont pu vendre aux gouvernements. Mais peu importe, ne laissons pas la réalité contrarier un si beau partenariat.

Tant que les GAFAM ne cherchent pas à empiéter sur les plates-bandes de l'État, en se plaçant par exemple en fournisseurs et garants de l'identité ou, pire, en proposant le lancement d'une monnaie (on se souvient de l'échec du libra de Facebook sur ce point), les États sont prêts à se laisser convaincre par le discours commercial. Finalement, tout le monde y gagne, à part la population : les GAFAM obtiennent plus de

pouvoir et sont toujours plus incontournables, les États réduisent le nombre d'interlocuteurs.

Au bout du compte, une chose apparaît en tout cas clairement : le rapprochement stratégique entre les entreprises privées et l'État s'opère sur (presque) tous les thèmes et si la centralisation qui en découle bénéficie aux deux parties, elle se fait toujours aux dépens de la population. Dans ce contexte, l'idée de l'interopérabilité des services, qui encourage la décentralisation du Web au détriment des grandes plateformes, redevient une idée radicale que la Quadrature pourra porter avec fierté. Nous y reviendrons.

Après trente-deux mois de débat, le règlement Terroriste est adopté par le Parlement européen le 28 avril 2021. Entré en vigueur le 6 juin 2021, il est applicable à partir du 7 juin 2022. Les terroristes tremblent déjà.

6. DE LA DÉMOCRATIE NUMÉRIQUE À L'EFFRITEMENT DE LA DÉMOCRATIE

La Quadrature a toujours eu pour but, dès sa création, de participer au débat démocratique de manière constructive et d'être force de proposition. Ce qui n'est pas une mince affaire.

Sous la présidence de Nicolas Sarkozy, tout effort de notre part était directement tué dans l'œuf. Chantre de l'« internet civilisé », il incarnait à peu près tout ce contre quoi la Quadrature se battait. Qu'en serait-il sous François Hollande ? Au début, nous avions bon espoir. Pendant la campagne présidentielle, Philippe Aigrain avait publié *Sharing*[1], un guide-manifeste pour un partage sur Internet qui protégerait aussi les créateurs. Il avait senti l'équipe de campagne du candidat Hollande (dont Aurélie Filipetti, future ministre de la Culture) plutôt réceptive à ses propositions, qui étaient aussi les nôtres. Mais une nouvelle leçon nous attendait : celle de la puissance des lobbies. Le programme de Hollande promettait d'en finir avec la Hadopi, mais au soir de l'élection, il n'en est déjà plus question. En quelques jours, tout le monde à la Quadrature prend conscience que notre opposition au gouvernement va demeurer la même, quel que soit son bord politique.

UNE CONSULTATION FANTOCHE SOUS HOLLANDE

En 2015, Axelle Lemaire est à la manœuvre du numérique en tant que secrétaire d'État au numérique. Elle propose une grande consultation

citoyenne avec pour objectif de « coécrire la loi pour une République numérique ». Les personnes intéressées par ces sujets ont trois semaines, du 26 septembre au 18 octobre 2015, pour faire des propositions, les amender et les voter, avant que le gouvernement n'y réponde pour choisir celles qui seront intégrées dans le projet de loi. Cette consultation bénéficie d'une forte participation de la société civile, dont celles de Wikimédia, de l'April et de La Quadrature du Net. Sans nous faire d'illusions en entrant dans le jeu de cette consultation, nous proposons neuf contributions (trois propositions et six amendements à des articles existants). Alors que ces propositions reçoivent plus de 95 % de soutien des votants à la plateforme, le gouvernement n'en accepte initialement que deux.

Les propositions de la société civile, pour certaines massivement plébiscitées aussi (la communication du code source d'un logiciel public[2], l'utilisation de logiciels libres & de GNU/Linux dans les écoles, les universités[3] ou les administrations, l'inscription dans la loi du délit de non-respect de la neutralité du Net, ou encore, la reconnaissance du droit au chiffrement) n'auront pas beaucoup plus de succès. Au mieux, des promesses de mise en place dans des chantiers en cours… mais surtout, pas trop de législation. Puis le texte, augmenté des quelques propositions issues de la consultation (pas forcément les plus plébiscitées, d'ailleurs), part en discussion à l'Assemblée nationale. En décembre 2015, l'avant-projet de loi est présenté et contient quelques avancées notables. L'ouverture des données publiques, largement soutenue par la société civile, y est proposée, et l'accès ouvert aux publications scientifiques financées par l'argent public semble enfin possible, via la reconnaissance d'un droit d'exploitation secondaire pour les chercheurs. Droit qui n'aurait probablement pas vu le jour sans la pression de la communauté… D'autres éléments du texte favorisent une diffusion plus large des informations et de la connaissance : l'inscription du droit à la portabilité des données, qui permet à l'utilisateur de ne pas se retrouver enfermé dans un écosystème captif et de faire lui-même usage de ses données – encore faut-il qu'un autre service existe où les déposer –, ou

encore le maintien de la connexion Internet pour les personnes en incapacité de paiement en sont des exemples.

Mais les textes retenus sont, lecture après lecture, vidés de leur substance[4]. Pour tenter de maintenir des avancées politiques, plusieurs organisations, dont la Quadrature, publient une liste d'amendements[5] en janvier 2016 : communs numériques, logiciels libres et formats ouverts, ou encore liberté de panorama (une exception au droit d'auteur permettant de prendre en photo des œuvres protégées par le droit d'auteur se trouvant dans l'espace public, souvent des œuvres d'art ou d'architecture). En juin 2016, les associations regroupées sous la bannière de l'Observatoire des libertés et du numérique (OLN) dénoncent le travail parlementaire réalisé par la secrétaire d'État et font état d'un bilan décevant des discussions autour du texte, alors même que le processus législatif n'est pas encore terminé. Elles dénoncent même qu'en l'état le texte introduit une notion dangereuse : un système de détection automatique de contenus illicites, mécanisme que la LCEN (loi pour la confiance dans l'économie numérique) avait tout juste effleuré en obligeant les hébergeurs – des entités privées – à retirer promptement les contenus « manifestement illicites » signalés. Désormais, les hébergeurs de contenus devraient mettre en place un système de contrôle a priori. Un texte censé apporter des droits positifs finirait donc par faire passer un article proprement sécuritaire.

En juillet, Axelle Lemaire se plaint ouvertement dans une interview à *Mediapart*[6] du communiqué de l'OLN, arguant que « certains » souhaiteraient mettre à bas la démocratie représentative en la remplaçant par une « geekocratie »… après avoir elle-même demandé aux geeks de participer à un processus de coconstruction de la loi. Nous persistons alors[7] par un état des lieux du « bilan catastrophique du gouvernement sur le numérique ».

Ce qui aurait pu être une réconciliation entre le pouvoir politique et les spécialistes du numérique tombe dans le calcul politique de bas étage. Si bonnes intentions il y a pu avoir au départ, elles ne résistent pas au cynisme des professionnels de la politique et du pouvoir : encore une fois,

la consultation laisse le sentiment d'avoir surtout eu pour but de se donner un vernis de démocratie consultative, pour mieux légitimer des choix politiques globalement déjà décidés en amont.

COMMENT MACRON SÉDUIT LES START-UP POUR LANCER SA CAMPAGNE

À l'été 2016, le ministre de l'Économie et des Finances de François Hollande quitte son poste pour lancer son mouvement politique. Il sort de nulle part, n'a sa carte dans aucun parti politique, n'a jamais été élu, et n'a surtout aucune base militante, mais souhaite néanmoins se présenter à l'élection présidentielle qui se déroulera moins d'un an plus tard. Emmanuel Macron est un homme jeune, qui baigne dans le milieu des entrepreneurs et des start-up. Et c'est comme une start-up qu'il va gérer sa campagne : en levant des fonds sur de vagues promesses de gains, et en s'entourant de ressources prêtes à suivre le projet qui leur a été vendu sans compter leurs heures. Comme il n'a pas de programme, seulement une réputation, il laisse ses fans de la première heure organiser des débats sur tous les sujets possibles. C'est la première fois qu'on utilise aussi massivement les outils collaboratifs en ligne. Cette aptitude à accepter ou à aller chercher des méthodes de travail et d'*empowerment* (ou « capacitation ») des militants, les échanges avec la communauté de spécialistes comme celle du logiciel libre, renforcent l'idée que vend Macron : il pourrait être vraiment capable de représenter « le meilleur de tous les courants ».

Des centaines de soirées-débats seront organisées sur tous les sujets, des travaux sur le programme, partout en France. Nous sommes invités à plusieurs reprises à y participer. Il n'est évidemment pas question pour nous de nous afficher avec un candidat plutôt qu'un autre, sachant bien l'usage et l'instrumentalisation qui pourraient en être ensuite faits. Ce qui n'empêche pas un membre d'aller incognito, dans une froide soirée de mi-janvier 2017, prendre la température du groupe En Marche du XIV^{e} arrondissement parisien. Le sujet de l'échange : « Quelle vie privée dans

nos sociétés connectées ? »[8]. Le public est intéressé et participe. Les questions fusent : « Est-ce vraiment utile de protéger notre vie privée ? », « Finalement, face au Big Data, l'anonymisation n'est-elle pas vaine ? », ou encore « Comment éduquer la population face à l'évolution rapide des technologies ? ». À cette époque, le programme du candidat Macron n'est toujours pas sorti, et ses soutiens ne peuvent donc se fonder que sur ses actions au gouvernement, et ses diverses déclarations depuis son départ de Bercy fin août 2016. Que reste-t-il de ces débats dans le programme du candidat, sorti tardivement, le 2 mars 2017, un mois et demi avant le premier tour ?

Probablement un grand sentiment d'amertume et une apathie renouvelée, confirmée ou peut-être même décuplée pour cette génération dont de nombreuses personnes se prenaient au jeu de la politique, au rêve de pouvoir changer les choses pour la première fois. Ce gloubi-boulga managérial emprunte aux méthodologies agiles et aux communautés *open source* leurs valeurs sincères d'égalité et d'horizontalité, surfant sur des vocables comme « méritocratie » et vantant la « French Tech » pour faire briller les yeux des jeunes cadres et les transformer au plus vite en base militante, alors que le management du parti-entreprise ne se donne aucune obligation d'écouter sa base. Il rappelle également les entreprises qui mettent en place du management faussement agile et vidé de sa substance ou font de l'« *open source washing* », en profitant de la bonne image du logiciel libre sans contribuer aux biens communs informationnels. À y réfléchir, à la manœuvre des partis et des entreprises, ce sont peut-être les mêmes !... Un parti ou un État ? Finalement tout se gère comme une entreprise.

Peu importent les dégâts ou le cynisme, ce mode de gouvernance initié pendant la campagne se poursuit sous le gouvernement Philippe. Plusieurs consultations sont mises en place : les États généraux de la bioéthique, la Convention citoyenne pour le climat, et même le très éphémère Collectif citoyen sur la vaccination – allant jusqu'à proposer que trente-cinq citoyens « veillent à la transparence de la politique vaccinale » et « fassent remonter les questionnements des Français »[9]…

Une illusion de la participation citoyenne qui n'aura que peu, voire aucun impact sur la politique du gouvernement.

Au niveau numérique[10], le projet du président est très vague (une « Europe du numérique »), carrément surréaliste (l'autorisation de « déroger au droit pour permettre l'expérimentation »), voire fort consensuel (« supprimer les zones blanches » et « fibrer le pays »). Sur le reste, Emmanuel Macron a finalement retourné sa veste (« transparence sur les données personnelles ») ou laissé la société civile faire le travail à sa place (« renégocier le Privacy Shield », finalement tombé grâce à l'Autrichien Max Schrems).

Il flatte franchement l'orgueil des entrepreneurs. Mise en avant du concept (fumeux) de « start-up nation », discours dans les incubateurs de start-up à la gloire des « gens qui réussissent » face à ceux « qui ne sont rien », le numérique de Macron est celui du clinquant, loin de ceux qui le font réellement. Il utilise le milieu geek comme un affichage, un ruban à la boutonnière qu'on arbore pour faire beau mais qu'on enlève une fois rentré à la maison. En mettant en avant des projets phares, des start-up qui réussissent, en les faisant financer à grand renfort d'argent public par la banque publique d'investissement, il cache finalement tout un pan de l'économie réelle, celle qui fait tourner la machine au quotidien. On le verra notamment dans le choix de Microsoft pour héberger le Health Data Hub (HDH) – le grand entrepôt de nos données de santé.

Ces choix du pouvoir politique donnent au numérique un aspect de décor en carton-pâte. Les licornes (ces start-up valorisées à plus d'un milliard de dollars) comme étendard, un objectif non pas de rendre service à la communauté ou de résoudre des problèmes importants, mais de devenir milliardaire[11] : c'est toute une économie du vent qui est mise en avant.

Comment, dès lors, continuer à travailler avec le politique ? Comment espérer un changement de société, ou même des changements à la marge, voire, soyons fous, un simple respect des libertés fondamentales, quand tout échange avec les politiques finit immanquablement dans la démagogie ou le lobbying d'entreprises

puissantes ? Quand nous passons des mois à expliquer qu'un texte est totalement anticonstitutionnel, mais que malgré tout il se trouve une majorité de députés et sénateurs pour les voter (loi Avia sur la haine en ligne, « loi Sécurité globale »…), et que ces textes finissent en effet par être censurés, que faire ?

Même les multiples victoires juridiques de 2021 (dont celles des drones, sur lesquelles nous reviendrons) ne réussissent pas à faire entendre raison aux politiques. Pire : attaquer certains textes devient un risque d'aboutir à une mauvaise décision et de créer une jurisprudence qui pourrait être pire que les textes initiaux. Alors que faire ? Mettre en sommeil ce mode d'action pour ne conserver que les actions les plus sûres ?

Et pourtant, quelle que soit la qualité de ses analyses, quelle que soit l'énergie que ses membres y mettent, il semble que la seule chose qui empêche ces textes illibéraux d'être appliqués soit le droit. Mais jusqu'à quand ? Les sujets numériques portés par la Quadrature sont en effet au cœur de nombreuses évolutions de la société, et par là même des enjeux forts pour les politiques. L'association se retrouve en première ligne des tentatives de mainmise de l'État sur un réseau qui concentre tant d'espoirs d'émancipation. En somme, plus le numérique envahit nos vies, plus la puissance publique s'acharne à en reprendre le contrôle, contre la population, effritant d'autant notre démocratie.

En 2017, il n'y a plus de raison de conserver un état d'urgence en application depuis deux ans – niant de fait cette notion d'urgence. Le président Macron, tout juste élu, se retrouve donc à faire entrer un état d'exception dans le droit commun, avec la bénédiction des parlementaires français. À partir de là, tout discours essayant de sortir de cet état de stupeur devient inaudible. Au moment où les politiques de Trump, Johnson, Erdogan, Bolsonaro ou encore Orban font dans la démagogie d'État, on pouvait encore se penser à l'abri en France. Il est certain que c'est désormais de plus en plus difficile.

On arrive au stade où, quelle que soit la nature de l'opposition, quoi qu'il soit proposé pour répondre à un problème, que ça vienne de la

société civile ou directement de parlementaires, la réponse politique ne fait désormais plus aucun cas de ce que certains nomment pourtant la *realpolitik*. Fi de l'efficacité, du droit ou même de la réalité observable, le positionnement politique devient purement idéologique.

7. LA CAMPAGNE GAFAM

Au début de l'année 2018, un bruissement. Des sujets commencent à apparaître dans les médias à propos d'une mesure qui risque de bouleverser les activités touchant de près ou de loin à la conservation des données personnelles. « Les délais sont trop courts », se plaignent les PME, pendant que les entreprises spécialisées dans la captation de données continuent comme si de rien n'était, persuadées d'être « conformes ». Il n'est pire aveugle que celui qui ne veut pas voir : le 25 mai entre en application un texte qui a été adopté deux ans plus tôt : le RGPD. Malgré les déclarations paniquées, les cabinets d'avocats ou autres responsables juridiques ont eu vingt-quatre mois pour accorder le fonctionnement de leur entreprise avec la loi.

Depuis des mois, les GAFAM proposent des campagnes de communication dans lesquelles elles se targuent de protéger les données de leurs utilisateurs… Il va falloir remettre de l'ordre dans tout ça, car depuis ce 25 mai une entreprise ne peut plus justifier de nous surveiller au motif que nous y aurions « consenti » en oubliant de décocher une case obscure rangée en fin de formulaire ou derrière divers menus. C'est la victoire du « consentement explicite », que continuent de bafouer Google, Apple ou Amazon.

Fin décembre 2017, une idée avait germé parmi l'équipe salariée de la Quadrature. Et si on rappelait à tout le monde que les GAFAM ne sont pas *seulement* de grosses industries hégémoniques de la tech, mais qu'elles ont aussi et surtout un impact foncièrement négatif sur

l'ensemble de la société, entre autres en captant illégalement des données de tous leurs utilisateurs (et des autres) ?

Une communication très visuelle est mise au point, formée de cinq affiches imprimées sur du papier coloré, une par entreprise visée, rappelant pour chacune d'entre elles une action contestable :

- **Google filtre ta pensée :** Google filtre les résultats de recherche et les recommandations YouTube pour analyser tes réactions et t'enfermer dans sa bulle.
- **Apple sait où est ta mère :** Si tu as un smartphone sous iOS ou Android, il permet à Apple, Google et leurs apps d'enregistrer ta position, sans toujours te le dire ou te laisser le choix.
- **Facebook contrôle ce que tu peux lire :** Facebook trie les contenus de son fil d'actualité pour analyser tes réactions et t'enfermer dans sa bulle.
- **Amazon sait quels cadeaux tu auras :** Les comportements qui te semblent les plus anodins, analysés en masse, révèlent précisément ta personnalité, tes attentes et celles de ton entourage.
- **Microsoft formate tes enfants :** En 2015, Microsoft a payé 13 millions d'euros à l'Éducation nationale pour pouvoir fournir ses outils aux élèves et aux enseignants et les former.

Sur le site de campagne, ces textes peuvent être modifiés permettant aux utilisateurs de générer leurs propres affiches.

Proposée au débotté en fin de soirée du Quadr'apéro qui a lieu trois jours plus tard, la campagne entraîne finalement plus d'une quinzaine de personnes dans les rues froides de Paris avec sous le bras des affiches et des seaux de colle faite avec de la farine, de l'eau et du sucre. La campagne GAFAM démarre le soir du vendredi 22 décembre 2017[1].

Cinq jours plus tard, le 27, l'association se rend comme chaque année en Allemagne, à Leipzig, à l'occasion d'un congrès de hackers, le 34C3, le 34^{e} Chaos Communication Congress[2] (CCC, ou C3), organisé par le Chaos Computer Club[3] (CCC), le principal club de hackers en Allemagne. Les affiches sont accrochées dans le centre des congrès, sur la Tea House, l'espace géré par la Quadrature où il fait bon débattre autour d'un thé, mais aussi dans les couloirs, sur les portes[4].

C'est pendant cet événement que nous décidons, bénévoles et salariés de la Quadrature, d'utiliser un nouvel outil rendu possible par le RGPD : lancer une action de groupe pour toucher le plus de monde possible. Autour de ces affiches, qui fonctionnent très bien, se développe toute une campagne participative et communicative, joyeuse mais utile. C'est l'occasion de renouer avec les bénévoles et les sympathisants, qui vont pouvoir donner leur voix, leur temps, et diffuser le message à l'aide de cette communication simple et efficace.

Le 11 janvier 2018, des bénévoles déposent en Allemagne, de leur propre initiative, le nom de domaine gafam.info, et démarrent un outil de création automatisée des affiches de campagne. C'est en pas moins de vingt-quatre langues que les affiches originales seront rendues disponibles.

Début avril 2018, la campagne de « recrutement » démarre via le site de campagne gafam.laquadrature.net, avec pour objectif d'obtenir le plus de mandats possible d'utilisateurs des services des GAFAM qui auraient donc et par définition subi leurs pratiques illégales. Chaque semaine, un GAFAM est présenté et on explique ce qui lui est reproché. Cette campagne est un succès : plus de 12 000 personnes complètent le

formulaire et nous donnent mandat pour nous permettre d'attaquer en leur nom un ou plusieurs services auprès de la CNIL. C'est à ce jour la plus importante plainte collective déposée devant une APD en Europe.

Nous avions par ailleurs préparé le terrain avec la CNIL, en expliquant notre démarche, en nous mettant d'accord avec elle sur la meilleure façon de rédiger les plaintes et le niveau d'information nécessaire sur les mandants (étant entendu que nous ne leur demanderions pas de preuve de leur identité). Une trame de plainte est ensuite rédigée sur le principe du non-respect du consentement libre, finalement équivalent chez les cinq entreprises. Il est nécessaire ensuite de compléter cette trame pour chacune d'entre elles. Suit ainsi un appel à participation à travers les listes de diffusion et sur les réseaux sociaux, le 21 mai[5]. Ce sont des dizaines de personnes qui se retrouvent sur des pads pour compléter les cinq textes qui seront présentés à la CNIL.

Nous déposons les plaintes le 28 mai, trois jours à peine après l'entrée en vigueur du RGPD sur lequel s'appuient nos demandes. Probablement l'une de ses utilisations les plus rapides. En visant les GAFAM, nous nous attaquons aux plus grosses entreprises du numérique… Mais que leur reprochions-nous – que leur reprochons-nous toujours d'ailleurs ?

LES GAFAM, QUI SONT-ILS ?

Fondée il y a vingt ans par Larry Page et Sergueï Brin, Google est aujourd'hui une filiale d'Alphabet, la maison mère d'un groupe implanté partout dans le monde. Ses services se sont multipliés : gestion des e-mails avec Gmail, du calendrier avec Agenda, stockage et édition de documents avec Drive et GSuite, navigateur Internet avec Chrome, régie publicitaire avec Network qui s'appuie sur les outils de développement Analytics et Ads, mais aussi plateforme pour smartphones avec Android, publication de vidéos avec YouTube, etc. En 2021, le groupe réalise 260

milliards de dollars de chiffre d'affaires, à plus de 80 % issus de la publicité en ligne.

Fondée en 1976, notamment par Steve Jobs et bien avant l'avènement d'Internet, l'entreprise Apple se concentre sur la vente de ses propres ordinateurs, équipés de systèmes d'exploitation qu'elle développe elle-même. En 1984, elle annonce le lancement de son Macintosh au moyen d'une publicité vidéo réalisée par Ridley Scott, intitulée « 1984 » et posant l'entreprise en rempart contre une future société de surveillance[6]. Tout comme le slogan interne de Google, « *Don't be evil* » (« Ne soyez pas malveillants »), la posture prise par Apple n'est finalement qu'une sinistre anti-prophétie : l'entreprise jouera bien un rôle décisif dans la transformation des outils numériques en moyens d'enfermement et de contrôle. Aujourd'hui, environ un smartphone sur cinq vendu dans le monde est un iPhone et le chiffre d'affaires annuel de l'entreprise (350 milliards d'euros) est supérieur au budget annuel de l'État français.

Facebook a été créé en 2004, notamment par Mark Zuckerberg, son actuel directeur général. Son chiffre d'affaires de 118 milliards de dollars en 2021 repose à 97 % sur la publicité, affichée à 2,9 milliards d'utilisateurs actifs mensuels sur la plateforme. L'entreprise détient également WhatsApp et Messenger (services de messagerie), ainsi qu'Instagram (réseau de partage de photos et de vidéos), qui lui apportent 3,6 milliards d'utilisateurs actifs mensuels. Un conglomérat regroupant toutes ces entités a été créé fin 2021 : Meta, l'équivalent de l'Alphabet de Google. L'entreprise explique sans pudeur son fonctionnement : des personnes qui souhaitent diffuser un message (une publicité, un article, un événement, etc.) désignent à Facebook un public cible, selon certains critères sociaux, économiques ou comportementaux, et paient l'entreprise pour qu'elle diffuse ce message à ce public, dans les meilleures conditions. Ce fonctionnement implique deux choses : connaître chaque utilisateur, puis afficher les messages devant être diffusés au bon moment et sous le bon format, pour influencer au mieux les personnes ciblées.

Créée par Jeff Bezos en 1994, Amazon est une entreprise de commerce en ligne. Alors qu'elle vendait initialement des livres à distance, on trouve aujourd'hui sur sa plateforme MarketPlace toutes sortes de produits, du culturel à l'alimentaire. Elle a racheté au fil des années des entreprises dans des secteurs variés, pour développer ses propres gammes. Parmi ses services, citons Prime Video (plateforme de streaming), Kindle (liseuse), Amazon Web Services (AWS – services d'infrastructure informatique), Amazon Mechanical Turk (AMT – plateforme de micro-travail), Amazon Halo (bracelet connecté qui analyse l'activité physique et les émotions), Amazon Care (télémédecine et télépharmacie), Ring (caméras et sonnettes de portes connectées), Amazon Key (déverrouillage de porte à distance, qui préoccupe depuis des failles démontrées par des recherches en cybersécurité), Amazon Pay (paiements dématérialisés), Amazon Go (supermarchés), Amazon Studio (production vidéo), Alexa, Astro, IMDb, Twitch… En 2021, Amazon génère 470 milliards de dollars de revenus, dont presque 10 sont issus de la publicité.

Enfin, Microsoft Corporation est une multinationale informatique, fondée en 1975 par Bill Gates et Paul Allen. Elle développe des systèmes d'exploitation (MS DOS, puis Windows), des logiciels (MS Office, Azure), du matériel informatique (les consoles Xbox, la tablette Surface, le smartphone Lumia, la montre connectée Band, le casque VR HoloLens…) et des sites Internet comme le portail MSN ou le moteur de recherche Bing. Au cours de l'année 2020-2021, Microsoft génère 168 milliards de dollars de revenus, dont 10 milliards viennent de LinkedIn, le réseau social aux 774 millions de comptes utilisateurs, racheté en 2016. C'est celui-ci qui nous intéresse ici. La publicité représente 10 % des revenus du réseau social et affiche une croissance annuelle de 97 %.

Ces chiffres vous font tourner la tête ? Nous aussi. D'autant plus quand on sait que ces entreprises dépensent chaque année (au moins) 4 millions d'euros cumulés pour leurs activités de lobbying, rien qu'en France[7]. Treize fois le budget annuel de la Quadrature !

LA COLLECTE DES DONNÉES SANS CONSENTEMENT LIBRE

Les GAFAM obligent leurs utilisateurs à accepter des « règles » ou « engagements » de confidentialité pour utiliser leurs services. Celles-ci prévoient que les entreprises peuvent collecter un certain nombre de données, dont :

- les classiques – nom, photo, adresse e-mail et numéro de téléphone des utilisateurs ;
- des informations sur l'utilisation des services : contenus consultés et interactions avec ceux-ci, historique de navigation, requêtes de recherches, contenus des conversations (Messenger, Gmail ou encore Instagram) ;
- des « métadonnées » (des données à propos des données) dont les informations des personnes contactées, la durée des appels, la localisation des appareils (définie à partir de l'adresse IP, de signaux GPS, des points d'accès wifi et des antennes-relais téléphoniques à proximité…), les cookies présents sur l'appareil… ;
- mais aussi parfois le flux des caméras ou des micros qu'embarquent les smartphones !

Notons qu'Apple fait référence à des données « non personnelles » au motif qu'elles seraient traitées indépendamment de l'adresse IP, ce qui révèle que la définition des « données personnelles » retenue par l'entreprise est bien différente de celle du droit européen. En droit européen, une information est une donnée personnelle dès lors qu'elle peut être associée à une personne unique, peu importe que l'identité de cette personne soit connue ou non. Or, l'identifiant unique de l'appareil, ou, dans bien des cas, les recherches effectuées ou la localisation sont bien associables à une personne unique.

Chacun des GAFAM explique qu'il utilise toutes ces données pour « améliorer le service » (ou le personnaliser) : mieux cibler ses utilisateurs, afin de leur proposer les publicités adaptées au bon moment. L'analyse en masse d'informations en apparence anodines permet d'établir des corrélations censées cerner en détail l'intimité de chaque personne. L'accès aux services implique l'obligation de céder nos informations personnelles à ces fins. Or, le RGPD prévoit que notre consentement n'est pas valide (car non libre) « si l'exécution d'un contrat, y compris la fourniture d'un service, est subordonnée au consentement au traitement de données à caractère personnel qui n'est pas nécessaire à l'exécution dudit contrat[8] »[9].

La collecte et l'analyse de nos données par les GAFAM sont illicites sur la base du RGPD. C'est ce que nous attaquons.

Pour faire bonne figure, la plupart des GAFAM donnent l'illusion que nous pouvons limiter l'interconnexion de certains types de données brutes, mais ce prétendu « contrôle » est tout à fait factice. Qui a déjà activé les options limitant la collecte de données personnelles par Google ? Qui a déjà désactivé l'identifiant unique de son appareil Apple en lui donnant la valeur « 0 » (et qui sait comment le faire ?) ? Le consentement est dérobé. Sans compter qu'il ne laisse aucun choix sur tous les autres types de données, et surtout qu'il ne bloque pas l'analyse faite sur les données dérivées (nos profils), qui sont pourtant les plus sensibles.

Heureusement, le RGPD a parfaitement anticipé cette tentative de contourner notre volonté. Il prévoit précisément que, pour être « valide », notre consentement doit être explicite, par un acte positif dont le seul but est d'accepter l'accès aux données : « Il ne saurait dès lors y avoir de consentement en cas de silence, de cases cochées par défaut ou d'inactivité » (considérant 32). Or, les mesures de surveillance sur lesquelles les GAFAM feignent de nous laisser la main sont « acceptées » par défaut au moyen de cases pré-cochées ou pré-installées sur nos appareils. Elles sont donc totalement illicites au regard du RGPD. Nous l'attaquons aussi.

De la même manière, la directive ePrivacy exige le consentement de l'utilisateur pour accéder aux informations contenues sur sa machine. Si l'utilisateur refuse l'installation de certains logiciels ou la génération d'un identifiant unique lié à sa machine, il devrait pouvoir terminer l'installation et utiliser librement l'appareil. C'est ce que nous exigeons collectivement devant la CNIL.

LES MÉGA-COOKIES GOOGLE ET FACEBOOK : PISTER, INFLUENCER

Google Network est un entremetteur publicitaire, qui met en relation des annonceurs avec « plus de deux millions » de sites ou de blogs tiers qui souhaitent se rémunérer par la publicité. Sur chacun de ces sites, c'est Google qui affiche techniquement chaque publicité, qui lui permet de déposer les cookies et autres pisteurs grâce auxquels il peut retracer la navigation de tout internaute, inscrit ou non à ses services. Ici encore, nous n'avons jamais consenti de façon active à ce pistage.

De la même façon, Google nous piste sur les innombrables sites qui ont recours au service Google Analytics, ce service qui aide les sites à analyser l'identité de leurs visiteurs, tout en laissant Google accéder aux mêmes informations. Une simple analyse de trafic sur lemonde.fr, lefigaro.fr, hadopi.fr ou defense.gouv.fr permet par exemple de constater l'envoi de requêtes à doubleclick.net (la régie publicitaire de Google) et/ou à google-analytics.com. Les responsables de ces sites sont tout aussi responsables que Google de ce pistage illégal, par lequel le géant publicitaire peut précisément nous ficher.

Enfin, Google compte bien étendre sa présence sur l'ensemble du Web en régulant lui-même la publicité : en configurant son navigateur Google Chrome (utilisé par 60 % des internautes) pour qu'il bloque partout sur le Web les publicités qui ne correspondent pas aux critères (de format, d'ergonomie…) décidés par l'entreprise. Le message est ainsi clair : « Si vous voulez faire de la publicité en ligne, utilisez les services Google, vous vous éviterez bien des soucis ! »

D'une pierre trois coups, Google passe pour un défenseur de la vie privée (puisqu'il bloque certaines publicités intrusives), invite les internautes à désactiver les bloqueurs tiers (tel que uBlock Origin qui neutralise efficacement nombre de traceurs dont ceux de Google) puisque Google Chrome en intègre un par défaut, et incite enfin encore plus

d'éditeurs de pages Web à afficher *ses* publicités, donc à intégrer *ses* traceurs, partout, tout le temps.

Quant à Facebook, le groupe ne cache plus son activité de traçage un peu partout sur le Web, même s'agissant de personnes n'ayant pas de compte Facebook (qui se voient alors créer un « profil fantôme[10] »). Les méthodes de pistage sont nombreuses : cookies, boutons « J'aime » ou « Partager » affichés sur de nombreux sites (qui remontent automatiquement à Facebook les adresses IP et les informations sur la configuration de l'utilisateur avec l'URL de la page visitée), pixels invisibles (images transparentes de 1x1 pixel fonctionnant comme les boutons et transmettant à Facebook les informations de connexion), Facebook Login (utilisé par certains sites ou applications comme outil pour authentifier leurs utilisateurs).

Les personnes ciblées sont rarement ou ne sont jamais informées et leur consentement n'est pas obtenu. Facebook se dédouane de cette responsabilité en la faisant peser sur les sites et les applications ayant intégré ses traceurs. Bien que ces derniers soient responsables juridiquement, Facebook l'est tout autant, l'entreprise étant régulièrement condamnée (par la CNIL française, espagnole et irlandaise ou encore la justice belge) pour ce pistage illicite, sans pour autant y mettre un terme[11].

Et sur mobile ? Google mène le développement d'Android, le système d'exploitation pour smartphones. L'entreprise offre par ailleurs des outils pour aider les développeurs à créer des applications mobiles pour Android, permettant par exemple de facilement connaître son nombre d'utilisateurs. Facebook fournit également une série d'outils aux développeurs d'applications. Dès qu'une application veut se connecter à Facebook, pour une raison ou une autre, un certain nombre de données personnelles sont transmises, souvent sans lien direct avec le but initial de l'application et, trop souvent, sans que l'utilisateur n'en soit même informé.

L'association Exodus Privacy a mis en évidence l'omniprésence de ces traqueurs. Le travail de ses infatigables bénévoles a relevé la présence

de pisteurs (AdMob, Analytics, ou DoubleClick pour Google, Ads, Analytics ou encore Login pour Facebook) dans plus de trois mille applications analysées, dont Deezer, Spotify, Uber, Tinder, Twitter, *Le Figaro*, *L'Équipe*, Crédit agricole, Boursorama ou Angry Birds. Ainsi, nous avons pu observer que l'application de suivi de grossesse Pregnancy + récolte les informations privées de l'enfant à naître (afin d'accompagner les parents dans la naissance) et les transmet à Facebook (semaine de grossesse et mois de naissance attendu). Grâce à Pregnancy +, votre enfant a déjà son compte Facebook avant même d'être né !

Autre exemple flagrant : en analysant les données émises par l'application_Diabetes:M, on constate qu'elle envoie à Facebook l'« advertising ID » de l'utilisateur, donnant ainsi à l'entreprise une liste de personnes atteintes de diabète. Sur son site, l'application se contente d'expliquer travailler avec des réseaux publicitaires, sans autre détail…

Sous couvert de mettre à disposition des outils pour faciliter la vie des développeurs, comme les divers *analytics*, les outils de surveillance de Google, Facebook et Apple sont intégrés à des milliers d'applis. Ces services – qui ne sont ni plus ni moins qu'un droit d'accès à un fragment de la surveillance de Google ou Facebook – sont gracieusement offerts aux entreprises tierces à l'origine de la pléthore d'applications qui rendent ces plateformes si populaires, afin d'attirer le plus grand nombre d'applications et donc d'utilisateurs sur leurs plateformes.

Côté Apple, ces entreprises tierces sont d'autant plus incitées à venir sur l'App Store depuis qu'Apple les empêche de recourir aux juteux « cookies tiers » sur le Web – le navigateur Safari les bloquant par défaut. La protection offerte par Safari apparaît dès lors sous des traits biens cyniques : viser l'App Store permet de recourir à bien plus de techniques de pistage.

Côté Google, en plus du système Android, l'entreprise impose aux constructeurs de smartphones partenaires d'embarquer sur leurs produits les fameux mouchards que sont ses applications. Et si Android est sous licence libre, il dépend très lourdement de composants et services propres à Google pour être en mesure d'offrir l'expérience qu'en attendent ses

utilisateurs. Ces services étendent les possibilités du système et deviennent souvent indispensables pour faire pleinement fonctionner un grand nombre d'applications, permettant à l'entreprise de traquer les utilisateurs de smartphones : la géolocalisation continue permet de connaître les habitudes de déplacement ; la liste des réseaux wifi est envoyée à Google quand bien même l'utilisateur a désactivé le wifi de son téléphone ; l'utilisation du Play Store (magasin d'applications) impose de connecter son appareil à son compte Google, permettant le recoupage des données.

Enfin, sur Android comme sur iOS, Google et Apple associent à chaque appareil un identifiant unique à des fins publicitaires, librement accessible par chaque application installée. Cet identifiant, encore plus efficace qu'un simple « cookie », permet d'individualiser chaque utilisateur et, ainsi, de retracer parfaitement ses activités sur l'ensemble de ses applications. Un outil décisif pour nous soumettre la bonne publicité au bon moment.

LES MULTIPLES DANGERS DU PROFILAGE

La majorité des données analysées ne sont pas celles que l'on publie spontanément, mais celles qui ressortent de nos activités et qui sont primordiales aux GAFAM pour nous « cibler » : l'ensemble des caractéristiques sociales, économiques et comportementales associées à chaque utilisateur.

En 2013, l'université de Cambridge a conduit l'étude suivante : 58 000 personnes ont répondu à un test de personnalité, puis ce test a été recoupé à tous leurs « j'aime » laissés sur Facebook. En repartant de leurs seuls « j'aime », l'université a ensuite pu estimer leur couleur de peau (avec 95 % de justesse), leur orientation politique (85 %) et leurs préférences sexuelles (88 %), leur confession religieuse (82 %), s'ils fumaient (73 %), buvaient (70 %) ou consommaient de la drogue (65 %)[12].

Cette démonstration a permis de mettre en lumière le fonctionnement profond de l'analyse de masse : quand beaucoup d'informations peuvent être recoupées sur un très grand nombre de personnes (plus de 2 milliards pour Facebook, rappelons-le), de très nombreuses corrélations apparaissent, donnant l'espoir, fondé ou non, de révéler le détail de la personnalité de chaque individu.

Aujourd'hui, Michal Kosinski, le chercheur ayant dirigé cette étude, continue de dénoncer les dangers de l'analyse de masse automatisée : il explique qu'à cause de cela de simples photos pourraient révéler l'orientation sexuelle d'une personne, ses opinions politiques, son QI ou ses prédispositions criminelles. Qu'importe la pertinence des corrélations résultant de telles analyses, c'est bien cette méthode qui a été à la source du fonctionnement de Cambridge Analytica, dont les conséquences politiques sont, elles, bien certaines.

Une fois que l'entreprise s'est fait une idée si précise de qui nous sommes, de nos envies, de nos craintes, de notre mode de vie et de nos faiblesses, la voie est libre pour nous proposer ses messages au bon moment et sous le bon format, quand ils sont les plus à même d'influencer notre volonté.

Le groupe Facebook s'est lui-même vanté de l'ampleur de cette emprise. En 2012, il a soumis 700 000 utilisateurs à une expérience, sans leur demander leur consentement ni les en informer. Pendant une semaine, la plateforme a manipulé leur fil d'actualité en cachant certains éléments, dans le but d'influencer leur humeur (rendre certaines personnes plus joyeuses, d'autres plus tristes). L'étude a conclu que « les utilisateurs ciblés commençaient à utiliser davantage de mots négatifs ou positifs selon la nature des contenus auxquels ils avaient été "exposés" ». Cette expérience n'a fait que révéler le fonctionnement normal des réseaux sociaux : afin de nous influencer, ils hiérarchisent les informations que nous pouvons consulter sur ces services.

Prenons l'exemple d'un autre réseau social. La plus grosse plateforme vidéo d'Internet (et le deuxième site le plus visité au monde), YouTube, qui appartient à Google. Elle ne se contente pas d'héberger des vidéos : il

s'agit d'un véritable réseau social de contenus multimédias, qui met en relation des individus et régule ces relations.

En effet, lorsqu'une vidéo est visionnée sur YouTube, dans 70 % des cas, l'utilisateur a été amené à cliquer sur cette vidéo via l'algorithme de recommandation du site[13]. Un ancien employé de YouTube, Guillaume Chaslot, expose les conséquences de cet algorithme, dont le but est de faire en sorte que l'utilisateur reste le plus longtemps possible sur la plateforme, devant les publicités[14]. L'employé raconte que lors de la mise en ligne d'une vidéo, celle-ci est d'abord montrée à un échantillon d'utilisateurs du site et n'est recommandée aux autres utilisateurs que si elle a retenu cet échantillon de spectateurs suffisamment longtemps devant l'écran.

Cet algorithme ne se pose pas la question du contenu de la vidéo – de sa nature, de son message… En pratique, cependant, les vidéos les plus mises en avant se trouvent être les plus incendiaires, choquantes, diffamantes ou complotistes. Guillaume Chaslot compare : « C'est comme une bagarre dans la rue, les gens s'arrêtent pour regarder. » De fait, on comprend que de nombreux créateurs de vidéos, qui plus est ceux qui cherchent à en tirer profit, proposent des vidéos de plus en plus agressives.

Dans le but de maximiser les vues, YouTube surveille donc les moindres faits et gestes des utilisateurs afin de les mettre dans les conditions les plus propices à recevoir de la publicité et de les exposer à cette publicité le plus longtemps possible… mais ce n'est pas tout ! YouTube, désirant ne pas perdre une seconde de visionnage de ses utilisateurs, ne prend pas le risque de leur recommander des contenus trop différents et se complaît à les maintenir dans leur « zone de confort » – une pratique confirmée par Guillaume Chaslot. Dans ces conditions, le débat public est entièrement déformé, les discussions les plus subtiles ou précises, jugées peu rentables, s'exposant à une censure par enterrement.

Cette hiérarchisation de l'information ne se contente pas d'écraser notre liberté de conscience personnelle : elle a aussi pour effet de distordre entièrement le débat public, selon des critères purement

économiques et opaques – pour preuve, la surdiffusion de *fake news*, qui n'en est qu'un des nombreux symptômes.

Dans son étude annuelle de 2017, le Conseil d'État lui-même mettait en garde contre la prétendue neutralité des algorithmes dans la mise en œuvre du tri : les algorithmes sont au service de la maximisation du profit des plateformes et sont dès lors conçus pour favoriser les revenus au détriment de la qualité de l'information.

LES SOLUTIONS LIBRES À UN MODÈLE ÉCONOMIQUE DÉPASSÉ

Le modèle économique fondé sur le ciblage publicitaire est en train d'être drastiquement remis en cause. Il n'est plus permis de rémunérer un service en contrepartie de libertés fondamentales. Facebook ne va pas forcément disparaître, mais ne pourra plus continuer à gagner de l'argent de la même façon.

Il existe déjà de nombreuses solutions de remplacement aux services des GAFAM qui sont réellement gratuites (c'est-à-dire qui n'impliquent pas de « monnayer » nos libertés). Leur financement repose sur le modèle originel d'Internet : la décentralisation, qui permet la mutualisation des coûts en stockage, en calcul et en bande passante.

Par exemple, La Quadrature du Net fournit à plus de 9 000 personnes l'accès au réseau social Mastodon, une sorte de Twitter libre et décentralisé, sur Mamot.fr, qui n'est qu'un des milliers de nœuds du réseau social, chaque nœud étant interconnecté avec les autres. Cela permet de répartir les coûts entre de très nombreux acteurs qui peuvent ainsi plus facilement les supporter, sans avoir à se financer par la pub (donc par la surveillance de masse) mais en opérant plutôt de façon transparente auprès de leurs utilisateurs.

De la même manière, contrairement à ce que Google (ou TikTok) tente de nous faire croire, la surveillance et la censure ne sont pas les conditions inévitables du partage de vidéos en ligne. On peut parfaitement le faire en respectant nos droits. PeerTube par exemple est

une plateforme de partage de vidéos similaire à YouTube mais avec une approche fondamentalement différente : les vidéos ne sont pas toutes hébergées au même endroit. N'importe qui peut créer son instance PeerTube et les héberger chez lui, qu'il soit un particulier ou une entreprise. Les différentes instances sont ensuite connectées entre elles. Chacune a ses propres règles, il n'y a pas de politique de censure unifiée comme sur YouTube, et surtout ces règles ne sont pas forcément dictées par une logique commerciale.

Permettre l'essor de ces nouveaux réseaux est bien l'objectif final de nos actions, mais pour y parvenir il est nécessaire que chacun et chacune puisse se libérer de l'emprise des GAFAM. Ce faisant, nous pourrons construire l'internet de nos rêves : libre, émancipateur et décentralisé.

ET LES PLAINTES DANS TOUT ÇA ?

Le 28 mai 2018, la Quadrature dépose auprès de la CNIL les cinq plaintes collectives. La CNIL transfère immédiatement celle visant Amazon au Luxembourg, et celles établies contre Microsoft, Apple et Facebook en Irlande, où ces entreprises ont leurs sièges sociaux respectifs. Or la Data Protection Commission (DPC), équivalent irlandais de la CNIL, est de notoriété publique en sous-effectif et débordée. Installer leur siège en Irlande permet donc aux entreprises de faire traîner les procédures judiciaires à leur encontre depuis des années. À ce jour, près de quatre ans plus tard, nous sommes toujours sans nouvelles des plaintes contre Microsoft, Apple et Facebook.

Pour ce qui est de Google, la CNIL commence par s'attaquer aux pratiques de l'entreprise concernant Android. Le 21 janvier 2019, elle prononce une sanction contre Google qui fait un certain bruit : une amende à hauteur de 50 millions d'euros, considérant que le ciblage publicitaire qu'il réalise sur son système d'exploitation Android n'est pas conforme au RGPD[15]. Cette sanction n'est qu'une toute première partie de la réponse à notre plainte, qui dénonçait surtout le ciblage publicitaire

imposé sur YouTube, Gmail et Google Search en violation de notre consentement, à laquelle s'ajoutait une autre plainte déposée elle aussi devant la CNIL par nos amis de l'association autrichienne NOYB (l'organisation de Max Schrems) contre Android[16].

50 millions d'euros : un montant « record » et néanmoins très faible en comparaison du chiffre d'affaires annuel de l'entreprise. La CNIL s'est limitée aux « traitements couverts par la politique de confidentialité présentée à l'utilisateur lors de la création de son compte à l'occasion de la configuration de son téléphone mobile sous Android » et a délégué le reste de notre plainte, au sujet de YouTube, Gmail et Google Search à l'APD irlandaise. En effet, Google avait, peu de temps après notre plainte, déménagé son siège en Irlande, pour bénéficier des longs délais de procédure. Or depuis, la DPC a constaté que, bien que l'entreprise ait un siège en Irlande, elle ne possède aucune autorité décisionnaire en Europe, celle-ci demeure aux États-Unis. En conséquence, elle s'estime non compétente et renvoie, en 2021, la plainte devant la CNIL française. En réaction, cette dernière a déposé une requête auprès du Comité européen pour la protection des données (CEPD) afin d'obtenir une décision contraignante quant à qui doit juger la plainte. Ce jeu de ping-pong dure depuis maintenant près de quatre ans, au cours desquels la plainte n'a même pas commencé à être examinée. Mais ce faisant, la CNIL se protège par anticipation, en demandant au CEPD de confirmer sa compétence pour juger l'affaire. C'est en effet un des arguments majeurs de la défense de Google, qui menace de faire retoquer une éventuelle sanction de la CNIL au prétexte de sa non-compétence, ce qui serait un désaveu politique énorme pour l'autorité française.

Sur le continent européen, une autre autorité que la CNIL travaille en silence. Le 16 juillet 2021, l'autorité luxembourgeoise de protection des données personnelles, la Commission nationale pour la protection des données (CNPD), s'est prononcée sur notre plainte collective appuyée par 10 000 personnes contre Amazon.

Après trois ans de silence absolu, c'est l'agence de presse Bloomberg, qui remarque, dans le *SEC filing* (déclaration fiscale américaine annuelle)

d'Amazon, un trou de plusieurs centaines de millions d'euros. En creusant, les journalistes remontent la piste de la plainte de la Quadrature, et quelques mois plus tard, la CNIL confirmera qu'ils avaient vu juste[17].

La décision semble sans ambiguïté : le système de ciblage publicitaire imposé par Amazon est réalisé sans notre consentement libre, en violation du RGPD[18]. L'entreprise est condamnée à une amende de 746 millions d'euros. Il s'agit du record européen en matière d'amendes prononcées contre une violation du RGPD. Cette sanction historique frappe au cœur du système de prédation des GAFAM. Elle rend encore plus flagrante la démission généralisée de l'autorité irlandaise de protection des données qui, en trois ans, n'a été capable de clore aucune des quatre autres plaintes que nous avions engagées contre Facebook, Apple, Microsoft et Google.

La posture exemplaire de l'autorité luxembourgeoise contraste avec la situation de la CNIL en France qui, pendant longtemps, faisait, en Europe, figure de tête de file pour la protection des données. En 2021, elle n'est plus que l'ombre d'elle-même, alors que nos plaintes collectives, initialement introduites devant elle, lui offraient l'occasion idéale d'être le fer de lance du RGPD contre les violations systémiques des données personnelles au cœur du modèle économique des GAFAM.

L'autorité luxembourgeoise, dans sa décision, reconnaît qu'Amazon nous cible bien à des fins publicitaires sans base légale et contrevient donc au RGPD. Mieux : Amazon a six mois pour corriger, c'est-à-dire mettre fin au ciblage publicitaire ou obtenir notre consentement libre pour ce faire, sans quoi il devra payer une astreinte de 746 000 euros par jour de retard[19]. C'est exactement le genre de décision que nous attendions ! Car avec des chiffres d'affaires colossaux rendus possibles par des violations permanentes du droit, ces entreprises peuvent se permettre de payer une amende de temps en temps, tout en continuant de générer des profits colossaux. L'astreinte est une manière efficace de maintenir une pression permanente sur les dirigeants et d'orienter leurs décisions dans le sens attendu.

Nos combats collectifs pour forcer les GAFAM à respecter le RGPD sont un travail de longue haleine et nécessitent la collaboration de toutes les autorités compétentes. Bien que les choses bougent lentement, c'est sans doute un des domaines où il est raisonnable de faire preuve d'un certain optimisme.

UN ESPOIR : L'INTEROPÉRABILITÉ

Nous poussions l'idée, dès 2018, qu'au lieu de combattre le mal par le mal en incitant les plateformes à la censure (sans même prendre en compte leur fonctionnement économique), il fallait contraindre celles-ci à être *interopérables* avec d'autres plateformes et à respecter la réglementation sur les données personnelles (qui freinerait leur influence néfaste sur les débats). Les géants du Web distordent nos échanges humains pour des raisons économiques en favorisant les propos anxiogènes, caricaturaux, violents ou payés… au détriment des autres. Il faut créer un statut juridique spécifique pour les encadrer, et leur imposer de renoncer à leur pouvoir de contrainte (et donc redevenir de simples hébergeurs) ou de devenir neutres. S'ils souhaitent conserver ce pouvoir, alors ils doivent devenir « interopérables » et implémenter un standard de communication ouvert, partagé avec d'autres services. Nous pourrons ainsi, sans avoir de compte chez Facebook, communiquer avec nos amis qui y sont inscrits.

En somme, soit la plateforme s'interdit les profitables hiérarchisations des contenus et de la censure privée, soit elle devient interopérable et permet à d'autres plateformes d'interagir de manière complète avec ses utilisateurs.

Mais n'oublions pas que ces entreprises sont principalement financées par la publicité. Ce « péché originel du Web », apparu en 1994 avec une simple bannière statique, s'est très vite retrouvé au cœur même du financement de l'information et du modèle économique des entreprises de la « nouvelle économie » en ligne. Comme une normalité,

comme s'il n'y avait pas d'autres solutions. La publicité des premiers jours, affichage statique et permanent, s'est heurtée à une vision néolibérale imposant une rentabilité toujours plus importante. Et ses promoteurs se sont vite aperçus qu'ils pourraient en tirer davantage de bénéfices si les messages promotionnels s'adressaient à des consommateurs potentiels triés : dès 2003, un brevet déposé par les équipes de Google prévoyait de « générer des informations utilisateurs à des fins de publicité ciblée ». C'est le début du capitalisme de surveillance.

Pour optimiser encore le processus de vente, l'idée est de personnaliser des techniques de manipulation permettant de modifier le comportement des individus qui lui sont soumis. Car non contents d'influencer nos comportements de plus en plus efficacement dans le seul dessein de nous afficher des réclames permettant de nous vendre des biens et services, Big Data et ses capacités supposément incroyables tentent des gouvernements peu démocratiques, comme la France : Gérald Darmanin posait ainsi la question, en mai 2021 : pourquoi l'État ne pourrait-il pas accéder à cette gigantesque quantité d'informations et à l'analyse algorithmique allant avec si les GAFAM, eux, y ont accès[20] ? Peut-être parce que c'est illégal et que lesdits GAFAM se font condamner les uns après les autres ? Mais ne leur donnons pas trop d'idées, en plus de coopter le secteur privé, ils sont souvent bien vite prêts à changer la loi et la Constitution pour se laisser les coudées franches.

Cette idéologie visant à considérer que ses concitoyens peuvent et devraient se soumettre à une surveillance totale et permanente est finalement un continuum, allant des caméras dans les rues à la surveillance algorithmique de Facebook, l'un alimentant l'autre et vice-versa. Avec pour étape suivante de mettre des algorithmes dans les caméras.

PARTIE : L'ÈRE DE LA TECHNOPOLICE - (-)

1. NAISSANCE DE LA TECHNOPOLICE

En mars 2021, la Quadrature publie un article sur les caméras de surveillance « intelligentes », mais illégales, installées devant la gendarmerie de Moirans, une petite commune de l'Isère[1]. Quelques semaines plus tôt, en décembre 2020, le Conseil d'État interdisait, à notre demande, les drones utilisés par la préfecture de police de Paris pour surveiller les manifestations dans les rues de la capitale – après une première interdiction en mai 2020, royalement ignorée par le préfet Didier Lallement[2].

Si l'un de nous, militant de l'association, s'était endormi au beau milieu de l'été 2009, juste après la lutte contre la loi Hadopi, pour se réveiller au printemps 2021, un peu ébouriffé et la langue sèche, il se serait sans doute posé deux questions : « Pourquoi cette grosse sieste de douze ans ? Et pourquoi La Quadrature du Net a-t-elle autant changé ? »

En ce qui concerne l'hypersomnie, nous n'avons pas de réponse. En revanche, nous pouvons comprendre son étonnement quant au positionnement de la Quadrature : comment l'association connue pour sa défense du partage et de la neutralité du Net, ou pour sa lutte contre l'exploitation commerciale des données personnelles, se retrouve-t-elle à compter les caméras de surveillance dans la rue et à contester les ordres d'un préfet de police ?

C'est l'histoire d'une modification lente, patiente comme l'évolution des espèces, et longue comme une prise de conscience. Pendant douze années, la société a changé, et nous avec elle ; si vous avez lu les pages

précédentes, vous le savez déjà. Prétendre s'engager pour « la défense des libertés à l'ère du numérique », alors que le numérique envahit tous les aspects de la vie quotidienne, c'est fatalement sortir d'Internet et embrasser tous les aspects de la société moderne. Reste à savoir comment on est passé de la lutte contre la censure administrative du Web, légalisée par la loi Renseignement (en 2015), à la dénonciation directe d'un système de surveillance installé dans les rues d'une petite ville de l'Isère (en 2021).

Raconter cette histoire, c'est remonter aux origines de la campagne Technopolice, lancée en septembre 2019.

LE FANTASME DE TOUT SAVOIR POUR TOUT GOUVERNER

Quand on cherche à reconstituer le cours des événements a posteriori, on risque de fixer des moments de bascule un peu artificiels. Comment retrouver la première formulation d'une idée ? Puisqu'on ne peut pas faire l'archéologie des pensées dans les têtes, qui ne se fossilisent pas bien, il faut se résigner à en chercher les premières traces écrites : les dates de publication serviront de date de naissance, alors que les idées ont mûri lentement avant d'oser s'exprimer.

Dans le cas de la campagne Technopolice, les historiens ont de la chance : les témoins de sa naissance sont bien vivants et plutôt bavards, et ils se souviennent distinctement de l'enchaînement des faits. Félix Tréguer, membre fondateur de la Quadrature qu'il a même présidée durant deux ans (de 2017 à 2019), est formel : l'origine de la campagne Technopolice se situe le 8 décembre 2017.

Ce jour-là, le journal *Le Monde* publie un article de la journaliste Claire Legros, intitulé : « À Marseille, le Big Data au service de la sécurité dans la ville[3] ». L'article cristallise de manière saisissante un très vieux fantasme politique : si la police sait tout, elle pourra mieux garantir la sécurité des rues. Et de façon plus large, si on connaissait mieux le

fonctionnement de la société, avec suffisamment de « données », alors la diriger deviendrait évident, et ne serait plus qu'une question de réglages.

On peut remonter le fil de cette ambition-là très loin dans le temps, jusqu'aux Lumières et peut-être avant, avec la découverte de la permanence des lois physiques, qui rend les causes calculables et les conséquences prévisibles. Le Dieu imaginé par le philosophe Leibniz, par exemple, est omniscient, et sa connaissance intime des innombrables déterminations, jusqu'aux plus petites, lui permet de connaître l'avenir aussi clairement que s'il avait déjà eu lieu. Un gouvernant qui aurait ce pouvoir pourrait à la fois satisfaire les aspirations véritables de ses sujets et se prémunir contre les révoltes, même les plus individuelles.

Le fantasme est ravivé par l'apparition des études statistiques, qui donnent naissance à l'économétrie et à la sociologie au XIX^e^ siècle : au-delà des comportements individuels, il existe des faits de masse que l'on peut mesurer, que l'on peut chiffrer à l'échelle de la société, et qui sont autant de possibles explications causales à des comportements majoritaires. Le travail du sociologue Émile Durkheim sur le suicide[4] est à ce titre souvent cité comme un acte fondateur de la science sociale, qui cherche dans les phénomènes décelables dans le grand nombre un éclairage sur les comportements apparemment erratiques des individus. On voit pourquoi le pouvoir politique veut acquérir ce savoir : si l'on isole les lois qui déterminent les personnes, alors on doit pouvoir prédire leur comportement et, pourquoi pas, l'orienter, le manipuler, le diriger.

Au XX^e^ siècle, la direction des masses a été confiée au cinéma, à la radio et à la propagande, selon des méthodes explicitées par exemple dans les ouvrages du propagandiste austro-américain Edward Bernays, parmi lesquels *Cristallisation de l'opinion publique* (1923) ou *Propagande* (1928). Le développement de la publicité, après la Seconde Guerre mondiale, a affiné l'analyse de la psychologie des foules, moins pour satisfaire ses attentes que pour les créer de toutes pièces. On est passé en quelques décennies de la réclame au marketing.

La compréhension du fonctionnement des « systèmes complexes » – une société humaine, une population animale, un cerveau, une

psychologie – et de la façon dont des machines pourraient imiter des comportements animaux pour devenir plus efficaces devient après la Seconde Guerre mondiale un champ d'étude à part entière, sous l'impulsion de penseurs comme Norbert Wiener, et reçoit le nom de *cybernétique*, ou « technique du contrôle ». Ces travaux aboutissent à la mise au point de concepts formels comme la « boucle de rétroaction » (ou *feedback*), utilisée dans des domaines aussi variés que la biologie, la psychologie, la mécanique, l'économie, etc. Cet exercice d'abstraction qui cherche des régularités ou des similitudes dans des domaines très distants les uns des autres établit un fort parallélisme entre le vivant et le mécanique, et entretient de manière explicite le fantasme d'un « pilotage » du vivant, à l'échelle d'un individu ou d'une société entière. L'idée s'est tellement bien implantée dans l'imaginaire collectif que la culture pop se l'est appropriée : le cinéma appelle les robots androïdes des *cyborgs*, un courant de la SF se baptise *cyberpunk*, et John Perry Barlow mentionne Internet par le beau nom de *cyberespace*[5].

Maintenant que toutes nos activités quotidiennes produisent des « données » numériques – nos déplacements, nos achats, nos discussions sur les réseaux sociaux, nos rendez-vous médicaux, et même nos conversations téléphoniques intimes –, alors il devient techniquement plausible de connaître non seulement les activités de la population mais aussi ses pensées et ses désirs, dans l'ensemble et en détail. Avec une bonne analyse de cette énorme masse de données, on doit pouvoir lire l'âme humaine. Et si on n'y arrive pas encore, c'est forcément parce qu'on s'y prend mal : soit on ne calcule pas assez vite, soit on n'a pas assez de données. Il en faut donc encore plus, et toujours plus.

ALERTE EN PROVENANCE DE LA PLANÈTE MARSEILLE

On l'a vu, la prolifération des « traces numériques » dans nos vies profite d'abord aux publicitaires, ou plutôt aux sites Web capables de vendre aux publicitaires nos profils de consommateurs, avec la garantie que notre

attention est bien retenue sur leurs pages à longueur de journée – le fameux « temps de cerveau disponible[6] ». C'est à cette activité peu reluisante mais très lucrative que les célèbres GAFAM doivent leur immense fortune en totalité (Google, Facebook) ou en partie (Microsoft, Apple, Amazon). Mais les pouvoirs publics entendent bien, eux aussi, tirer profit du traitement de notre vie numérisée, et de l'immense savoir qu'elle renferme.

Le capitalisme gouverne notre économie et notre façon de travailler, de consommer et de vivre, la bourgeoisie capitaliste occupe les postes de gouvernement, rien d'étonnant à ce que la logique des entreprises se retrouve au sein des ministères, ou des grandes villes.

« L'analyse de données numériques peut-elle contribuer à prévenir les troubles à l'ordre public ? », s'interroge donc logiquement *Le Monde*, le 8 décembre 2017, avant de présenter le projet de la municipalité marseillaise : « Alors que de nombreuses collectivités en France misent sur les plateformes de données pour optimiser les déplacements et l'empreinte énergétique urbaine, la ville de Marseille annonce la création d'un outil d'analyse pour "garantir de manière plus efficace la sécurité et la tranquillité publique des citoyens". »

Après quoi l'article décrit en détail le fonctionnement idéal du premier « observatoire Big Data de la tranquillité publique » envisagé en France. C'est le nom choisi par la ville de Marseille pour désigner ce nouveau dispositif de surveillance, mais le costume de Mère-Grand cache mal les canines et les babines du loup.

L'article du *Monde* tombe malheureusement dans le panneau : les termes utilisés pour décrire le projet paraissent directement empruntés au discours valorisant des communiqués de presse et de la communication d'entreprise. On croit lire une plaquette publicitaire, là où on s'attend à une mise en perspective, à une mise en situation sociale et politique du projet municipal.

D'emblée, la « sécurité », terme rassurant mais sans contenu, cache la réalité des pratiques policières. Ni képi ni matraque dans le projet marseillais. Il s'agit de croiser innocemment des données, dans une

démarche à la pureté quasiment scientifique (un « observatoire »), de laquelle découlera naturellement la « tranquillité ». Si « la sécurité est la première des libertés[7] », alors la tranquillité peut bien devenir un service municipal à part entière.

L'article énumère quelques-unes des sources de données que le grand « outil Big Data de la tranquillité publique[8] » se propose d'agréger : « mains courantes de la police municipale, captations des caméras de surveillance, informations relevées par les marins-pompiers ou les agents des espaces verts… ». Il faut reconnaître que l'ambition du projet peut éblouir : « Au-delà de la collecte, l'outil développé par Engie Ineo vise à analyser ces informations et à les croiser avec d'autres données, comme celles des opérateurs de téléphonie mobile, de transport public, de l'AP-HM (Assistance publique-Hôpitaux de Marseille), pour "mieux anticiper les risques". "Nous allons également utiliser les données de météo et les grandes tendances des réseaux sociaux dans une finalité de sécurité", explique Caroline Pozmentier, adjointe au maire chargée de la sécurité publique, qui évoque un "Big Data de la tranquillité publique, premier pilier de la *smart city* marseillaise"[9]. »

La *smart city* : le mot est lâché.

GOUVERNER SUR UN ÉCRAN

La *smart city* est un projet général de gestion des villes au moyen des outils numériques. Elle suppose le fantasme cybernétique de la mise en données du monde. Les foules qui prennent les transports en commun, les automobilistes qui vont et viennent pour travailler ou faire des courses, les livraisons de marchandises, les ordures à collecter et à évacuer, les eaux propres et les eaux usées, le gaz et l'électricité, sont autant de flux qu'il est nécessaire de connaître pour les faciliter, les optimiser, ou au contraire les réduire, en tous les cas les contrôler. On voit que le vocabulaire qui gravite autour du mot « flux » n'est pas celui de la rêverie devant les vagues, ni d'une méditation métaphysique face au

cours toujours fuyant de la rivière (dans laquelle on ne se baigne jamais deux fois).

Ce sont des concepts et des mots de gestionnaires, de personnes soucieuses d'affecter au bon endroit et au bon moment des moyens humains et financiers toujours plus réduits. Les politiques publiques dépendent évidemment des finances publiques, dont on sait qu'elles sont soumises depuis une quarantaine d'années à une logique d'économie, d'appauvrissement, de réduction volontaire. Il s'agit donc d'être d'autant plus efficace.

Dans ce contexte général, les forces de police sont un flux à gérer comme les autres : on dispose de « ressources » limitées (les agents de la police municipale, les agents de la police nationale, des véhicules, des horaires de travail) et d'un volume de problèmes à « traiter » (des faits d'incivilité, de délinquance, de criminalité bien sûr, mais aussi des zones d'accidents de la route ou d'incendie à sécuriser, des événements publics festifs, sportifs ou militants, ou encore des sorties d'école à protéger le matin et le soir, etc.). Il est donc évident et nécessaire, pour tout gestionnaire municipal avisé, d'adapter ses ressources à ses besoins, et de savoir où et quand il doit disposer ses agents de police pour être efficace.

La *smart city* propose de répondre à cette question, et à toutes les autres du même genre, grâce aux « données ». Et pour obtenir des « données », il faut des sources de données. C'est-à-dire des capteurs de données.

Pour le traitement des ordures, ce sera la contenance volumique des camions de collecte, multipliée par le nombre de rotations et le nombre de camions. Pour les eaux propres, ce sera le volume indiqué par les compteurs. Pour les eaux sales, la capacité et le niveau de remplissage des bassins de collecte et de retraitement. Pour les flux d'automobiles, on posera des câbles de comptage aux points de convergence, où on comptera les véhicules minute par minute sur un enregistrement vidéo continu, etc. Mais la *city* n'aurait rien de *smart* si elle s'en tenait à ces moyens grossiers et à des « capteurs » aussi classiques. La *smart city* mesure tout, tout le temps, et pour cela elle doit multiplier les capteurs,

partout où c'est possible. Dans les immeubles, les portes auront des serrures électriques qui s'ouvrent avec des badges ou des codes, ainsi on saura à quelle heure les résidents entrent et sortent. Les ordures seront collectées dans des conteneurs munis de balances, pour savoir à quelle fréquence et en quelle quantité les résidents jettent leurs déchets. Les rues et les axes routiers seront filmés en permanence et des logiciels de reconnaissance de formes compteront les véhicules avec une précision inégalable, et pourront même indiquer le nombre de passagers visibles de chaque voiture, ou le nombre de vélos qui se mêlent à la circulation motorisée pour savoir si cela justifierait la création d'une voie cyclable protégée.

La *smart city* exploite toutes les sources de données en provenance d'autres institutions qui sont autant de « capteurs » : le nombre et l'emplacement des accidents fournis par les commissariats de police et les services de secours, les blessures et les décès comptés par les hôpitaux, les flux de voyageurs constatés par les compagnies de transport en commun (la RATP en Île-de-France, les TCL à Lyon, etc.).

Chaque habitant de la ville, avec son smartphone dans la poche, est une source potentielle de données. Cette contribution est souvent passive : on peut suivre les déplacements de chacun grâce aux bornes téléphoniques « accrochées » par le smartphone[10], deviner le moyen de locomotion en fonction de la vitesse de transition d'une borne à l'autre, et encore plus finement avec les bornes wifi publiques de la ville. Certaines galeries marchandes disposent de capteurs Bluetooth ou wifi pour identifier les téléphones qui passent près des boutiques et savoir lesquels s'arrêtent devant la vitrine, ceux qui entrent ou non, après combien de temps d'hésitation… tout cela dans le but de proposer des publicités ou des promotions ciblées par SMS… Les municipalités aimeront savoir comment leurs habitants circulent dans la ville et quels sont leurs circuits, leurs habitudes, etc.

Mais la contribution des habitants de la *smart city* peut aussi être active : il existe déjà dans de nombreuses villes des applications pour signaler des ordures abandonnées, des décharges sauvages, des

équipements cassés ou – pourquoi pas – des faits de délinquance. Derrière ces ébauches d'interactivité, on devine tout un imaginaire politique où les rapports entre une administration locale (la mairie) et ses administrés (les habitants de la commune) sont expurgés de tout enjeu politique réel, pour ne garder que des relations de client à fournisseur, ou de capteur à unité centrale. Le choix politique n'est jamais à venir, jamais discuté, mais toujours déjà là.

Cette vision d'une *smart city* entièrement technologique commence à être sérieusement remise en cause, y compris par ses promoteurs en France[11], qui ont bien perçu le peu d'attrait de leur fantasme industriel : les pouvoirs locaux ont pu constater, par expérience, que les « solutions » proposées par les opérateurs de la surveillance étaient souvent des gadgets trop chers pour un résultat insuffisant. On préfère désormais lui accoler d'autres fantasmes, comme celui d'une ville « durable », capable de trouver l'équilibre entre la surconsommation énergétique des équipements numériques et les marges d'économies que ces mêmes équipements pourront permettre d'identifier.

Mais il reste un domaine dans lequel les lignes budgétaires sont encore faciles à débloquer, sans susciter le moindre mécontentement des administrés, et qui peut même rapporter des voix aux élections : c'est la sécurité.

RÉACTION POLITIQUE À UN SUJET TECHNIQUE

Dès la parution de l'article du *Monde*, Twitter a réagi. La Quadrature aussi, et parmi nous Félix Tréguer, membre fondateur de l'association et habitant de Marseille. Claire Legros, l'autrice de l'article, a été d'un fair-play parfait : le jour même, elle interviewait Félix et publiait sa réaction[12].

Que dit Félix, au nom de la Quadrature ? Rien de révolutionnaire ni d'extrémiste, seulement des évidences qu'il fallait énoncer pour ne pas laisser penser que le projet de « l'observatoire Big Data de la tranquillité

publique » allait de soi : « C'est la logique même de ces outils qui doit être interrogée. L'idée selon laquelle la technologie va résoudre des problèmes sociaux et qu'en investissant des milliers d'euros on arrivera à garantir la sécurité représente un leurre. Des études ont montré aux États-Unis à quel point ces programmes renforcent des biais tels que la discrimination liée à la couleur de peau. On assiste à un saut en avant technologique lié au Big Data qui entraîne la possibilité de croiser toutes ces données issues de bases diverses. Même si au début on nous vend des dispositifs encadrés, on constate une accoutumance à ces systèmes qui banalisent la société de surveillance. »

Pour étayer ces évidences, il nous faut nous forger une connaissance et un avis de première main sur la question. L'association doit pouvoir argumenter, prouver, illustrer… Pour cela, il existe un outil précieux : les « demandes Cada ».

Depuis le 17 juillet 1978, les citoyens ont un « droit d'accès aux documents administratifs ». Ils peuvent consulter « tous les documents produits ou reçus par une administration publique (administrations d'État, collectivités territoriales, établissements publics) », et même par « les organismes privés chargés d'une mission de service public » en faisant une simple demande par courrier. Ce droit est garanti par la Commission d'accès aux documents administratifs (Cada), qui contrôle la nature des documents pouvant échapper à cette obligation de communication, et qui est aussi l'autorité de recours quand les citoyens estiment que leur droit de consultation n'a pas été correctement respecté.

On devrait dire qu'on envoie une « dada » – une « demande d'accès à un document administratif » – mais dans la langue commune des Garagistes de la Quadrature, c'est devenu une « demande Cada ». Dès qu'il prend connaissance du projet de « l'observatoire Big Data de la tranquillité publique », Félix Tréguer envoie une « demande Cada » à la mairie de Marseille. Les documents qu'il reçoit sont publiés dans un article intitulé « La surveillance policière dopée aux Big Data arrive près de chez vous ![13] », le 20 mars 2018, et complété par l'arrivée de nouveaux documents dès le mois de juin. On sort des discours de

déploration, trop facilement attaquables, pour entrer dans la description documentée des faits. Chacun peut désormais voir de ses propres yeux ce qui est : fin des fantasmes d'épouvante, et commencement de l'angoisse lucide.

Le projet marseillais de « l'observatoire Big Data de la tranquillité publique » se propose d'agréger des informations venues de toutes parts : des fichiers de la police nationale et des mains courantes de la police municipale, qui géolocalise ses données, des décisions de justice, des procès-verbaux des pompiers (à Marseille, ce sont les marins-pompiers), des informations fournies par les transports publics, par les parkings privés, par les caméras de surveillance du trafic routier, par les services locaux de la météo, évidemment, les flux vidéo des caméras municipales (avec l'objectif explicite de disposer à terme de deux mille caméras et de drones), des données fournies par l'État et d'autres collectivités locales, des données en provenance des hôpitaux, et même des données fournies par des sociétés privées (opérateurs téléphoniques par exemple). Sans oublier, et ce n'est pas la moindre, la participation des habitants, invités à fournir des informations à partir de leur smartphone de manière active (envoi de signalements par SMS, de photos ou d'enregistrements audio) ou passive (localisation, vitesse de déplacement, etc.).

Voilà qui est clair : la sardine de l'Observatoire marseillais est en réalité une baleine qui veut tout avaler, et toutes les données qui passent à portée, plancton ou sable, seront aussitôt englouties. Mais dans quel but, ce « Big Data » pantagruélique ? En vue de quelles espérances, de quelles finalités, de quelles observations ? C'est beaucoup moins clair.

« Analyser le passé, apprécier le présent et anticiper l'avenir », dit en substance le cahier des charges du projet marseillais[14]. Ses concepteurs se vantent aussi d'une « approche particulièrement exploratoire et créative » *:* en d'autres termes, ils ne savent pas ce qu'ils font, mais ils sont prêts à tout. Et d'expérience en expérience, de tâtonnement en tâtonnement, ils espèrent bien trouver quelque chose.

Le grand fantasme de l'esprit policier a deux formes spectaculaires que le cinéma nous a beaucoup montrées. La première consiste à vouloir

« punir tous les criminels, et pour tous les crimes » – en cela, le regard total sur la ville est sans doute à la fois une façon d'assouvir ce désir, et un moyen de laisser entendre à la population que rien n'échappera à l'œil qui la surveille. La menace vaut comme mesure. C'est la fameuse « impunité zéro », ou la fameuse « tolérance zéro » chère aux discours démagogiques dont se moque si brillamment le film *Robocop*[15]. L'autre rêve, c'est d'anticiper les crimes, comme dans *Minority Report*[16].

Le fantasme de l'avenir calculable, on l'a vu, existe au moins depuis Leibniz, mais le dernier demi-siècle, témoin à la fois de l'accroissement fulgurant de la puissance de calcul des ordinateurs et de la baisse de leur prix, lui a donné une nouvelle vigueur. Le rêve devient une idée en trouvant le moyen de s'actualiser. Et les pouvoirs publics en 2021 envisagent sérieusement que la police soit dotée des moyens d'anticiper la délinquance ou les crimes graves. On a déjà vu comment, dans le domaine du renseignement, l'horreur du terrorisme était sans cesse rappelée et amplifiée par les politiciens et les médias pour justifier les passe-droits et les mesures de surveillance de masse. Dans le domaine de la « sécurité du quotidien », la « prévention » tient ce rôle d'argument massue, qui tue toute réflexion. Qui serait assez fou pour rejeter la sagesse selon laquelle « mieux vaut prévenir que guérir » ?

La « police prédictive » n'est pas une nouveauté ni une idée marseillaise : elle a déjà été envisagée très sérieusement aux États-Unis, dans de grandes villes à fort taux de criminalité, comme Chicago ou Atlanta. Et là où le renseignement antiterroriste cherche à identifier des personnes ou des réseaux susceptibles de passer à l'action violente, les outils de la police prédictive s'attachent plutôt à dresser des cartes de l'espace urbain, ce qu'on appelle des *heat maps* (« cartes de chaleur ») où les zones à plus forte probabilité de délinquance sont signalées par des couleurs plus chaudes (plus rouges) que les zones urbaines moins dangereuses et plus froides (plus bleues). Le temps est également pris en compte, et les zones de chaleur peuvent se déplacer sur la carte au fil des heures du jour et de la nuit. De telles représentations cartographiques des

risques permettent aux services de police de mieux répartir leurs moyens, des agents ou des voitures de patrouille par exemple.

Mais à l'heure où l'on voit Marseille et d'autres villes françaises s'emparer du fantasme de la « police prédictive », on constate que les villes américaines qui l'avaient expérimentée les premières renoncent à ces outils, et n'en font plus le cœur de leurs investissements en personnel et en argent. On apprend par ailleurs que le logiciel PredPol, vendu par la société du même nom depuis 2012, se fonde sur un algorithme développé par le sismologue David Marsan, de l'université de Savoie à Chambéry[17], sous prétexte que les faits de délinquance se diffuseraient dans la ville à la manière des ondes sismiques dans les sols… Les bases intellectuelles de ces outils ont à peu près le sérieux de l'astrologie. On n'en attendait pas moins de la part d'outils capables de prédire que la délinquance surviendra probablement dans les zones de forte délinquance.

Outre leur moralité et leur scientificité très discutables, les outils numériques de la « tranquillité publique » et de la « police prédictive » ont un coût, que d'autres perçoivent comme un juteux bénéfice. Les caméras, les analyses, les barrières et les armes sont fabriquées et vendues par des groupes industriels et des entreprises dont la peur et la mise sous surveillance de nos vies sont le très profitable fonds de commerce. Et c'est l'autre enseignement que donnent les documents obtenus par les « demandes Cada » : on voit apparaître les noms, les budgets, et les tractations commerciales.

Mettre au jour des discours politiques qui relèvent autant de l'idéologie que du marketing ; suivre d'une ville à l'autre le déploiement de dispositifs de surveillance inutiles, fantaisistes et coûteux ; repérer les acteurs politiques et industriels de la surveillance généralisée ; connaître l'état des systèmes pour dénoncer la surveillance de masse en pleine connaissance de cause : c'est l'ambition originelle de la campagne Technopolice de La Quadrature du Net, lancée en septembre 2019.

2. LA TECHNOPOLICE EST DÉJÀ PARTOUT : RETOUR SUR UN FUTUR SANS AVENIR

Le coup de tonnerre de « l'observatoire Big Data de la tranquillité publique » de Marseille n'est pas arrivé dans un ciel bleu. Mais avec l'avantage donné par le regard rétrospectif, on retrouve très facilement les premiers nuages auxquels on n'avait pas prêté suffisamment attention, et les impacts de foudre qui étaient tombés tout près sans qu'on les entende.

LE SPORT, UN LABORATOIRE SÉCURITAIRE

Les grands rassemblements publics font évidemment l'objet d'une attention particulière de la part des autorités de police, qui craignent à la fois la petite délinquance (dont le gagne-pain se trouve dans les poches des touristes), les débordements de supporters rivaux pleins d'alcool et de fierté chauvine mais aussi, désormais, les attaques terroristes.

Leur crainte est, hélas, fondée sur des faits douloureux. On se souvient par exemple de la bombe qui avait explosé dans la foule lors des Jeux olympiques d'Atlanta, en 1996, posée là par un militant d'extrême droite opposé à la légalisation de l'avortement par le gouvernement fédéral des États-Unis. Mais le terrorisme « domestique » n'est pas le seul problème. Les pays qui accueillent les Jeux olympiques craignent

surtout son exposition internationale : toutes les caméras sont braquées sur l'événement.

Un épisode traumatique est à l'origine de cette peur : la prise d'otages des athlètes israéliens par un groupe armé pro-palestinien lors des Jeux de Munich en 1972, qui avait fait dix-sept morts, dont onze athlètes. Depuis lors, les Jeux olympiques sont sous très haute surveillance.

Les Jeux olympiques de Londres, en août 2012, ont été l'occasion d'un déploiement de force sécuritaire démesuré, mais qui avait en grande partie été médiatisé en raison de son organisation désastreuse[1]. Les sociétés privées de surveillance qui avaient raflé le marché du gardiennage des sites et des événements olympiques s'étaient couvertes de ridicule, en se montrant incapables d'embaucher assez de personnel pour remplir leur contrat[2], au point que le gouvernement britannique, qui donnait une grande importance à la question de la sécurité, avait eu recours à l'armée pour sauver la face. Les Londoniens vivant près des grandes installations olympiques avaient même eu la surprise de voir l'armée britannique installer des batteries de missiles anti-aériens sur le toit de leurs immeubles. Le souvenir des avions détournés du 11 septembre 2001 aux États-Unis, et le souvenir plus proche des attentats simultanés du 7 juillet 2005 (quatre bombes avaient explosé dans les transports londoniens à quelques minutes d'intervalle), tout justifiait la paranoïa du gouvernement britannique et son besoin de rassurer sa population[3] et les très nombreux touristes attendus pour l'occasion, quitte à placer la ville dans une sorte de camp militaire à ciel ouvert.

Quatre ans plus tôt, en 2008, on avait regardé avec incrédulité la République populaire de Chine organiser les Jeux olympiques de Pékin dans une ambiance policière qui défiait l'imagination. À peine vingt ans après la répression sanglante de l'occupation de la place Tiananmen, il était devenu une évidence pour le monde entier que « la Chine » désignait tout à la fois, ou alternativement, une usine géante fournissant le capitalisme mondial en produits de toutes sortes, un enfer écologique lointain en raison de cette « délocalisation » industrielle, et un État-prison maintenant l'ordre d'une main de fer dans une société très

inégalitaire, où l'enrichissement de quelques-uns côtoyait la très grande pauvreté de la masse laborieuse, sous un drapeau communiste devenu tout à fait incongru. « La Chine » était même devenue une expression toute faite pour désigner cette bizarrerie du monde moderne, avec sans doute un bon fond de condescendance et de préjugés xénophobes, comme si « les Chinois » avaient une prédisposition culturelle pour la surveillance de masse et les régimes policiers de toute éternité.

Lors des Jeux de Pékin, la presse occidentale décrit un monde qui fait sans doute frémir les lecteurs de 2008, mais en leur ménageant la possibilité de sourire de soulagement, tant l'exotisme et la distance géographique atténuent la portée du constat : « Un réseau de caméras couvrant l'ensemble de la capitale a été mis en place. Chaque quartier a été doté d'une salle de surveillance équipée de caméras et d'un système d'enregistrement. Dès 2006, on avait atteint un taux de couverture de 100 %. Avant les Jeux, les caméras devaient être mises en réseau, pour que la police pékinoise puisse avoir une vue d'ensemble de la capitale. Cela concerne non seulement les caméras de quartier, mais aussi les caméras de surveillance des banques, ainsi que celles fixées aux feux tricolores ou dans les rues. La même scène pourra ainsi être filmée par plusieurs caméras, ce qui permettra d'avoir des preuves d'origine différente. Les poubelles des secteurs stratégiques de la capitale ont été numérotées et placées sous la surveillance de caméras. Sans en avoir l'impression, on est contrôlé en permanence par un système d'alerte très dense. "Tout Pékin se trouve couvert par un filet tendu de toutes parts", fait remarquer Ma Xin[4]. »

Et pourtant, ce que décrit cet article paraît malheureusement banal, et même familier, à un lecteur français de 2021 : les « centres de supervision urbaine » (CSU) dont la *safe city* et les polices municipales sont friandes sont très exactement ce dont il est question dans « la Chine » exotique et lointaine de 2008.

En matière de surveillance, le Royaume-Uni de 2012 n'est pas en reste, comme on l'a vu. Il est d'ailleurs intéressant de noter que la Grande-Bretagne fait figure, en Europe, avec son statut d'outsider encore

aggravé depuis le « Brexit », de pionnière en la matière. Nos collègues de l'association Big Brother Watch[5], par exemple, sont plus avancés que nous dans la prise de conscience de la vidéosurveillance totale, parce que leur pays est couvert de caméras depuis plus de deux décennies. On se rappellera par ailleurs que la police du comté du Kent a été l'une des premières à utiliser le logiciel PredPol dès 2013, ou encore que le Royaume-Uni fait partie des *Five Eyes* – un réseau d'espionnage et de partage d'informations qui réunit aussi les États-Unis, le Canada, l'Australie, la Nouvelle-Zélande et le Royaume-Uni – et dont les documents rendus publics par Edward Snowden en 2013 ont révélé plusieurs programmes de surveillance, dont le programme PRISM[6].

Les Jeux olympiques sont l'occasion de faire deux fois la publicité de la sécurité : d'une part comme affichage politique, à l'intérieur comme en direction de l'étranger, et d'autre part comme vitrine commerciale, avec la mise en avant des savoir-faire et des équipements vendus par les sociétés nationales. Mais le sport sert aussi, et depuis longtemps, de terrain d'expérimentation pour la surveillance.

En France, les supporters de foot sont traités comme une population dangereuse, et à ce titre comme une population aux droits inférieurs. On peut interdire administrativement, et sans jugement, à des personnes d'assister à un match. On peut fermer une tribune, un stade, ou interdire des déplacements collectifs. Mais on peut aussi viser une personne, sans qu'elle puisse se défendre. Les préfets ont les mains libres pour punir et humilier les supporters, assimilés dans leur ensemble à des hooligans, quels que soient leurs agissements réels. Les décisions de police administrative, dont la motivation ou la proportionnalité ne sont pas contrôlées au préalable par la justice, nouveauté scandaleuse qui inquiéta beaucoup au moment de l'état d'urgence fin 2015, n'avaient rien d'une nouveauté pour les habitués des stades : ils connaissaient ces punitions arbitraires depuis des années. Bien sûr, il existe des recours devant la justice administrative. Mais la mauvaise réputation des « mauvais garçons » les précède et saborde leur défense d'avance.

Début 2020, on apprend par Olivier Tesquet, journaliste et auteur de *À la trace : enquête sur les nouveaux territoires de la surveillance*[7], à l'occasion d'une interview confiée au journal S*treetPress*[8], que les supporters du FC Metz auraient été soumis à la reconnaissance faciale à l'entrée du stade Saint-Symphorien. Olivier Tesquet a découvert cela en s'intéressant à la société Two-i[9], une start-up messine de l'intelligence artificielle appliquée à la surveillance vidéo. Jusqu'à présent, le club n'en avait pas parlé. Mais à la publication de cette interview, les supporters du FC Metz relient les points : ils se souviennent de ce jour où il leur a été demandé d'enlever écharpes, casquettes et lunettes à l'entrée d'un match contre Strasbourg. L'Association nationale des supporters publie aussitôt un communiqué pour dénoncer une pratique attentatoire aux libertés : « Nous refusons de devenir les rats de laboratoire de la reconnaissance faciale[10]. » Face au tollé, la société Two-i et les responsables du FC Metz se noient ensuite dans une série de justifications décousues : c'était seulement une expérimentation, dans un cadre légal puisque la loi Larrivé[11] autorise la surveillance des personnes interdites d'entrée au stade, mais c'est aussi un moyen de lutter contre le terrorisme puisque le traitement d'image permet de reconnaître des armes ou des colis suspects, d'ailleurs le test n'a pas eu lieu, mais on a le matériel pour le faire, et enfin s'il a eu lieu, c'était seulement avec des salariés volontaires de l'entreprise de surveillance. Bref, une salade de contradictions. La CNIL tranche le débat un an plus tard, en publiant une mise en garde formelle contre le club[12] : la reconnaissance faciale sauvage dans les stades est illégale.

On se retrouve une fois de plus face à la démission de l'autorité chargée de protéger nos données personnelles. Les données biométriques, strictement encadrées par le RGPD en tant que « données sensibles », « ne doivent pas être traitées », sauf exception dans des cas bien précis (mais pas celui-ci). La légèreté avec laquelle certains décident d'utiliser des technologies largement attentatoires aux libertés devrait faire réagir l'autorité et provoquer la condamnation et le paiement d'une amende

pouvant aller jusqu'à plusieurs millions d'euros. Dans le cas contraire, aucune raison que l'atteinte aux droits ne se réitère pas, ici ou ailleurs.

Au printemps 2020, une autre expérimentation se tient lors du tournoi de tennis de Roland-Garros. En toute discrétion là encore, puisqu'on en entend parler presque par hasard, en janvier 2021, par le biais d'une réponse du gouvernement à une question écrite posée par un sénateur… un an plus tôt[13]. À une question du sénateur Karoutchi (les Républicains), qui s'enquiert de la volonté du gouvernement de lever les entraves légales qui gênent l'expérimentation de la reconnaissance faciale à grande échelle, le secrétariat d'État chargé de la Transition numérique et des Communications électroniques répond d'abord avec une description du cadre légal (RGPD, directive Police-Justice), puis énumère les expériences déjà réalisées. Parmi celles qu'on connaît déjà, on en découvre une nouvelle : « […] une autre expérimentation a été conduite dans le cadre du tournoi de Roland-Garros 2020. Élaborée en coordination entre le secrétariat général de la Défense et de la Sécurité nationale et le Comité national à la sécurité des Jeux olympiques, elle a notamment permis de tester un dispositif de contrôle d'accès pour les arbitres dans le cadre d'un grand événement sportif, en vue d'une possible application durant les Jeux olympiques de Paris 2024. »

Sur cette expérimentation, on a très peu d'informations. On sait seulement que les outils utilisés étaient fournis par Thales, grande entreprise de l'armement qui veut élargir ses débouchés en se lançant dans la *smart city* et la surveillance civile. On constate aussi que des autorités publiques et militaires chapeautaient l'opération. La finalité de l'expérience semblait être l'authentification des juges-arbitres au moment de leur entrée dans les espaces réservés du tournoi : il s'agissait de s'assurer que seules les personnes autorisées pouvaient accéder aux coulisses et aux espaces professionnels de l'événement.

Mais du stade de Metz à Roland-Garros, l'ambiance n'est pas la même. La reconnaissance faciale a, elle aussi, plusieurs visages. À Metz, on se sert de la reconnaissance faciale pour fliquer, sans les prévenir, des spectateurs qui ont mauvaise réputation, et viennent en grand nombre

apprécier bruyamment un sport populaire. Quant à l'opération de reconnaissance faciale en tant que telle, elle relève techniquement d'une identification : c'est-à-dire qu'on examine chaque visage et qu'on tente d'identifier dans la foule des personnes dont le visage est déjà connu par ailleurs, et dont la présence n'est pas souhaitée. On recherche activement un visage dangereux dans une foule. Ici, à Metz, la reconnaissance faciale est utilisée pour surveiller les masses dangereuses.

Là, à Roland-Garros, il s'agit d'authentification. L'authentification consiste à analyser un visage unique qui se présente devant la caméra et à le comparer avec un visage unique de référence, gardé en mémoire dans un badge par exemple. Il s'agit de prouver qu'une personne est bien celle qu'elle dit être. L'authentification est beaucoup plus protectrice que l'identification. Quand vous déverrouillez votre téléphone avec votre visage, ou avec votre empreinte digitale, autre donnée biométrique unique, vous vous authentifiez et c'est bien pour protéger l'accès à vos données. Quand un juge-arbitre de Roland-Garros se présente à l'entrée de l'espace réservé aux officiels du tournoi et place son visage devant une caméra, ce n'est pas pour être puni, ce n'est pas pour vérifier qu'il n'est pas un terroriste fiché ou un supporter violent, mais c'est pour accéder à un espace où sa présence est légitime. La reconnaissance faciale fonctionne alors comme une reconnaissance sociale.

L'authentification ouvre des portes légitimes, l'identification ferme des portes et exclut. C'est pourquoi il est vain de parler de la reconnaissance faciale de manière abstraite. Il faut toujours se demander de quelle reconnaissance faciale il est question, appliquée à qui, dans quel but, et par qui. Compliquer la vie des pauvres ou faciliter la vie des riches reste malgré tout, sous des abords caricaturaux, une assez bonne approximation de la situation, qu'il faut ensuite affiner. Mais il est bon d'avoir en tête ces quelques éléments de repère la prochaine fois que vous entendrez quelqu'un s'enthousiasmer pour un usage ou l'autre de la reconnaissance faciale. Nous, à la Quadrature, nous insistons depuis longtemps sur les nécessaires distinctions, et sur la façon dont les usages positifs ou ludiques de la biométrie (sécuriser mon téléphone)

fonctionnent aussi comme autant de points d'entrée et de banalisation de l'outil technique pour des usages beaucoup plus graves (tri social, surveillance, criminalisation et suppression des comportements minoritaires[14]).

LA VIDÉOSURVEILLANCE INTELLIGENTE

Entre 1990 et 2015, les caméras de surveillance ont recouvert le territoire français. Ce déploiement massif, sur fonds publics, était porté par une idéologie sécuritaire, et soutenu par une industrie. Malgré quelques réticences, locales et minoritaires, l'installation des caméras a rencontré peu d'obstacles. Le discours médiatico-politique matraque depuis trente ou quarante ans comme une évidence la montée de l'insécurité, et même du « sentiment d'insécurité ». Le cinéma et les séries télé participent à banaliser l'idée que les images de vidéosurveillance sont essentielles pour identifier les délinquants, résoudre très rapidement les enquêtes criminelles, et même trouver les terroristes dans les rues.

Mais vingt ans plus tard, on se rend compte qu'on n'a tout bêtement pas le temps matériel, le temps humain, de regarder autant d'images. Oui, c'est aussi bête que ça, et c'est d'ailleurs un argument qu'on rencontre dans les cahiers des charges des communes, ou dans les plaquettes publicitaires des équipementiers de la vidéosurveillance automatisée : il y a désormais trop de caméras, qui produisent trop d'heures de vidéo, et pas assez de personnel pour les regarder toutes.

Pour y parvenir, il faudrait embaucher, idée honnie par l'économie capitaliste. Heureusement, l'informatique est arrivée à un stade où elle peut analyser des flux d'images avec une certaine efficacité, et à moindre coût ! D'où l'idée de confier le travail à des logiciels ou, mieux encore : à « l'intelligence artificielle ». L'intelligence artificielle, finalement, n'est rien d'autre qu'une machine qui peut exécuter des tâches intellectuelles.

Voici sans doute une des premières découvertes que nous avons faites grâce aux « demandes Cada » envoyées tous azimuts : la

vidéosurveillance automatisée est déjà très répandue dans les communes françaises. On ne parle pas de « banales » caméras de surveillance, ce qui serait un moindre mal, mais d'analyse des images par des logiciels autonomes, dans le cadre de la « vidéosurveillance intelligente ».

De quelle intelligence s'agit-il ? On demande aux caméras de surveillance de comprendre ce qu'elles filment : les logiciels sont chargés de « lire » les images en temps réel, de les interpréter, et de lancer une alerte en fonction de la situation détectée. Par exemple, les bénévoles de la campagne Technopolice ont trouvé en ligne les vidéos publicitaires d'un logiciel vendu à des chaînes de supermarchés, prétendument capable d'identifier les comportements des voleurs en train d'agir dans les rayons[15]. Le peu d'informations disponibles en ligne permet cependant de comprendre que le programme de cette « intelligence artificielle » repose en grande partie sur du travail humain. Les alertes sont envoyées dans les supermarchés par SMS, accompagnées d'une capture d'écran, et souvent suivies d'un échange entre l'opérateur de surveillance et le supermarché : « Vous l'avez attrapé ? — Oui c'est bon, merci ! », ou « Fausse alerte, merci quand même ».

Les « travailleurs du clic » chers au sociologue Antonio Casilli[16] sont nombreux dans tous les domaines où l'on promet les miracles de « l'intelligence artificielle », alors que les outils ne sont pas arrivés à maturité. Les commerciaux vendent des fonctions ou des performances imaginaires, et les équipes d'employés sont chargées de remplir les tâches qualifiées qu'on croit avoir confiées à des machines. Il serait étonnant que la surveillance échappe entièrement à la règle.

Mais au-delà des arnaques commerciales et des discours publicitaires, l'interprétation numérique des images est une réalité : les logiciels sont capables de reconnaître des formes, des séquences, des situations, parce qu'on leur a appris à le faire, en leur montrant des quantités d'exemples « bons » et « mauvais » – les meilleurs d'entre eux étant supposément capables de « s'auto-former », et d'améliorer la précision de leur détection au fil du temps, en accumulant les nouveaux cas. Comme à chaque fois qu'il est question « d'intelligence artificielle », expression

poudre aux yeux, il faut comprendre qu'un logiciel auquel on a fourni de très grandes quantités d'exemples qualifiés, au prix d'un grand travail humain préalable, est capable d'identifier les cas similaires dans les nouvelles images qu'on lui montrera. C'est une définition de l'intelligence assez médiocre, mais suffisante pour monter la garde dans un parking et différencier un humain d'une voiture ou d'un cheval.

D'après les cas recueillis au cours de la campagne Technopolice, les critères retenus pour la vidéosurveillance sont souvent assez simples, et ne doivent pas demander un travail informatique très poussé. Il s'agit par exemple, dans les couloirs du métro parisien, d'identifier les personnes qui stationnent trop longtemps au même endroit : ça s'appelle du « maraudage » dans le jargon des surveillants professionnels, et pour une caméra « intelligente » c'est défini par une silhouette humaine en station immobile pendant plus de trois cents secondes (ou cinq minutes) dans un lieu que la « normalité » estime devoir être consacré au passage : un couloir de métro, ou les allées d'un centre commercial. L'immobilité dans les lieux de passage est un excellent critère pour repérer un mendiant, un sans-abri qui s'installe au chaud, ou un musicien qui fait la manche. Guerre aux pauvres, dit le niveau zéro de la surveillance. Le prétexte invoqué étant, bien entendu, toujours le pire : un homme immobile ne sera jamais envisagé comme un homme fatigué ou contemplatif, ni même comme un vendeur de cigarettes à la sauvette, mais toujours comme un dealer de drogue, ou bien entendu un terroriste qui attend le signal pour passer à l'action.

Dès les premiers temps de la campagne Technopolice, nous nous rendons compte que les caméras « intelligentes » sont bien plus répandues qu'on le pensait, mais qu'il est plutôt difficile de savoir ce qui est exactement mis en place. Il semble que certaines communes ne savent pas vraiment ce qu'elles ont acheté. Que les fonctions des logiciels ne sont pas toujours activées, ou utilisées. Ou qu'elles le sont sans que la population soit avertie. Il existe une large gamme de « fonctions » ou de « tâches » que peut remplir un logiciel de surveillance : des plus impersonnelles (détecter des tags, repérer des bagages abandonnés,

compter les individus composant une foule) aux plus individuelles, comme suivre une personne précise d'une caméra à l'autre, ou réagir à des gestes violents, des coups, une fuite au pas de course…

Tout le problème est dans les points de suspension. On les voit souvent dans les plaquettes de communication des entreprises : « détection des comportements suspects… ». C'est quoi, un comportement suspect ? Des points de suspension… Impossible d'en savoir plus. Le comportement suspect est un implicite, et chaque société sait très bien ce qu'elle entend, quand elle parle de « crime », ou de « suspect ». Il y a les *usual suspects*, les « suspects habituels » dont chacun sait qu'ils ont la peau sombre et portent un jogging, des baskets, une casquette ou une capuche. Mais les choses ne sont jamais dites. Puisque c'est évident, pourquoi le dire ? Un comportement suspect, c'est une chose qu'on laisse au non-dit, à l'inconscient collectif et au préjugé, sous couvert de bon sens. Les préjugés se renforcent de n'être jamais explicités.

Mais il y a aussi tout ce qu'il est préférable de taire, pour que la détection soit efficace. Saviez-vous que si vous restez immobile plus de trois cents secondes dans un couloir du métro parisien, vous déclenchez peut-être une alerte sur un écran, quelque part dans un centre de surveillance vidéo ? Et maintenant que vous le savez, allez-vous changer votre comportement pour devenir indétectable, ou déclencher au contraire volontairement des alertes « bruitistes » pour brouiller et saboter la surveillance en saturant les capteurs ?

Le flou entretenu par tous les acteurs de la surveillance bénéficie bien sûr uniquement à la surveillance. Le célèbre *chilling effect*, l'effet « glaçant » ou inhibant d'une menace à la réalité diffuse et imprécise, est beaucoup plus puissant que la crainte précise d'une surveillance localisée. Mais le flou sur les techniques et les logiciels nous est souvent renvoyé, sous la forme d'une accusation de fantasme ou de délire : « Vous vous montez le bourrichon, Big Brother n'existe pas, la surveillance ne marche pas bien, les logiciels ne sont pas au point, etc. » On ne peut évidemment pas se contenter d'une telle logique. Qu'est-ce qui est le plus inquiétant ? Devoir se contenter d'en savoir si peu sur les systèmes de

surveillance qui sont déployés au-dessus de nous ? Ou devoir faire confiance à nos gouvernants qui disent « Ne vous inquiétez pas » ? L'enquête est nécessaire, et l'évaluation publique de la surveillance est une nécessité démocratique fondamentale.

3. Décentraliser la lutte contre la technopolice

Les expérimentations de surveillance automatisée sont nombreuses, et dans tout le pays. Les pratiques sont déjà là, cachées sans l'être, invisibles seulement parce que personne ne semble s'en soucier. Après des décennies d'idéologie sécuritaire dominante et décomplexée, et après des années de menace terroriste bien réelle, la surveillance du quotidien paraît être devenue une banalité. Les villes qui surveillent et les entreprises qui les équipent ont même souvent assez de candeur pour s'en vanter. L'époque semble trouver évident le besoin de surveiller les gens.

À la Quadrature, nous avons une sensibilité particulière à la question. Depuis des années, on voit la surveillance progresser et s'immiscer partout, des outils magnifiques être détournés de leur finalité première et devenir des instruments d'espionnage et de coercition. Qu'il s'agisse de la façon dont les entreprises privées se sont emparées du Web pour en faire une gigantesque machine publicitaire[1], ou de la façon dont la police et les services de renseignement cherchent à faire légaliser l'enregistrement et l'exploitation de toutes nos activités numériques, la logique à l'œuvre est la même : collecter nos traces et les croiser, cerner nos faits et gestes, deviner nos pensées, et nous classer dans des comportements prévisibles, qu'il s'agisse de nos pulsions d'achat ou de nos revendications politiques.

Avec un pas de recul, le tableau est terriblement noir : nos vies numérisées – et elles le sont très largement, que nous l'admettions ou non, à partir du moment où nous avons un smartphone dans la poche ou

un ordinateur à la maison –, nos vies connectées sont tout bonnement des vies sous surveillance.

LA FIERTÉ DE SURVEILLER

Le techno-flicage est une industrie comme une autre, il a ses entreprises, son marché, et il a ses catalogues : par exemple, on recommande aux esprits curieux la lecture du catalogue de l'AN2V. Ce sigle est celui de l'Association nationale de la vidéoprotection[2], un groupement d'intérêt qui rassemble des « communes vidéosurveillées » et des dizaines d'entreprises locales, nationales ou internationales, toutes spécialisées dans la fabrication ou la vente d'équipements de surveillance : caméras, capteurs, drones, logiciels, etc. En lisant ce beau catalogue où s'échangent les « bonnes pratiques » (de surveillance) et les « retours d'expériences » (de surveillance), les entreprises mettent en avant leurs réussites, avec l'appui complice des mairies (leurs clientes), pour convaincre de nouvelles mairies (et de futures clientes). On se vante, on se fait mousser, on met son plus beau costume, on fait de belles phrases et de belles photos. On fait du lobbying. Mais pour qui veut savoir comment il est surveillé, pour qui se demande qui surveille et comment, c'est une mine d'or à ciel ouvert.

On y apprend par exemple que Christian Estrosi, maire de Nice et paladin de la *safe city*, aurait testé la vidéosurveillance automatisée dans sa ville, avec la reconnaissance des émotions. Il est fier d'être aussi le tout premier à tester la reconnaissance faciale sur la voie publique, lors du carnaval de Nice, en février 2019[3] : ce test grandeur nature est présenté comme parfaitement légal, même la CNIL serait d'accord ! Pas de chance, c'est un gros mensonge. Médiatisé une première fois lors du carnaval, le test connaît une deuxième couverture médiatique, plus importante et moins favorable, en août 2019, lorsque la CNIL s'alarme de l'illégalité de l'opération, pour laquelle elle n'a en réalité pas été consultée, et qu'elle n'a absolument jamais autorisée.

Le dispositif du test niçois est très simple. On soumet à un logiciel nommé AnyVision, développé par une entreprise monégasque (qui est à l'initiative de l'opération), une cinquantaine de photos fournies par des volontaires (la plupart sont des employés de la mairie) : le logiciel est chargé de retrouver les cinquante cobayes dans les images de vidéosurveillance de la ville, au moment où la foule du carnaval envahit les rues. Pour corser l'affaire, et mettre en valeur la qualité du logiciel, certaines photos datent même de « plusieurs décennies[4] », et la reconnaissance faciale doit donc prendre en compte le vieillissement probable des protagonistes. D'après la ville et l'entreprise, l'opération est un succès total, avec une reconnaissance réussie à 100 %. Le microclimat de Nice serait donc très favorable au développement des palmiers, des orangers, et de la reconnaissance faciale.

Mais la CNIL n'a pas beaucoup apprécié d'être citée comme caution de l'expérience, alors qu'elle n'avait pas émis d'avis sur le projet. Son communiqué d'août 2019 douche l'enthousiasme niçois. Trop tard, le mal est fait : Estrosi a pu se poser en précurseur de la surveillance et en personnalité forte, à qui les opérations en dehors du cadre légal ne font pas peur.

La région PACA, avec ses élus de droite volontiers démagos qui misent tout sur la sécurité, est un paradis de la technopolice. À peine a-t-on laissé Nice et son carnaval de la surveillance, qu'on y revient pour une autre expérimentation, cette fois-ci à l'initiative de la région. Nous sommes alertés par des militants syndicaux de l'Éducation nationale : la région, là aussi avec l'appui de Christian Estrosi, veut installer aux portes de deux lycées, à Marseille et à Nice, un portique de reconnaissance faciale pour filtrer l'entrée des élèves. Ceux-ci auront un badge sur lequel sera enregistrée leur photo : ils devront se présenter devant la caméra, et si le visage ne correspond pas à l'image du badge, le portail ne s'ouvre pas.

Cette fois, il n'est pas trop tard pour agir. Les portiques sont déjà en cours d'installation – des parents d'élèves nous envoient même des photos de l'avancée des travaux –, mais il est encore temps d'attaquer la

décision de la région devant le tribunal administratif. C'est ce que nous faisons en février 2019, avec la Ligue des droits de l'homme (LDH), la CGT Éduc'action des Alpes-Maritimes et la Fédération des conseils de parents d'élèves des écoles publiques des Alpes-Maritimes. L'argumentaire juridique s'appuie principalement sur le RGPD et la façon dont il encadre le recours à la biométrie : dans le cas présent, l'usage de la reconnaissance faciale paraît nettement disproportionné par rapport à la finalité visée[5]. L'affaire traîne un peu. En octobre 2019, la CNIL vient en renfort, en publiant un communiqué qui arrive aux mêmes conclusions que nous : « Après un examen attentif du projet, la CNIL a considéré que le dispositif projeté est contraire aux grands principes de proportionnalité et de minimisation des données posés par le RGPD[6]. » Le tribunal administratif de Marseille nous donne enfin raison, en février 2020, un an après le dépôt du recours[7]. La reconnaissance faciale à l'entrée des lycées est illégale, et les portiques de Marseille et de Nice n'entreront jamais en service.

Cette victoire nous galvanise ! Nous pouvons gagner et faire arrêter des projets ! Non, la surveillance n'est pas une fatalité. Elle est encore en grande partie illégale, elle devrait être un scandale démocratique, et nous n'allons pas la laisser s'installer sans rien faire…

DES MICROS DANS LES RUES DE SAINT-ÉTIENNE

Dès l'affaire de « l'observatoire Big Data de la tranquillité publique », à Marseille en décembre 2019, Félix Tréguer a l'intuition que l'exemple marseillais n'est pas un cas isolé, une exception ou une aberration, mais plutôt le sommet émergé d'un iceberg. Il faudrait plonger pour en voir plus. Pour cela, les « demandes Cada » sont un outil merveilleux auquel il devient urgent de recourir.

Les mairies à qui on les adresse peuvent avoir de nombreuses raisons de ne pas vouloir nous répondre positivement. Elles peuvent jouer sur les exceptions prévues par la loi : les documents sont « en cours d'édition »,

ou concernent une affaire « en cours », ou leur publication constitue un risque pour la sécurité publique, etc. Parfois, les mairies ne savent même pas ce qu'elles achètent ou possèdent : il est arrivé plus d'une fois, nous avons pu le constater, qu'une mairie renouvelle son matériel ou passe un contrat global de vidéosurveillance sans savoir qu'un logiciel de vidéosurveillance automatisée (VSA) lui était vendu en même temps. Et bien sûr, certaines autorités locales ne jouent pas le jeu. Non, l'expression n'est pas juste : certaines autorités locales ne respectent pas la loi. Elles ont deux mois pour instruire la demande et répondre. Passé ce délai, nous pouvons nous tourner vers la Cada elle-même, l'autorité chargée de veiller à l'application de la loi. Mais ces recours sont très longs – trop longs.

Malgré tous les obstacles et les lenteurs de bonne ou de mauvaise volonté, nous recevons des réponses à nos demandes. Qu'espère-t-on obtenir ? Des délibérations, des cahiers des charges, des appels d'offres, des devis, des contrats, bref, tout ce qui peut décrire avec la plus grande précision possible les systèmes vendus aux communes, et leurs conditions réelles d'utilisation. Au fur et à mesure de l'avancée de la campagne Technopolice, les informations nouvelles sont de plus en plus rares : on commence à connaître les outils et les entreprises qui les vendent. Mais ça ne veut pas dire pour autant que les informations ordinaires ne sont pas pertinentes : leur banalité dit quelque chose de la réalité qui s'installe, de la banalité de la surveillance, et de la surenchère commerciale qui l'aggrave d'année en année. Et au milieu de cette masse, on trouve quelques pépites, quelques divines surprises.

La meilleure de toutes est sans doute venue de Saint-Étienne. Alerté par des articles de presse publiés en mars 2019[8], un petit groupe de la Quadrature adresse à la mairie de la ville une « demande Cada » au sujet d'un projet étrange : l'installation de cinquante micros, dans un quartier pauvre de la ville, pour identifier les sons susceptibles de déclencher une intervention de police.

La réponse arrive dans les temps, début avril, et elle est merveilleuse : soit par ignorance, soit par zèle, la personne chargée de notre dossier a

tout donné. Plus de deux cents pages sur les rendez-vous de la mairie avec l'entreprise Serenicity, les projets abandonnés, les comptes rendus de réunions… Une vraie transparence ! Le 15 avril 2019, nous publions tout, documents bruts et analyses, sur le site (alors encore embryonnaire) de la campagne Technopolice[9]. On découvre que les micros sont les premiers maillons d'une chaîne. Les fameux « capteurs sonores » enregistreraient des « anormalités sonores » (dont la liste est si impressionnante – coups de feu, cris, perceuse, meuleuse, klaxons, coups de sifflet, bombes aérosols, crépitements… – qu'on se demande quels bruits n'en font pas partie), déclenchant aussitôt une alerte auprès de la police, qui décide alors s'il convient ou non d'intervenir.

Mais ce n'est pas tout ! On apprend ensuite que le projet initial comportait une seconde phase, qui donnait la part belle aux drones pour « lever le doute » des alertes et, éventuellement, suivre à la trace les fuyards. Elle s'appuyait aussi sur le développement d'une application, permettant aux habitants de signaler « un problème ». Drones et application sont pour l'instant abandonnés, du fait d'une « législation trop stricte », mais jusqu'à quand ?

Non, vous ne rêvez pas : c'est une robotisation totale de l'espace public, avec disparition de l'humain, comme si la personne se déplaçant dans les rues n'était pas seulement suspecte mais dangereuse par nature. Les quartiers pauvres considérés comme des zones de non-droit, des territoires à réprimer, ce n'est pas une exagération de militant ou un fantasme d'opprimé imaginaire : c'est une réalité pratique, une façon de faire, un état de fait dont les personnes sérieuses parlent entre elles sur le ton de l'évidence, en costume-cravate et en uniforme, une calculette à la main. Nous laissons à l'appréciation des lecteurs et des lectrices la difficulté de savoir dans quel quartier de la ville, de la banlieue ou du centre de décision qui lui envoie des drones, l'humanité semble se retirer le plus violemment.

En même temps que nous publions l'article et les documents généreusement fournis par la mairie de Saint-Étienne, nous adressons un courrier à la CNIL, car les articles de presse qui évoquent le projet

confirment tous son accord préalable, mis en avant par la mairie de Saint-Étienne pour se couvrir et rassurer tout le monde. En mai 2019, la ville annonce qu'elle repousse la mise en place de l'expérience[10]. Le 25 octobre 2019, Marie-Laure Denis, toute nouvelle présidente de la CNIL, adresse à la ville un courrier très sec[11] : « Je vous avertis qu'à défaut d'un cadre légal spécifique et adapté […], le traitement de données à caractère personnel en question ne saurait être mis en œuvre de façon licite. »

Ce « je vous avertis » n'est pas une menace de cour de récréation : il s'agit bel et bien d'un avertissement à valeur légale, un des pouvoirs dont la CNIL est investie[12]. Le projet de micros policiers est aussitôt abandonné[13].

DÉCENTRALISER LA LUTTE

Valenciennes qui se lance dans la vidéosurveillance automatisée avec les outils du Chinois Huawei, Toulouse qui s'acoquine avec IBM, des drones à Istres, des capteurs sonores à Saint-Étienne ou à Strasbourg, un « observatoire Big Data de la tranquillité publique » à Marseille, de la détection d'émotions dans le tramway de Nice, une société israélienne (Briefcam) qui affirme être présente dans cent villes de France avec son logiciel « d'aide à la vision » !… Au fur et à mesure de notre avancée dans le nouveau monde de la technopolice, l'évidence s'impose : les expériences partent dans tous les sens, rien n'est vraiment centralisé ou valable à l'échelle nationale.

Le financement est parfois national, en partie grâce à des fonds dédiés du ministère de l'Intérieur, et le discours politique sécuritaire qui sous-tend l'ensemble est bien entendu national, tout comme l'idéologie triomphante de l'alliance entre la technologie, l'entreprise privée et la sécurité. Mais l'essentiel de la mise en œuvre semble se passer de gré à gré entre des communes et des entreprises. Loin d'un grand plan national et gouvernemental concerté, on assiste à un fourmillement de petits

projets locaux. Il va donc falloir se livrer à un travail de fourmi pour documenter et analyser ce que les communes inventent, ici ou là, avec l'aide et l'incitation très active des entreprises de la surveillance.

Beaucoup de régions, de départements, de villes grandes ou petites, mettent à jour leur système de vidéosurveillance, et les entreprises les embarquent alors dans leur logique « mieux-disante » de technique dernier cri. Certaines sont en relation avec des entreprises locales, des start-up hébergées dans des pépinières d'entreprises subventionnées, avec qui elles échangent régulièrement, et qui se trouvent être des partenaires « naturelles » quand vient le jour de tester leurs outils : ainsi les micros de Saint-Étienne étaient-ils installés par la société stéphanoise Serenicity, créée par le propriétaire et dirigeant de la maison stéphanoise Vernay-Carron, qui fabrique des armes de chasse depuis deux cents ans (« L'art de la chasse, l'amour de la nature ») et s'est rendue célèbre en fabriquant le fameux Flash-Ball ou lanceur de balle de défense (LBD), popularisé depuis 2016 par la police nationale. Du côté d'Orléans, une autre expérience de micros dans les rues « sensibles » est menée durant l'hiver 2021-2022 par une entreprise locale nommée Sensivic, intégrée dans un groupe baptisé Lorias, et hébergée par un incubateur numérique appelé Le Lab'O, le tout étant financé en partie par la région, la commune, et le département. La pomme ne tombe jamais loin de l'arbre.

D'autres communes travaillent en revanche avec de grandes sociétés internationales comme Thales (armement) ou Engie Ineo (cybersécurité et vidéosurveillance), ou encore Huawei, IBM, etc.[14]. Mais le point commun entre toutes ces initiatives locales semble être la nullité politique. Quand l'heure est à l'abandon des politiques publiques, sous la double injonction idéologique de la « réduction de la dette » et de la meilleure performance indiscutable de l'entreprise privée, les personnalités politiques – à tous les étages, nationaux, régionaux, et municipaux – investissent toute leur autorité et leur capacité d'action dans le seul domaine qui semble encore relever de façon légitime du bien public : « la sécurité ». Les maires paraissent résignés à l'idée de n'être

réélus que pour leur seule et unique capacité à mettre partout et toujours plus de police et de matériel de surveillance.

Devant la grande uniformité de ce désir de surveillance, et devant la grande dispersion de ses formes locales, le constat s'impose à la Quadrature : on ne pourra pas tout faire tout seul, il faut que d'autres s'y mettent aussi.

Et des autres, il y en a plein ! À Saint-Étienne, par exemple, les militants locaux se sont d'abord réunis dans un groupe appelé Serenicity-Google, car ils refusaient aussi l'implantation d'un « atelier Google » dans la ville, avant de se renommer Halte au contrôle numérique. À Dijon, Rennes, Amiens, Toulouse ou Lyon, des militants bien implantés et très au fait de ce qui se passe dans leur ville nous contactent pour parler de ces sujets. L'enjeu pour la Quadrature devient donc, très naturellement (parce que c'est dans sa logique depuis sa création), de se concentrer sur la fabrication des outils qui permettront aux groupes locaux de se rencontrer, et de partager des informations, des méthodes et de la motivation. On ne peut pas tout faire, mais on peut aider les autres à le faire ensemble.

Il suffit souvent de mettre en lumière des luttes qui existent déjà. Par exemple, il est impossible de parler de technopolice sans parler du projet sous-surveillance.net, qui s'est longtemps chargé de cartographier dans toute la France les caméras de surveillance, chaque ville ayant sa propre page.

Nous nous sommes inspirés de ce travail car, en lançant le tour de France du délire numérique et sécuritaire, la toute première chose qu'on imaginait, c'était une carte. Comme dans les albums d'Astérix, mais avec les projets sécuritaires de Thales et de Huawei à la place des camps romains de Petibonum et de Babaorum. Chacun peut cliquer sur le nom de sa ville et avoir aussitôt un résumé clair de la situation, avec des liens vers des fiches plus détaillées sur les projets, les acteurs locaux et les

entreprises, les techniques utilisées, et tous les documents bruts obtenus par « demande Cada »[15].

La « technocarte[16] » est un outil pratique pour les visiteurs du site, un point d'entrée accessible à toutes les curiosités – simple passant, militant, journaliste, chercheur – mais c'est aussi devenu un des aspects les plus spectaculaires de la campagne Technopolice pour celles et ceux qui l'alimentent au quotidien : « C'est un travail assez flippant, où l'on se rend compte du côté toile d'araignée, presque gangrenant de ces expérimentations et de ces techniques de surveillance », explique par exemple Martin Drago, un des piliers de la campagne, juriste à La Quadrature du Net de 2018 à 2021. L'infographie qui trace les liens de travail entre les entreprises et les collectivités locales renforce encore l'image de la toile d'araignée[17]…

Mais si la carte est un outil de navigation, de consultation des informations, le plus difficile est en amont, quand il s'agit de rassembler les énergies, de fouiller dans la presse et dans les sites spécialisés, dans la communication des entreprises et des communes, de lancer des « demandes Cada », d'organiser le travail pour éviter les doublons et les recherches inutiles, de dépouiller les documents reçus, de les analyser, de les synthétiser, puis de publier les fiches, d'écrire des articles, etc. Derrière la carte, il y a le travail collectif des bénévoles de la campagne Technopolice.

L'outil premier, par lequel les gens se rencontrent, c'est un forum[18] : ouvert à toutes et à tous, consultable par tout le monde, pour essayer de mutualiser les différentes luttes, échanger, s'informer aussi, se tenir au courant. On est loin des réseaux sociaux sophistiqués et des applications que le Web des GAFAM multiplie depuis bientôt quinze ans. Retour au Web *low tech* à l'ancienne : un forum, c'est ouvert, c'est simple, et c'est costaud. Tout le monde peut s'inscrire très vite, avec une adresse e-mail et un pseudonyme, et tout aussitôt lire, répondre, participer. Les messages sont classés par grandes catégories, « Projets et villes technopolicières » (l'entrée géographique), « Technologies et industries de surveillance » (l'entrée par les entreprises et par les techniques mises en œuvre :

vidéosurveillance, reconnaissance faciale, etc.), ou « Stratégies et formats de mobilisation » (comment lutter ensemble). Un espace est prévu pour les nouveaux venus qui veulent se présenter et lire les présentations des autres participants, et même une rubrique pour les discussions libres, qui n'entrent dans aucune catégorie ou qui n'auraient même aucun rapport avec le travail en cours. Tout l'intérêt du forum est de rester ouvert et transparent, pour que chacun puisse venir se renseigner, et trouver le plus vite possible une place, un rôle, une réponse ou quelque chose à faire pour aider.

Le site fournit aussi des packs de communication, des flyers, des affiches et des images à imprimer chez soi. Tous les textes écrits par la Quadrature ou le site Technopolice, ainsi que les images, sont publiés sous licence libre CC by-SA[19], qui permet la libre reproduction à la condition de créditer la source.

Le plus important, du point de vue de l'action efficace, se trouve sans doute dans la rubrique « Se mobiliser[20] ». Elle renvoie vers le forum, vers l'espace de rédaction collective des fiches de synthèse (un ensemble de pads baptisé le Carré[21]), vers la base de données des documents collectés, mais aussi, et surtout, vers la page des guides juridiques[22]. Ici, les bénévoles qui souhaitent contribuer à la campagne et documenter les pratiques de technopolice dans leur commune peuvent apprendre la base de la méthode de travail. D'abord, ils trouveront un guide pratique de la « demande Cada »[23] : quels documents demander, à qui, et comment. L'explication est très simple, même les novices peuvent se lancer le jour même. Enfin, la page des guides juridiques renvoie vers les textes de plusieurs recours en justice que nous avons écrits pour contester des dispositifs de technopolice : bien que ce soit un exercice qui s'adresse plutôt à des juristes, tout le monde est invité à s'emparer des moyens que la loi donne aux citoyens pour faire valoir leurs droits et défendre leurs libertés.

La campagne Technopolice est lancée de façon très officielle en septembre 2019. Une soirée est organisée à Nice, la ville où Christian Estrosi a voulu, sans grand succès :

– lancer « Reporty », une application de délation civique pour que les habitants de la ville dénoncent, avec la caméra de leur smartphone, les faits dont ils sont les témoins[24],

– tester la reconnaissance faciale dans la foule du carnaval de la ville,

– envisager la détection des émotions dans les transports publics de la ville « en vue de détecter d'éventuels mouvements de panique et de stress[25] » ou des passages à l'acte violents,

– obliger les lycéens à se soumettre à la reconnaissance faciale pour entrer dans leur lycée.

Un tel talent pour la surveillance et la surenchère technologique méritait au minimum un satisfecit, et désignait Nice comme la meilleure ville technopolicière de France. À tout seigneur tout honneur, la conférence de presse de lancement a donc lieu à Nice, avec les associations en compagnie desquelles nous déposons un recours au tribunal administratif contre l'expérience de reconnaissance à l'entrée des lycées. Un recours gagné, comme on l'a vu plus haut.

Avec un peu de recul, deux années après le lancement du site et de la campagne officielle, force est de reconnaître que notre idéal d'une lutte décentralisée, réseautée et disséminée dans toute la France est encore loin d'être atteint. Nous chapeautons encore le site et abattons 95 % du travail d'information, d'analyse, de cartographie, ou de communication. Mais il est difficile de mesurer combien nos analyses et nos cartographies sont diffusées ou reprises. Des discussions sur le forum se font sans nous, des échanges et des groupes locaux aussi. Et un mouvement Technopolice autonome s'est créé en Belgique ! *Last but not least*, le terme « technopolice » s'est fait une place dans la presse et dans le débat public, ce qui n'est pas la moindre des victoires…

« AH NON, PAS VOUS ! »

Deux mois après le lancement de la campagne, fin novembre 2019, nous partons joyeusement, sous une pluie fine et glaciale, pour une soirée de

tractage devant Paris Expo (un grand centre de congrès situé porte de Versailles à Paris), où se tient le 102e congrès de l'Association des maires de France. Depuis plusieurs mois nous voyons la reconnaissance faciale envisagée partout en France, en même temps que de grandes villes et des collectivités locales aux États-Unis prennent, avec un temps d'avance, des décisions démocratiques pour interdire la reconnaissance faciale policière sur leur territoire (c'est par exemple le cas de l'État de Californie, en octobre 2019[26]). Le tract que nous avons préparé pour les « maires de France » est une invitation très nette, d'abord à mener des politiques municipales plus intelligentes, plus sociales et moins sécuritaires, et ensuite à prendre publiquement position contre l'utilisation de la reconnaissance faciale policière.

Ce jeudi 21 novembre, la nuit est tombée tôt et la pluie est têtue. C'est le dernier jour du congrès annuel des maires, les plus pressés partent déjà attraper le train du retour, d'autres arrivent en bavardant, après avoir pris un dernier verre au buffet de clôture offert par l'organisation du congrès. À toutes et à tous nous tendons notre petit tract orange ou vert le plus joyeusement possible : « La Quadrature du Net ! Refusez la reconnaissance faciale ! » Beaucoup prennent le petit papier, quelques-uns le refusent avec un air pressé, comme on l'a tous fait au moins une fois devant les démarcheurs de rue, avec parfois un rapide échange de plaisanteries, « merci et bonne soirée », et enfin, bien sûr, quelquefois la discussion s'engage.

Un maire nous demande ce que nous avons contre la reconnaissance faciale, qui aide à lutter contre le terrorisme. Plusieurs affirment que la vidéosurveillance est souvent utile et donc parfaitement nécessaire. On répond avec autant de conviction mais avec la certitude inverse, on cite des chiffres, des études, en essayant d'entrouvrir une vision plus large de la société qu'on est en train de construire. Un maire d'une commune rurale explique, désolé, à l'abri d'un auvent, qu'il a dû faire installer trois caméras autour de la salle des fêtes de son village sous la pression des assureurs : après un cambriolage, les voleurs ayant emporté le matériel de la sono et de l'éclairage, l'assurance du bâtiment était soumise à

l'installation préalable des caméras. Un autre élu estime qu'avec la reconnaissance faciale on pourra enfin savoir qui pisse dans les rues. D'autres, enfin, plutôt des femmes d'ailleurs, manifestent un intérêt réel pour nos idées, et veulent savoir comment faire pour exprimer leur refus de la surveillance automatisée. Plusieurs nous demandent comment nous contacter plus tard.

Les discussions sont passionnantes, parce que dans cette coupe sociologique mince – les maires des communes de France encore présents à la clôture d'un congrès parisien un soir pluvieux de novembre –, on voit déjà tout un éventail de discours et de positions, on constate la prégnance de l'idéologie sécuritaire dominante, le ton d'évidence incontestable sur lequel elle s'exprime, et le peu de place laissé dans les imaginaires à la possibilité d'une société qui ne serait pas celle de la surveillance généralisée.

Il fait froid, on n'a presque plus de tracts, on envisage de lever le camp. Arrive un petit groupe pressé, au milieu duquel se trouve Gaël Perdriau, le maire de Saint-Étienne. On lui tend un tract, sa réponse fuse : « Ah non, pas vous ! » L'annulation des micros a dû lui rester en travers de la gorge.

LES CENT VISAGES DE LA RECONNAISSANCE FACIALE

L'année 2019 fut pour nous celle de la reconnaissance faciale. La technologie est partout, au point qu'on publie un article sur le sujet, en dehors de toute actualité précise, simplement pour poser quelques définitions et quelques pistes de réflexion sur le sujet[27] : distinction entre identification et authentification, nécessité de distinguer les différentes finalités des usages, saut anthropologique d'une société où le visage trahit la personne et la livre au pouvoir policier – on esquisse, on défriche, on découvre.

Pendant ce temps, autour de nous, la mise en place de la technologie s'accélère, dans un contexte social très tendu. Chaque samedi, les « gilets

jaunes » manifestent dans la France entière, et la majorité gouvernementale semble trouver secondaire que la police réprime durement les manifestations, au prix de mains ou d'yeux arrachés, quand la réalité de ces blessures atroces n'est pas tout simplement occultée par les grands médias, ou niée par les ministres et le chef de l'État lui-même. Dans un contexte où les luttes sociales sont criminalisées et matées par les armes (des armes « non létales », bien entendu), nous voyons la reconnaissance faciale s'imposer dans des domaines aussi divers que la vidéosurveillance, le ciblage publicitaire, les démarches administratives ou les contrôles policiers de routine. On découvre ce qui n'était d'ailleurs pas caché, parce que personne ne s'en était jamais offusqué : depuis 2012, les policiers peuvent utiliser les images de vidéosurveillance, les images des réseaux sociaux, ou les photos qu'ils prennent lors des manifestations ou des contrôles, et les comparer par reconnaissance faciale avec les photos enregistrées dans le TAJ.

Le TAJ, pour « traitement des antécédents judiciaires », est un énorme fichier de police dans lequel sont entassées, pêle-mêle, toutes les personnes avec qui la police a eu affaire durant ses enquêtes : mis en cause, complices éventuels, et bien sûr victimes. Si les policiers appliquaient la loi, ils devraient effacer de ce fichier les personnes dont la mise en cause n'a pas donné lieu à une condamnation judiciaire. Malheureusement, les procureurs le reconnaissent, personne ne veille à effacer ces données. Les photos et les noms s'accumulent donc dans le fichier pour vingt ans[28]. En 2018, le fichier TAJ comptait 18 millions de fiches et 8 millions de photos[29]. Or, la reconnaissance faciale est autorisée au sein du fichier TAJ[30].

En 2019, les policiers envoient 375 000 requêtes de reconnaissance faciale dans le TAJ. Plus de mille fois par jour, le fichier est interrogé pour tenter d'identifier des personnes dont on ne connaît que le visage sur une photo. Des délinquants ? Sûrement. Des personnes qui subissent un banal contrôle routier ? C'est fort probable. Des manifestants dans la rue ? C'est possible. C'est pourquoi nous publions en novembre 2019 un

article qui saisit justement la question sous cet angle : « La reconnaissance faciale des manifestants est déjà autorisée ».

Il n'existe (pour l'heure) aucune loi rendant explicitement possible la reconnaissance faciale des manifestants, mais cet article démontre pourtant, point par point, que la chose est techniquement et surtout légalement possible. Comment ? D'abord, comme on l'a vu, la reconnaissance faciale est une des fonctions disponibles du TAJ. Ensuite, parce que les policiers peuvent accéder depuis 2007 au fichier TES (pour « titres électroniques sécurisés »), qui rassemble depuis 2005 toutes les personnes ayant obtenu une carte d'identité ou un passeport biométriques obligatoires, et conserve depuis 2008 toutes les photos d'identité numérisées qui sont imprimées sur les pièces d'identité. Voilà qui ajoute quelques dizaines de millions de visages au grand vivier disponible pour la reconnaissance faciale de masse… L'article se termine en annonçant que nous avons envoyé au gouvernement une demande d'abrogation des fonctions de reconnaissance faciale dans le TAJ, qui serait ensuite formulée, en cas de refus, sous forme de recours devant le Conseil d'État. Sans surprise, le recours est déposé en août 2020[31]. En janvier 2022, le Conseil d'État n'a toujours pas rendu sa décision.

Autre porte d'entrée de la reconnaissance faciale : l'application Alicem, pour « application de lecture de l'identité d'un citoyen en mobilité ». Si vous ne la connaissez pas, c'est normal. Pour aller vite : les agences d'État ont développé, dans la logique du « guichet numérique », un système d'identifiant unique pour les services publics en ligne, nommé France Connect. Sur cette base s'appuie un « projet d'application pour prouver son identité en ligne » et cette application prototype s'appelait Alicem. Mais pour créer votre profil vérifié, l'application vous imposait de scanner la puce RFID de votre pièce d'identité numérique (qui contient votre photo d'identité), puis de vous photographier et de vous filmer avec votre smartphone, pour analyser les images par comparaison faciale.

De notre point de vue, ce genre de gadget banalise la reconnaissance faciale en laissant croire qu'elle est efficace, moderne et sûre, et en lui

donnant un rôle positif. Comment des personnes qui ont utilisé la reconnaissance faciale sur elles-mêmes de manière inoffensive et même rassurante pourraient-elles refuser ensuite de s'y soumettre dans la rue, quand des caméras « intelligentes » les dévisageront et les identifieront plusieurs fois par jour ? En juillet 2019, nous attaquons donc l'application Alicem devant le Conseil d'État[32]. Le droit précise bien que la biométrie doit être minimisée et utilisée seulement en cas de nécessité, c'est-à-dire lorsque aucune autre possibilité pratique ne permet d'atteindre le même but. Mais Alicem ne permet pas aux personnes qui veulent créer une identité numérique de le faire sans se soumettre à la reconnaissance faciale. Même la CNIL est d'accord avec nous et publie un avis opposé à l'expérimentation gouvernementale : « Le consentement au traitement des données biométriques ne peut être regardé comme libre et comme étant par suite susceptible de lever l'interdiction posée par l'article 9.1 du RGPD. » Malgré cela et comme souvent, le gouvernement n'a pas modifié son décret en le publiant. Il s'agit donc bien ici de normaliser la reconnaissance faciale comme outil d'identification, en passant outre la seule condition qui devrait être acceptable pour son utilisation : notre consentement libre et explicite. Le Conseil d'État rejette sèchement notre recours en novembre 2020, et nous concède seulement la nécessité de proposer un autre moyen d'identification que la reconnaissance faciale… qui semble pour l'instant enterrée dans le projet Alicem.

Mais la reconnaissance faciale, on vous le dit, est partout[33] : si vous passez par un aéroport dans les semaines qui viennent, on vous proposera peut-être de passer par un portique de reconnaissance faciale, mais seulement avec votre consentement explicite – et vous pourrez refuser. Il existe deux projets expérimentaux, PARAFE (pour les voyageurs hors espace Schengen) et MONA (pour les voyages à l'intérieur de l'Union européenne), et tous deux sont menés par Idemia, une société française spécialiste des techniques de l'identité biométrique. La CNIL a validé les deux expérimentations, parce qu'elles sont soumises au consentement explicite des participants. Mais comme avec Alicem, nous craignons que

la banalisation de ce type de gadgets ludiques, qui « fluidifient » la vie des personnes les plus aisées, ne masque dans les imaginaires la réalité d'une reconnaissance faciale de surveillance, massive, subie et beaucoup moins « cool ».

DRONES POLICIERS : UN ŒIL VOLANT

Autre découverte notable de la campagne Technopolice en 2019 : des drones policiers volent déjà au-dessus de nos têtes. On l'a appris à la faveur d'une « demande Cada » adressée à la ville d'Istres, dans les Bouches-du-Rhône, à la suite de la lecture d'un article paru dans *Le Monde*[34]. Dans les documents obtenus, la ville reconnaît sans difficulté que les deux drones vidéo de très haute définition qu'elle a achetés ont servi, pour 73 % de leur temps de vol, à surveiller des manifestations, en complément des quatre-vingt-dix caméras fixes déjà installées dans les rues de la ville[35]…

C'est un point capital des tendances actuelles de la technopolice : la multiplication des caméras. En même temps que l'intelligence artificielle pour analyser les images se développe et s'implante partout, les sources d'images se multiplient dans toutes les directions. On installe toujours plus de caméras fixes de vidéosurveillance, mais aussi des caméras personnelles portées par les policiers et les gendarmes, et plus haut, les drones. Voilà pourquoi nous n'hésitons pas à parler de contrôle total de l'espace public : des caméras partout, et qui peuvent se déplacer, et une intelligence artificielle au sol qui peut tout analyser, et même appliquer de la reconnaissance faciale. Voilà l'état des lieux à la fin de 2019. L'année 2020, à la faveur de la crise sanitaire, accélérera cette tendance d'une manière stupéfiante. Mais comme disait Rudyard Kipling, c'est une autre histoire…

ORGANISER LES FUITES

Les « demandes Cada » sont une source généreuse de documents et d'informations. Mais elles ont l'inconvénient de ne concerner que les administrations publiques. Que se passe-t-il, que se prépare-t-il dans le secret des entreprises ? Que manigancent les partis et les états-majors politiques ? Pour le savoir, il faut bénéficier de fuites, d'indiscrétions, de confidences. On peut apprendre beaucoup de choses en fréquentant les personnes chargées de prendre les décisions, c'est un travail de journaliste. Mais comment accueillir les informations vraiment sensibles ? Si une personne employée dans une entreprise de la surveillance, ou dans un ministère, entendait parler d'une chose vraiment grave, oserait-elle la rendre publique ? Le risque peut retenir les plus lucides, surtout quand on voit le sort réservé dans la loi, à dessein, aux lanceurs et aux lanceuses d'alerte. C'est pourquoi nous avons mis en place un dépôt sécurisé pour que les personnes en possession de documents sensibles puissent venir les déposer de manière anonyme. Aucun besoin d'être ingénieur en informatique, une page du site Technopolice explique pas à pas comment faire : https://technopolice.fr/leak/.

4. QUAND LE NUMÉRIQUE MENACE LES LIBERTÉS

L'histoire de la Quadrature est peut-être – et c'est sans doute le fil de ce livre – celle de la prise de conscience douloureuse que le numérique et le Web, qu'on avait crus émancipateurs, progressistes et humanistes par nature, dans leur conception même, se sont retournés contre nous comme outils de surveillance, de censure, de manipulation des personnes et de gavage publicitaire. Ce n'est pas l'histoire d'une naïveté : le Web mondial a aussi donné à l'humanité une nouvelle puissance et une nouvelle conscience d'elle-même, sur ce point, les rêveurs ne se sont pas trompés. Le réseau mondial a bel et bien bouleversé l'éducation, les échanges savants et les échanges quotidiens, révolutionné l'organisation politique en donnant un moyen d'expression aux sans-voix, et changé mille aspects de nos vies pour le meilleur.

Mais ce que nous n'avions pas envisagé – parce que, selon nous, ce n'était désirable pour personne –, c'est que le pouvoir économique et politique retournerait cet outil révolutionnaire contre ceux qui l'utilisent, pour perpétuer l'ordre existant. On pense en particulier à l'utilisation des réseaux (Web et téléphoniques) pour contrôler, contraindre, et surveiller les populations : à la fois surveiller tout le monde, et surveiller chacun avec une finesse inégalée jusqu'à présent. Ce que l'ère numérique offre de nouveau sur le plan historique, c'est aussi un contrôle politique sans précédent dans l'histoire. Le numérique est à ce titre vecteur de menaces très concrètes sur les libertés publiques, et la période 2018-2019 est généreuse en exemples. On l'a vu, la technopolice fait son trou et oblige

la Quadrature à quitter sa « zone de confort » et son champ d'étude habituel. Mais même dans le champ bien familier des libertés sur Internet, nous faisons face à de nouveaux assauts, et à de nouvelles reculades.

« LOI *FAKE NEWS* » : LA CENSURE QUI FAIT PSCHITT

Si on devait classer ces mesures par degré croissant de nocivité, on commencerait sans doute par la loi « contre les *fake news* », tellement mal fichue qu'elle en devient presque rigolote. Pour être honnête, il faut bien reconnaître que la Quadrature ne lui a pas consacré beaucoup de temps ni d'énergie, tant il paraissait évident dès le départ que le projet s'écroulerait sur lui-même. Malgré tout, cette loi dit évidemment quelque chose de l'état d'esprit des gouvernants qui l'ont imaginée, et des moyens qu'ils se donnent.

En janvier 2018, dans ses vœux à la presse[1], le président de la République Emmanuel Macron dresse un constat : « Au-delà même des tentations illibérales, c'est le modèle du métier de journaliste qui est aujourd'hui remis en cause ou, pour le dire plus justement, dévoyé car nous vivons l'irruption dans le champ médiatique des fausses nouvelles, les *fake news*, comme on le dit dans le monde anglo-saxon, et des médias qui les propagent. »

À quoi pense-t-il ? Difficile de le dire avec précision… Peut-être visait-il l'apparition dans le paysage francophone de médias russes financés par les partisans de Poutine (la chaîne RT France est lancée en décembre 2017) : « Entre le complotisme et le populisme, le combat est en effet commun, il est de saper toute confiance dans le jeu démocratique, d'y faire apercevoir un jeu de dupe, une valse de faux-semblants et c'est vous, c'est nous qui sommes visés par cette stratégie au profit d'une propagande déterminée. Cette montée des fausses nouvelles est aujourd'hui […] utilisée par des puissances qui s'amusent en quelque sorte des faiblesses de la démocratie, de son ouverture extrême, de son

incapacité à trier, à hiérarchiser, à reconnaître au fond une forme d'autorité. »

Peut-être craint-il de voir arriver en France, alors que Donald Trump est président des États-Unis depuis un an déjà, les méthodes médiatiques qui ont porté le promoteur immobilier new-yorkais au poste d'homme le plus puissant de monde, ou celles qui ont amené la majorité des Britanniques à voter en faveur du « Brexit » : « Entre ces machines à répandre les fausses nouvelles et les médias professionnels, la porosité menace. Des barrières ont été érigées mais les campagnes présidentielles d'à peu près toutes les démocraties contemporaines ont montré la faiblesse de celles-ci et notre incapacité collective à apporter des réponses qui sont à la hauteur aujourd'hui des menaces. »

En tout cas, Donald Trump est bien à l'origine de l'expression *fake news.* Sa campagne électorale, dans la deuxième moitié de l'année 2015, a consisté en grande partie à balancer dans le débat public des énormités qui polarisaient les discussions et qui monopolisaient l'attention médiatique. Et il avait pris l'habitude de répondre, quand la presse lui objectait un fait vérifiable, un chiffre, ou un raisonnement : *« This is fake news »* (une fausse information, une invention, un mensonge). À un reporter de CNN qui le contredisait en conférence de presse, il lança même : *« You are fake news! »* Trump revendiquait sa propre lecture du monde, allant jusqu'à parler de « vérité alternative », fondée même sur des « faits alternatifs ». Adieu la vérité objective, au revoir la possibilité d'un monde commun, il ne reste plus que des vérités de points de vue, et la bataille électorale n'est plus qu'une compétition d'affirmations sans arbitre et sans arbitrage possible. Créé par un menteur professionnel pour désigner les propos de ses détracteurs, le terme a rapidement changé de sens et, quand Emmanuel Macron l'utilise à son tour un an plus tard, c'est pour désigner, à l'inverse, les mensonges des propagandistes et des affabulateurs cyniques, et pour défendre la presse *mainstream* qui était l'ennemi désigné de Trump. Et d'après vous, comment circulent ces fausses nouvelles qui menacent la vraie presse et la démocratie libérale ? Par Internet.

Le discours d'Emmanuel Macron ne se limite donc pas à dénoncer un danger, ni à exhorter les journalistes à lutter avec leurs propres moyens contre les *fake news*. Il annonce aussi une prochaine loi pour réglementer « les plateformes Internet » : « C'est pourquoi j'ai décidé que nous allions faire évoluer notre dispositif juridique pour protéger la vie démocratique de ces fausses nouvelles. Un texte de loi sera prochainement déposé à ce sujet. En période électorale, sur les plateformes Internet, les contenus n'auront plus tout à fait les mêmes règles. [...] Les plateformes se verront ainsi imposer des obligations de transparence accrue sur tous les contenus sponsorisés afin de rendre publique l'identité des annonceurs et de ceux qui les contrôlent, mais aussi de limiter les montants consacrés à ces contenus. [...] En cas de propagation d'une fausse nouvelle, il sera possible de saisir le juge à travers une nouvelle action en référé permettant le cas échéant de supprimer le contenu mis en cause, de déréférencer le site, de fermer le compte utilisateur concerné, voire de bloquer l'accès au site Internet. »

Nous retrouvons de vieilles lunes : la bonne vieille incrimination du Web et la bonne vieille censure sont toujours là. Défraîchies, décaties, déplumées, mais toujours debout. Elles vont servir encore une fois. Quand les causes sont lointaines, attaquons-nous aux effets proches…

Le titre de l'article que nous publions le lendemain du discours à la presse, le 4 janvier 2018, annonce la couleur : « Derrière l'effet d'annonce, Macron esquive le vrai débat[2] ». Quel est-il, le vrai débat ? Selon nous, Macron se trompe en chargeant les plateformes géantes (YouTube, Facebook, Twitter, etc.) de faire le ménage parmi les sources de désinformation dont elles ne seraient que le lieu de passage et les premières victimes. En réalité, dit notre article, le régime de la désinformation, du clash, de la polarisation aux extrêmes et de l'invective permanente est précisément créé par l'économie de ces plateformes. Elles cherchent à retenir l'attention des visiteurs, leur soumettent donc de préférence les contenus polémiques qui suscitent le plus grand « engagement », et retiennent les gens dans les filets des réseaux sociaux, sous perfusion de publicités et de contenus « sponsorisés » (qu'ils soient

marchands ou politiques). Donald Trump et les *fake news* sont les enfants monstrueux de l'économie de l'attention et du ciblage publicitaire.

Par ailleurs, souligne l'article, les lois sur la presse de 1881 et la loi pour la confiance dans l'économie numérique de 2004 (LCEN) donnent déjà à la police et aux juges tous les outils nécessaires pour faire supprimer un contenu illicite ou dommageable.

La « loi *Fake news* » promise par Emmanuel Macron s'intitule en réalité « loi relative à la lutte contre la manipulation de l'information ». Elle est adoptée en novembre 2018, et ne s'applique que dans une période de trois mois avant chaque élection à valeur nationale. En 2019, après la campagne des élections européennes, les juges n'ont été saisis qu'une seule fois sur le fondement de cette loi : c'était à l'initiative de deux parlementaires qui voulaient démontrer son inanité[3]…

LOI AVIA « CONTRE LA HAINE EN LIGNE » (FÉVRIER-DÉCEMBRE 2 1)

Plus sérieuse et plus grave, dans l'ordre des atteintes à la liberté en ligne, la loi Avia « contre la haine » nous occupe en revanche pendant une bonne partie de l'année 2019. C'est pour nous une année forte en émotions (en particulier l'angoisse), puisque nous travaillons sur la campagne Technopolice et sur le règlement européen antiterroriste, dans lequel la France en particulier pousse des dispositions liberticides très fortes, comme la censure de sites Web en une heure et sans juge.

Le 14 février 2019, Cédric O (secrétaire d'État au numérique), Marlène Schiappa (secrétaire d'État pour l'égalité femmes-hommes) et Lætitia Avia (députée de la majorité LREM) tiennent une conférence de presse à Bercy pour présenter leur stratégie de lutte « contre la haine en ligne ». Nous sommes présents dans la salle, ce qui nous permet de publier une réaction le jour même : « Mahjoubi et Schiappa croient lutter contre la haine en méprisant le droit européen[4] ». Un titre sévère, mais juste.

Que proposent les stratèges de la « lutte contre la haine » ? Leurs solutions contre les discours de haine sont avant tout, voire exclusivement, technologiques : un bouton pour signaler rapidement les nouveaux contenus illicites, des robots pour les bloquer en masse, et des obligations de censure qui reposent sur les hébergeurs.

D'abord, cette stratégie recycle l'existant. Le « bouton » pour signaler les contenus haineux est prévu depuis 2004 par la loi pour la confiance dans l'économie numérique (LCEN). Le non-respect de cette mesure est même puni d'un an de prison et de 75 000 euros d'amende. Mais depuis sa promulgation, les gouvernements n'ont jamais jugé opportun de la faire appliquer. Pourquoi ? Sans doute parce que les politiques savent – les acteurs du domaine le leur ont expliqué – que cette mesure est inapplicable : les hébergeurs n'auraient pas les moyens matériels et humains de traiter les signalements que cela générerait. Sortir la mesure de la cave, c'est donc faire preuve d'une absence de réalisme, ou d'une solide démagogie. D'autres moyens existent, par ailleurs, comme la plateforme d'harmonisation, d'analyse, de recoupement et d'orientation des signalements (Pharos), qui dépend de la police[5].

Ensuite, les stratèges chantent les louanges des filtres automatiques mis en place sur des plateformes comme Facebook et YouTube (Google), capables de supprimer en masse des contenus illicites, soit parce qu'ils ont déjà été repérés (une vidéo ou une photo par exemple), soit parce qu'ils contiennent des éléments facilement repérables (certains mots par exemple). Ces « robots » logiciels actifs sur les serveurs ont été développés à l'origine pour reconnaître les œuvres protégées par des droits d'auteur et les supprimer (des films ou des morceaux de musique). Sur YouTube, où ils fonctionnent quotidiennement, ils bloquent des vidéos en nombre et avec de nombreux « dégâts collatéraux » : on a vu par exemple une vidéo diffusée sur YouTube se trouver brutalement censurée, parce qu'une chaîne de télévision en avait parlé et diffusé des extraits ; mais les émissions de la chaîne en question étant elles aussi protégées par les robots, la vidéo d'origine était perçue par ceux-ci comme un piratage de l'émission de télévision…

Par ailleurs, le fait de confier la surveillance et la censure du Web aux GAFAM ne cesse de nous étonner. Et pourtant, c'est dans la suite logique de ce que nous constatons depuis plusieurs années déjà, et qui est à l'œuvre aussi dans le règlement européen contre la propagande terroriste : demander à quelques interlocuteurs fiables et reconnus d'effectuer le travail, quand bien même il s'agirait de grandes entreprises privées américaines. Pour des gouvernants pragmatiques, il est raisonnable de prendre en compte les forces en présence et le Web tel qu'il est. Pour nous, qui voulons le décentraliser et l'arracher des mains des GAFAM, c'est un aveu d'échec.

Le « règlement Terro » demande aux hébergeurs de retirer les contenus terroristes en une heure. La loi Avia demande aux hébergeurs de retirer les contenus haineux en 24 heures. C'est plus long, mais ce n'est pas mieux. Seules de très grosses structures ont les moyens techniques et humains de répondre à de telles requêtes dans un délai aussi court. Seuls les GAFAM peuvent le faire, les petits deviendront leurs clients et leur délégueront le travail, ou leur achèteront leurs outils. Comme le manquement est sévèrement puni (l'amende pouvant s'élever à 4 % du chiffre d'affaires annuel), les GAFAM appliqueront par prudence un filtrage préalable sévère, qui se répercutera aussitôt chez les petits qu'ils fournissent en instruments de censure. Résultat : un Web uniformisé, édulcoré, sans saveur et censuré.

Contre cette volonté de confier la censure des contenus aux grandes plateformes, nous avons un allié de circonstance inattendu : le ministère de la Justice. Dans une circulaire publiée en avril 2019[6], il appelle en effet à recourir davantage au juge pour lutter contre la haine en ligne et dénonce, l'« usage abusif » pouvant être fait des « dispositions permettant d'engager la responsabilité des acteurs d'Internet ». Alors que le gouvernement propose avec la loi Avia de contourner le juge pour gagner en « efficacité », la circulaire ministérielle constate que les procureurs saisissent bien trop peu la justice dans ces affaires…

Enfin, nos stratèges nationaux réactivent le fantasme de « la fin de l'anonymat sur Internet ». On peut leur objecter que l'anonymat n'existe

pas : les hébergeurs connaissent les adresses IP des internautes, et les FAI connaissent leur nom. Mais les mesures qu'ils proposent sont en contradiction directe avec le droit européen : depuis des années, la France impose aux fournisseurs d'accès à Internet (FAI), aux hébergeurs et aux opérateurs téléphoniques de conserver les données de connexion de tous les utilisateurs pendant un an, alors que le droit européen limite cette conservation de données à la fois en étendue, et dans le temps. Ce point est d'ailleurs à l'origine de l'un de nos plus importants contentieux.

LA CONSERVATION ILLÉGALE DES DONNÉES DE CONNEXION

L'histoire commence en 2015, avec l'adoption de la loi Renseignement. Dans un contexte de terrorisme exacerbé, entre l'assassinat de la rédaction de *Charlie Hebdo* et les attentats coordonnés du 13 novembre 2015, elle donne de larges pouvoirs de surveillance aux services de renseignement, et leur ouvre en grand l'accès aux données de connexion collectées par les opérateurs télécoms français (opérateurs téléphoniques et FAI). Par ailleurs, la loi française oblige depuis 2011 les opérateurs à conserver pendant une durée d'un an toutes les « données de connexion » de leurs utilisateurs, ce qu'on appelle aussi les « métadonnées ». Non pas le contenu de vos conversations, mais leur description technique : tel abonné a envoyé à telle abonnée un SMS de tant de caractères à telle heure, telle abonnée a téléphoné à tel abonné entre telle heure et telle heure, etc. Concernant le Web, les opérateurs et les hébergeurs sont obligés de conserver l'historique des pages consultées, à partir de quelle adresse IP, etc. Or, la loi européenne n'autorise pas une telle collecte de données, ni en masse, ni pour une telle durée. Et non, ce n'est évidemment pas parce que l'Union européenne, pas plus que la Quadrature, voudrait protéger les terroristes – l'idée est absurde et inutilement insultante pour l'intelligence de celui qui la profère.

La Cour de justice de l'Union européenne (CJUE) avait invalidé en 2014 une directive européenne de 2006 précisément pour cette raison :

elle autorisait une collecte de données trop large, trop peu ciblée, et disproportionnée dans son atteinte à la vie privée et à la liberté d'expression des citoyens, en regard de sa finalité avouée. Il faut lire en creux les reproches formulés par la CJUE : « […] ladite directive ne requiert aucune relation entre les données dont la conservation est prévue et une menace pour la sécurité publique et, notamment, elle n'est pas limitée à une conservation portant soit sur des données afférentes à une période temporelle et/ou une zone géographique déterminée et/ou sur un cercle de personnes données susceptibles d'être mêlées d'une manière ou d'une autre à une infraction grave, soit sur des personnes qui pourraient, pour d'autres motifs, contribuer, par la conservation de leurs données, à la prévention, à la détection ou à la poursuite d'infractions graves. »

En d'autres termes, surveiller tout le monde pour attraper des criminels, c'est illégal. Il faut cibler les gens qu'on surveille, dans l'espace et dans le temps, et motiver la surveillance : « Les dérogations à la protection des données à caractère personnel et les limitations de celle-ci doivent s'opérer dans les limites du strict nécessaire[7]. »

À nos yeux, la collecte et la conservation des données de connexion de toute la population française pendant un an tombent, pour des raisons similaires, dans la même illégalité. Nous attaquons donc devant le Conseil d'État (d'une part) les décrets d'applications de la loi Renseignement, et (d'autre part) la conservation des données, sur la base du jugement de la CJUE. Et nous demandons au Conseil d'État de demander formellement à la CJUE si l'obligation française de conservation des données est conforme ou non au droit européen.

Tout cela est très lent. Nous déposons nos recours en septembre 2015. Le Conseil d'État les examine en audience en juillet 2018[8], et renvoie enfin la question à la CJUE. L'audience devant la CJUE se tient les 9 et 10 septembre 2019[9]. On fait le voyage pour accompagner et soutenir Alexis Fitzjean, avocat et membre de la Quadrature, qui défend brillamment notre recours devant les juges européens. Un grand moment collectif. On n'a jamais plaidé aussi haut, et après autant d'attente, sur une affaire aussi grosse : la Quadrature contre Premier ministre, garde

des Sceaux, ministre de la Justice, ministre de l'Intérieur et ministre des Armées, ça n'arrive pas tous les jours. La cour rendra sa décision en octobre 2020 – nous y reviendrons.

ÉLABORATION DIFFICILE DE LA LOI AVIA

Mais revenons à la loi « contre la haine en ligne » ! La proposition de loi est présentée le 20 mars 2019 par Lætitia Avia. Elle est soutenue par un certain nombre d'associations d'aide aux victimes de discriminations (SOS Racisme, SOS Homophobie, Licra, etc.), qui souhaitent évidemment et à bon droit que le harcèlement en ligne soit réprimé, mais sans se poser les mêmes questions que nous, à la Quadrature.

Nous faisions pourtant partie de la quinzaine d'associations qui ont été auditionnées par les rédacteurs et les rédactrices de la loi. On a dit ce qu'on sait, et ce qu'on n'a jamais cessé de dire : le danger de la censure automatisée, le danger de la censure qui contourne les juges et confie le pouvoir à la police et aux entreprises privées, le danger de la censure administrative et policière qui peut être instrumentalisée par le pouvoir en place pour exercer une censure politique, etc. On nous a ri au nez : il s'agit seulement de supprimer des propos antisémites, homophobes, et de protéger des enfants harcelés. Oui, répondons-nous, mais pour cela il existe déjà des instruments juridiques et policiers, des juges, des procédures, et il n'est pas nécessaire de ratisser le Web avec des robots censeurs confiés à l'appréciation de Facebook et de Google. Rien n'y fait, tout se retrouve tel quel dans la loi Avia.

Pendant des mois, nous publions des articles et des tribunes pour dénoncer l'absurdité et les dangers de ces mesures. Nous dénonçons la possibilité d'une censure politique aux ordres du gouvernement en place : un risque réel alors que nous avons l'exemple d'une demande policière ridicule pour supprimer une caricature de Macron[10], et qu'on se trouve en plein mouvement des « gilets jaunes » que le gouvernement et les chaînes d'information en continu assimilent volontiers à des terroristes. On

rappelle les échecs des filtres des GAFAM : de l'aveu même de Facebook, la vidéo de la tuerie islamophobe de Christchurch, en Nouvelle-Zélande, le 15 mars 2019, avait été partagée 1,5 million de fois, et les robots filtreurs de Facebook en avaient laissé passer 300 000 copies… Sous le régime de la loi Avia, il aurait quasiment fallu fermer Facebook dans les 24 heures[11].

On produit des analyses juridiques, adaptées après chaque vote, pour donner des arguments de travail aux parlementaires. On dit et on redit ce que tous les professionnels du secteur expliquent : les algorithmes de recommandation des plateformes (ceux de Facebook et YouTube en tête) conduisent les internautes de contenu polémique en contenu plus polémique encore, car l'économie publicitaire de ces entreprises exige que les gens restent, le plus longtemps possible, présents sur la page, captifs de la plateforme. Vouloir légiférer contre la haine en ligne sans prendre en compte la nocivité sociale de ce modèle de rentabilité exclusivement économique, c'est fournir un travail inutile.

Dernière aberration : la loi Avia prévoit une autorité de contrôle, et plutôt que la CNIL ou un organisme ad hoc qui aurait l'intelligence et la connaissance de la réalité du Web, elle désigne le bon vieux Conseil supérieur de l'audiovisuel (CSA), rebaptisé pour l'occasion en Arcom : Autorité de régulation de la communication audiovisuelle et numérique. Pourquoi est-ce un problème ? Parce que le CSA a l'habitude de parler avec des chaînes émettrices et centralisées[12]. Aborder le Web sous cet angle, c'est forcément retomber sur les GAFAM et les plateformes géantes comme seuls interlocuteurs possibles pour « réguler le Web[13] ». Or, contre la « mise en silo » et contre la centralisation du Web par des plateformes toxiques, nous voyons d'autres solutions que le renforcement du centralisme… La première de ces solutions s'appelle « l'interopérabilité ».

L'INTEROPÉRABILITÉ CONTRE LA MISE EN SILO DU WEB

Que reproche-t-on aux grandes plateformes comme Facebook ou YouTube ? Principalement de monopoliser l'attention et le trafic du Web, au détriment de sa diversité et de sa résistance, en employant des moyens déloyaux et toxiques pour les personnes et pour les sociétés. Rien que ça. Les algorithmes de recommandations, conçus pour proposer les contenus à plus fort « engagement » émotionnel, c'est-à-dire concrètement les plus polémiques et les plus choquants, favorisent les discours politiques d'antagonisme plutôt que d'adhésion. Le pistage et le ciblage publicitaires enferment aussi les utilisateurs dans la confirmation en spirale de leur propre point de vue. Sur Instagram, les jeunes gens sont confrontés de manière obsessionnelle à des représentations irréalistes du corps et du bonheur matériel, et sont surexposés à la dépression et à la haine d'eux-mêmes. Voilà pour la toxicité sociale.

Mais le Web lui-même pâtit de cette nouvelle centralisation. On n'y circule plus en suivant des liens, dans une errance d'affinités qui traverse la Toile et trace des randonnées, des escapades, des points de fuite et de découverte, mais en rayonnant toujours depuis le centre qu'est devenu le réseau social, dans un va-et-vient permanent entre cet unique foyer et de minuscules portions du reste du Web. La plupart des réseaux sociaux « encapsulent » même les sites liés dans leur propre interface, de telle sorte qu'on ne quitte parfois même plus la plateforme pour aller voir une vidéo ou lire un article de presse.

Ce phénomène a « recentralisé » le Web, pourtant imaginé sur la logique inverse de la navigation. Les internautes que nous sommes se retrouvent « mis en silo » dans leur réseau social d'élection, et exploités par celui-ci comme une matière première qui sécrète des données de ciblage et ingurgite en retour de la publicité, avec tous les effets néfastes dont on a déjà parlé. Les plateformes ont su, avec des inventions de design et des fonctions astucieuses, préempter la culture communautaire du Web, et, renonçant peu à peu aux standards techniques qui permettaient de communiquer d'une plateforme à l'autre, ont enfermé leurs utilisateurs[14]. Il est très difficile de quitter une plateforme sans perdre le contact avec les personnes rencontrées, souvent sous

pseudonyme, par l'intermédiaire de la plateforme. C'est un renoncement qui coûte, et qui retient les utilisateurs.

Comment abattre ces murs ? Comment ouvrir ces enclos ? En obligeant les grandes plateformes à l'interopérabilité. Il s'agit d'une obligation technique : les contenus publiés sur la plateforme A doivent être lisibles sur la plateforme B. Comment une telle chose est-elle possible ? Il faut que les deux plateformes utilisent les mêmes standards techniques de publication, et que leurs API[15] soient ouvertes. La chose n'a rien d'extraordinaire : si un utilisateur de Gmail peut envoyer un e-mail à un utilisateur de Protonmail, c'est bien parce que les deux services utilisent un protocole unifié.

Non seulement la chose est possible, mais elle existe déjà. Le standard ActivityPub, par exemple, permet depuis 2018 de construire des réseaux sociaux interopérables, parce que tout le monde utilise des critères communs pour mettre en forme les informations publiées : si votre voisin diffuse ses données sous la même forme que vous, vous pouvez très facilement les publier dans votre interface. Des services distincts, des « instances », peuvent donc coexister et entrer en relation sans que l'un dévore l'autre, ou se renferme sur lui-même (et ses utilisateurs avec lui). Par exemple, le réseau Mastodon, jumeau de Twitter dans son apparence et dans ses fonctions, est fondé sur ActivityPub, et fonctionne par « instances » : chaque service peut choisir de se « fédérer » ou non avec d'autres instances pour échanger des messages et mettre ses utilisateurs en relation. Si Twitter devenait interopérable et adoptait aussi ActivityPub, les utilisateurs de Mastodon pourraient échanger avec eux.

Cette logique de la construction de nouveaux univers par fédération d'instances est très forte, on parle même de « fédivers » (ou *fediverse* en anglais). La rupture ou l'adhésion entre les instances n'est plus une chose imposée, mais un choix électif et politique : une instance peut à tout moment rompre le lien d'échange avec une autre, si elle considère par exemple que ses membres ont un comportement hostile.

Le reproche qui nous est souvent fait, quand nous faisons la promotion de ces scénarios d'interopérabilité, c'est de favoriser « le communautarisme ». Laissons de côté les insinuations misérables « d'islamo-gauchisme », ou de tout ce que le mot « communautarisme » peut recouvrir comme non-dit xénophobe, et intéressons-nous sérieusement au problème.

Oui, c'est vrai, une instance aura tendance à se former et à se regrouper autour d'un intérêt commun, au détriment des autres. Mais cela ne suffit pas à définir un « communautarisme » quelconque, ou alors toutes les associations de pétanque et de philatélie sont « communautaristes ». Le choix de couper les liens avec une autre instance signifie-t-il un refus du dialogue, de l'échange, un péril pour la démocratie et une atteinte à la liberté d'expression ? Là encore, il faut arrêter de se bercer de mots. La liberté d'expression est un droit garanti par l'État, qui s'engage à ne pas empêcher l'expression des idées, mis à part quelques exceptions bien connues d'incitations délibérées à la haine (racisme, homophobie, etc.). Mais la liberté d'expression n'a jamais été, et n'est en aucun cas une obligation de s'infliger la fréquentation de personnes désagréables ou d'écouter leurs discours, et encore moins de subir leur harcèlement.

Sur Twitter, par exemple, tout le monde se croise dans le même espace – homosexuels et homophobes, racistes et personnes racisées, etc. – et les « raids » des uns chez les autres sont des phénomènes quotidiens, dans une ambiance d'hostilité et de surenchère permanentes dont on a déjà vu qu'elles sont la fatalité logique et le carburant internes des plateformes unifiées. Si les uns et les autres discutent sur des instances distinctes, la fréquentation n'est plus imposée. Et si une instance a une attitude hostile envers une autre, elle peut être « bloquée ». À l'inverse, rien n'empêche une personne d'en suivre une autre sur une autre instance, même non fédérée, à condition qu'elle ne soit pas « bloquée ». En d'autres termes : chacun choisit avec qui il veut parler, et ne subit plus, ni une audience infinie et potentiellement hostile, ni l'arbitraire algorithmique des recommandations et des contenus imposés.

Au moment de la préparation de la loi Avia, lors de notre audition, nous avons parlé de l'interopérabilité pour casser les logiques de harcèlement en ligne. Mme Avia l'a refusée, en évoquant une solution lâche. Elle tenait beaucoup à l'image d'une cour d'école : si un enfant est harcelé pendant la récréation, est-il responsable de conseiller aux parents de changer d'école ? Ce à quoi nous répondons : est-il responsable de laisser l'enfant dans une école qui organise et couvre le harcèlement scolaire ?

Il est possible d'ouvrir les plateformes, et il est temps de le faire. C'est une idée que nous poussons autant que possible partout où l'on nous consulte, en rédigeant des amendements en ce sens chaque fois que les lois le permettent. Nous avons d'ailleurs réuni plus de soixante-quinze associations et structures du logiciel libre autour d'une lettre ouverte pour promouvoir l'interopérabilité [16].

L'idée a fini par être discutée au niveau européen[17] en 2022, dans le *Digital Services Act* (DSA) et le *Digital Markets Act* (DMA). La Commission et le Parlement ont introduit une obligation d'interopérabilité pour les réseaux sociaux et les messageries interpersonnelles. Mais pour Cédric O, secrétaire d'État français au numérique, ce choix est « excessivement agressif pour le modèle économique des grandes plateformes ». Au premier semestre 2022, profitant de la présidence française du Conseil de l'Union européenne, la France s'oppose alors à toute obligation, et la négociation aboutit à l'abandon de l'interopérabilité pour les réseaux sociaux et réduit à presque rien l'obligation faite aux messageries. Deux pas en avant, un pas et demi en arrière.

AGGRAVATION ET CENSURE DE LA LOI AVIA

En France, le texte de la loi Avia évolue au fil des discussions dans les deux assemblées, par le jeu des amendements. Mais de notre point de vue, c'est pour aller toujours vers le pire. Et le jeu parlementaire de la

navette entre l'Assemblée nationale (acquise par définition à la majorité gouvernementale) et le Sénat (dominé par l'opposition de droite) ne nous épargne pas en matière de retournements et de coups de théâtre. Le 11 décembre 2019[18], le Sénat supprime dans l'article 1er l'obligation de retrait des contenus signalés en 24 heures. Le 18 décembre, le même Sénat réintroduit cette mesure dans l'article 2[19]… En janvier, on titre même un de nos articles avec les mots « coup d'État[20] ». Le gouvernement vient d'introduire de force dans le projet de loi « contre la haine » la pire mesure du règlement Terro qu'il soutient par ailleurs sur le plan européen, c'est-à-dire le retrait en une heure des propos faisant l'apologie du terrorisme. On est si loin de l'intention première du texte (la rapporteure nous parlait des propos homophobes et du cyberharcèlement en milieu scolaire !) que les bras nous en tombent. On peut parler de « cavalier législatif »[21].

Au bout du compte, le texte adopté en mai 2020 est à nos yeux entièrement mauvais[22]. Des sénateurs ayant demandé l'intervention du Conseil constitutionnel, nous ajoutons une contribution écrite avec nos amis de Franciliens.net (fournisseur d'accès associatif[23]), concernés au premier chef par les mesures de censure express. En juin 2020, les sages censurent la quasi-intégralité de la loi Avia, vue comme une atteinte majeure à la liberté d'expression. Nous ne cachons pas notre joie. Ce n'est pas faute d'avoir largement prévenu les législateurs…

LE FISC SURVEILLE LES RÉSEAUX SOCIAUX

C'est acquis, le Web est devenu pour les pouvoirs publics un lieu à surveiller, mais aussi un moyen de surveillance. La fin de l'année 2019 en offre une illustration nouvelle, avec un article étonnant de la loi de finance 2020 – votée chaque année pour définir les ressources et les dépenses de l'État durant l'année à venir – qui autorise les services du fisc[24] à analyser les informations postées par les contribuables sur les

réseaux sociaux, dans le but de découvrir des incohérences entre un niveau de revenus déclarés et un train de vie affiché…

Avez-vous déclaré la construction de la piscine au bord de laquelle vous vous affichez en ligne en maillot de bain ? De façon plus curieuse, les informations publiées sur les réseaux sociaux et sur les sites de vente en ligne seraient collectées et analysées par des algorithmes de traitement en masse. Des algorithmes capables d'identifier une vie de nabab ? Non bien sûr, mais capables de reconnaître la vente de cigarettes de contrebande ou de vêtements de contrefaçon, par exemple, qui intéressent beaucoup le fisc et les douanes[25]. Le législateur évoque aussi la possibilité d'identifier, grâce à la reconnaissance des paysages et des décors urbains, le véritable lieu d'habitation d'une personne qui aurait déclaré sa résidence principale à l'étranger pour des raisons fiscales.

Bref, vos photos de restaurant en terrasse postées sur Instagram intéressent les services des impôts[26]. Nous déposons un recours devant le Conseil constitutionnel, mais peine perdue : l'article de loi est validé. L'épisode confirme donc que la surveillance des citoyens par l'intermédiaire des outils numériques est une source inépuisable d'inspiration pour les gouvernements, et semble ne pas poser plus de problème aux yeux du législateur.

Cette fin d'année 2019 et le commencement de 2020 sont d'autant plus difficiles à la Quadrature que les mauvaises nouvelles s'accumulent. D'abord, la « directive Copyright » est adoptée par le Parlement européen en mars 2019, alors que nous sommes accaparés par le travail sur le règlement Terro. Première défaite. Les articles les plus mauvais sont adoptés, et les défenseurs du partage sont amers. Par ailleurs, le règlement Terro est adopté une première fois par le Parlement européen pendant l'été 2019, avec toutes les dispositions que nous combattions. Deuxième défaite. C'est dur.

Ce double échec est très mal reçu par bon nombre de nos soutiens « historiques », de l'époque de la lutte contre la loi Hadopi, qui le prennent comme une trahison de leurs combats anciens. S'opposer à l'envahissement sécuritaire n'est visiblement pas aussi essentiel à leurs

yeux, ou les touche moins directement. En tout cas, la période est délicate pour le groupe : engueulades avec les amis, coups bas sur les réseaux sociaux, départs de l'association. On lance la campagne contre la technopolice avec le doute au cœur, et dans une ambiance de grande solitude face à la montée d'un monde sécuritaire auquel le numérique collabore de toute sa puissance.

Pendant ce temps, en Chine, une pneumopathie fulgurante touche plusieurs personnes dans la ville de Wuhan. Et déjà l'année 2020 nous fonce dessus à toute vitesse.

5. L'ÉTAT D'URGENCE SANITAIRE, NOUVELLE STRATÉGIE DU CHOC

En mars 2020, le ciel nous tombe sur la tête. Dans la stupeur du confinement décrété le 17 mars, l'association est comme à l'arrêt. Chacun chez soi, nous sommes scotchés aux réseaux sociaux, à la télé et aux sites de presse pour essayer de comprendre ce qui se passe. Et très vite, ce qu'on voit nous pousse à agir – sans sortir de chez nous, et dans le respect des gestes barrières.

L'ATTAQUE DES DRONES

Première stupéfaction : les drones policiers envahissent les villes. En quelques jours, ils sont partout. Quelques semaines plus tôt, en décembre 2019 ou en janvier 2020, on voyait sur les chaînes d'info des reportages amusés et condescendants sur « la Chine », pays lointain, exotique et totalitaire, dans lequel la population était entièrement confinée sur ordre du pouvoir (imaginez ça chez nous !), dans une spectaculaire tentative d'endiguer une épidémie mystérieuse, mortelle et fulgurante. Regardez ces images, mesdames et messieurs, c'est incroyable : des drones pilotés par des policiers sillonnent les rues pour rappeler à l'ordre les habitants terrorisés, et pour filmer les contrevenants.

Fin mars 2020, les mêmes reportages sont tournés en France : regardez comment ces sympathiques policiers utilisent un matériel ultramoderne et hypertechnologique pour rassurer nos concitoyens !

Regardez comme le gouvernement prend bien les choses en main, et comme nos rues sont sûres ! Gros plan sur l'appareil au sol, plan de coupe sur les visages des policiers, l'air soucieux et impliqués, penchés sur l'écran de contrôle du drone, plan sur le drone en vol, interview de l'officier qui explique, ton responsable et ferme, que c'est un outil moderne et que les incivilités doivent être combattues pour le bien de tous. C'est dans la boîte.

Aucune exagération. Le réel s'est caricaturé lui-même, au prix d'un retournement de veste hautement acrobatique. Trois éléments sont frappants. D'abord, la docilité des grands médias télé, qui assurent bénévolement la communication des préfets et du ministère de l'Intérieur, sans aucune distance critique. Ensuite, la facilité avec laquelle ce qui était présenté il y a peu comme le symbole du totalitarisme peut devenir, en changeant seulement la légende qui accompagne l'image, le symbole de l'ordre et de la paix : c'est à quoi l'on s'expose, à force de dire que la sécurité est la première des libertés. Enfin, le cynisme avec lequel le ministère de l'Intérieur pousse son agenda. On pourrait penser à une sorte de gesticulation dans le vide, dans une période où il est privé de son efficacité – la police ne sait soigner personne. Mais connaissant la hiérarchie policière et le ministère de l'Intérieur, il faut envisager aussi une stratégie délibérée, qui n'hésite pas à saisir toutes les occasions de rendre la police nécessaire et la surveillance sympathique. La motivation d'ordre politique est peut-être renforcée aussi par un impératif plus trivial de publicité : dans une logique de privatisation de l'État et de rétrécissement des budgets publics, chaque ministère doit se mettre en avant pour gagner des arbitrages et augmenter ses dotations.

Quoi qu'il en soit, l'irruption des drones dans le paysage sécuritaire est si frappante que nous publions dès le 4 avril 2020, dans la troisième semaine du confinement, un article intitulé « L'attaque des drones[1] ». Le texte recense d'abord un certain nombre de vols de drones médiatisés et documentés, pour donner la mesure de l'ampleur et de la gravité des choses : les reportages télévisés montraient des drones équipés de haut-parleurs pour diffuser les consignes de confinement dans les rues et «

prévenir », mais on apprend que des personnes qui se promenaient ont été suivies par des drones avant d'être verbalisées par la police – pour les « guérir » ? L'article replace ensuite cette utilisation nouvelle dans une continuité : les drones sont utilisés depuis 2014 au moins, pour surveiller les migrants aux frontières, les manifestations, ou les ZAD, mais avec une grande discrétion médiatique, dans un brouillard de secret presque militaire. Tout se passe comme si la crise sanitaire venait soudain décomplexer les policiers, justifier la posture sécuritaire. Enfin, l'article constate que l'utilisation des drones de surveillance n'est pas encadrée par la loi.

Bizarrement, le sujet prend. Dans la vacuité de l'actualité, ou dans sa grande monotonie, la présence des drones policiers surprend et choque l'opinion. Sans doute le contraste entre la débauche de haute technologie de surveillance et le dénuement de l'hôpital public a-t-il aussi un rôle de révélateur. En tout cas, si l'on en croit les rares indicateurs de l'humeur publique que nous pouvions avoir en restant confinés chez nous, à savoir les dons de soutien à l'association et les e-mails reçus à notre adresse publique (contact@laquadrature.net), le sujet déchaîne les passions. Beaucoup plus, par exemple, que la surveillance des manifestations pendant les quatorze mois de « gilets jaunes » qu'on vient de traverser. C'est une surveillance concrète qu'on peut voir et qui, en plus, parle. On a l'impression que tous les commissariats se lâchent et se mettent à surveiller à travers leurs robots volants : surveillance des plages, des forêts, des villes, à distance.

Le 12 avril 2020, après un mois de confinement strict, le ministère de l'Intérieur publie un appel d'offres pour l'achat de 650 drones, pour un montant de 4 millions d'euros. Parmi les clauses de détail, on découvre « 180 micro-drones du quotidien[2] ». Vous le saviez, vous, qu'il existait des drones de surveillance « du quotidien » ? « Devant les sénateurs, Christophe Castaner a réfuté tout lien avec le confinement mais ne se privera pas de les utiliser dans cette optique[3] », précise LCI.

Une utilisation décomplexée, mais une utilisation illégale. Conjointement avec la LDH, nous déposons le 4 mai 2020 un recours

devant le tribunal administratif de Paris[4], contre l'utilisation des drones par la préfecture de police de Paris, sous les ordres du préfet Didier Lallement. Le tribunal administratif nous déboute de notre référé-liberté, une procédure qui juge en urgence d'une atteinte aux libertés. Qu'à cela ne tienne, nous allons devant le Conseil d'État pour une décision sur le fond. L'audience se tient le 15 mai, et le Conseil d'État écoute longuement notre avocat, celui de la LDH, et le représentant du ministère de l'Intérieur. Le 18 mai, l'ordonnance du Conseil d'État cloue les drones au sol. Nous avons gagné[5].

Mais le préfet emploie de nouveau les drones au-dessus des manifestations parisiennes, dès le « déconfinement », en toute illégalité. Comme nous sommes encore plus têtus que le préfet, nous retournons fin octobre 2020 devant le Conseil d'État[6], qui réitère son jugement : en l'absence d'une nécessité démontrée, les drones en manifestation sont interdits[7]. Les goélands parisiens, qui attaquaient les drones pendant les manifestations, deviennent notre mascotte officielle.

FLAMBÉE DE L'ÉPIDÉMIE DE SURVEILLANCE

L'ivresse sécuritaire en pleine épidémie ne s'arrête pas aux drones. La vidéosurveillance automatisée refait son apparition, avec de nouveaux gadgets. Des mairies proposent d'utiliser des caméras thermiques pour détecter les personnes fiévreuses, et donc probablement infectées et contagieuses, à l'entrée des magasins ou des bâtiments recevant du public. Une telle proposition aurait fait sauter au plafond en 2019. En 2020, on se contente de souligner – et le lobby industriel le premier – que ça ne fonctionne pas encore très bien. Comme si le principal était de « faire quelque chose », et de montrer qu'on fait quelque chose – donc, certaines villes mettent des caméras thermiques à l'entrée des écoles[8]…

Les entreprises de la surveillance ont elles aussi une imagination sans limite et une solide propension à l'opportunisme – qualités entrepreneuriales par excellence, appelées souplesse, réactivité, créativité,

proactivité, adaptabilité, disruption, ou quelque chose comme ça. Prenez par exemple la société Datakalab[9]. Cette petite start-up qui se réclame de la *brain-tech* (concept audacieux) s'est spécialisée dans la détection des émotions par reconnaissance faciale, en visant plutôt des applications marketing, comme la mesure de l'efficacité des publicités. Bel exemple de capitalisme de surveillance : en avril 2020, la société propose à la ville de Cannes de tester ses logiciels sur les caméras municipales, pour voir si les habitants portent bien le masque sur les marchés de la ville et dans les bus[10]. Loin de choquer, l'initiative plaît : en mai 2020, la RATP passe un contrat avec Datakalab, pour une expérience d'ampleur à la station Châtelet, une des plus fréquentées de Paris. Les logiciels de l'entreprise sont couplés aux caméras de surveillance de la régie pour vérifier si les voyageurs portent un masque et respectent bien la « distanciation sociale » dans les couloirs de la station[11]. Mais cette fois-ci, la CNIL s'interpose. Elle avait laissé faire l'expérience cannoise, jugeant que les données étaient suffisamment anonymisées pour ne présenter aucun risque pour la vie privée. Et puis les personnes qui ne donnaient pas leur consentement pouvaient faire « non » avec la tête… Mais dans le métro Châtelet, aucune possibilité de ne pas donner son consentement : c'est illégal. L'expérience est suspendue en juin 2020[12].

L'avis de la CNIL précise : « Si des données sensibles sont traitées, telles que la captation d'informations personnelles de santé ou d'informations biométriques, ou si le droit d'opposition n'est pas possible (du fait, par exemple, du "balayage vidéo" de la caméra dans une rue), il est nécessaire de mettre en place un cadre légal adapté qui respecte l'article 9 et/ou l'article 23 du RGPD[13]. » S'il faut une loi, on fait une loi : le ministère des Transports la fait passer un an plus tard, sans que personne ne se demande si le fait que tous nos visages soient analysés et décortiqués dans les transports a vraiment une utilité, ou si l'argent ne pourrait pas servir à autre chose. Mais pour le gouvernement néolibéral, de l'argent public investi dans les services publics est perdu, alors que l'argent public qui paye des entreprises privées est bien dépensé, dans « l'économie réelle ». Ce n'est pas une blague ni une exagération : le

milliardaire Bernard Arnault, soutien d'Emmanuel Macron en 2017 et jamais démenti depuis lors, déclarait en 2016 que « les emplois publics ne sont pas de vrais emplois ». Bref.

Fort heureusement, l'épidémie crée sans cesse de nouveaux débouchés pour les maniaques de la surveillance, et autant de « leviers de croissance ». Le confinement strict, avec le télétravail obligatoire et la scolarité à distance, ouvre de nouvelles perspectives aux surveillants. Comment s'assurer que les élèves sont attentifs et ne trichent pas pendant les devoirs surveillés ? Comment s'assurer que les salariés travaillent bien autant d'heures qu'on leur en paye ?

On a bien entendu décidé, car « plus rien ne serait comme avant », de faire confiance aux gens. Les étudiants ont tout intérêt à étudier sérieusement, puisqu'il s'agit de leur propre éducation et de leur avenir. Il est par ailleurs très facile de vérifier si les salariés ont fait ou non le travail qui leur est demandé. Ha ha ! C'est une plaisanterie, bien sûr.

Les entreprises de la surveillance ont aussitôt proposé d'innombrables outils astucieux pour surveiller les gens, en utilisant notamment la webcam de leur ordinateur de travail. Comme avec les drones, il s'agit de maintenir sous surveillance celles et ceux qui sont trop loin pour être directement sous l'œil du chef. Pour les étudiants, les start-up vendent aux universités la possibilité de surveiller les examens et d'éviter la triche (car tout est là) : une caméra ouverte en permanence, parfois un smartphone pour filmer le contrechamp et s'assurer que personne n'est présent pour aider l'étudiant, avec analyse des sons et des images, et parfois jusqu'à l'analyse de l'activité du globe oculaire[14]…

Derrière toutes ces initiatives disparates, l'idée est au fond la même : dans une crise profonde comme peut l'être une épidémie mondiale, il faut afficher son action et promettre une solution rapide et facile. L'intelligence artificielle est parfaite pour ça : mystérieuse, moderne et un peu floue, elle permet de promettre qu'on va résoudre magiquement les difficultés de fond, et si le résultat tarde à venir, c'est qu'il faut aller plus loin et perfectionner les outils. Caméras thermiques : les personnes fiévreuses ne pourront plus entrer dans les lieux fermés. Robots qui

vérifient la distance physique. Robots qui vérifient le port du masque. Utilisation des données GPS : tout à coup, Orange sort du bois et propose d'utiliser de nouveau les données de bornage de nos téléphones, pour savoir qui respecte ou non le confinement…

Dans l'idéal, il faudrait pouvoir suivre chaque personne en permanence, et savoir qui croise qui, pour tracer le parcours des contaminations… C'est ce que propose sans honte Sigfox, une entreprise toulousaine d'objets connectés : fournir des bracelets électroniques pour suivre les malades à la trace[15].

TRAÇAGE INDIVIDUEL ET RELATIONS SOCIALES

Ce fantasme ultime, c'est bien sûr l'application StopCovid : développée par l'Institut national de recherche en sciences et technologies du numérique (Inria) et disponible le 2 juin 2020, elle est voulue et promue par le gouvernement comme solution moderne de suivi et de contrôle des contaminations. Chaque personne est invitée à l'installer sur son smartphone, et à activer en permanence la fonction Bluetooth du téléphone. Ce dispositif de liaison sans fil, par ondes radio de courte portée, est relativement sensible à la distance. Il est donc utilisé pour identifier, grâce à leur adresse matérielle, les téléphones du voisinage. Un système de chiffrement permet d'anonymiser ces données : le logiciel attribue à chaque appareil un identifiant qui ne doit pas permettre de retrouver l'adresse MAC[16] ou le numéro de téléphone de l'utilisateur. Ensuite, les personnes qui s'avèrent contaminées par le Covid-19 sont censées l'indiquer dans leur application. Leur identifiant déclenche aussitôt une alerte à destination de toutes les personnes qui les ont « croisées » suffisamment longtemps et dans une période compatible avec la durée d'incubation du virus. Le but : que chacun puisse s'isoler et se tester au plus tôt, quand il peut avoir été contaminé, afin de casser la chaîne de la contagion.

Avant même qu'elle existe, la seule idée de cette application de « traçage » (le mot « *tracking* » est employé par les épidémiologistes dans les médias) déchaîne un débat furieux, dans lequel nous prenons notre part. Personne ne nie l'utilité de suivre les contagions, et de prévenir les personnes ayant été en contact avec une personne malade. Ce qui est contesté, c'est la nécessité de passer par une application numérique pour le faire. Ici comme ailleurs, on craint que la facilité, au lieu d'être un argument en faveur du numérique, soit le centre même du danger. Le sociologue Antonio Casilli, par ailleurs membre de La Quadrature du Net, signe le 25 avril 2020 dans *Le Monde* une tribune intitulée « StopCovid est un projet désastreux piloté par des apprentis sorciers[17] ». En amont du débat parlementaire du 28 avril, la tribune invite les députés à rejeter le projet : « Les parlementaires français seront amenés à voter sur StopCovid, l'application mobile de traçage des individus imposée par l'exécutif. Nous souhaitons que, par leur vote, ils convainquent ce dernier de renoncer à cette idée tant qu'il est encore temps. Non pas de l'améliorer, mais d'y renoncer tout court. [...] Cette "solution" technologique ne serait qu'une continuation du confinement par d'autres moyens. Si, avec ce dernier, nous avons fait l'expérience d'une assignation à résidence collective, les applications mobiles de surveillance risquent de banaliser le port du bracelet électronique. »

Le 14 avril 2020, nous avions publié nos « arguments pour rejeter StopCovid[18] ». Dans une période aujourd'hui oubliée, où les masques manquaient, où les tests existaient à peine, où le vaccin était encore un rêve, le côté magique de la solution numérique pouvait séduire. On allait pouvoir être averti par SMS de la proximité du virus. Il est intéressant de lire a posteriori nos arguments contre l'application, car ils sont assez proches de ceux qu'on peut adresser, dix-huit mois plus tard, au « passe sanitaire » (2021) ou au « passe vaccinal » (2022).

Le plus frappant : l'installation de l'application risque de devenir un prérequis pour accéder aux activités sociales ordinaires (prendre un train, voir un spectacle), et risque de créer des inégalités réelles dans la population, quand un quart des habitants du pays ne possède pas de

smartphone. Le reste des arguments tourne autour de la faiblesse technique de l'outil (problèmes de l'anonymisation, imprécision du Bluetooth, alertes inutiles dans les zones densément peuplées, etc.), et surtout sur la très redoutée banalisation des outils de contrôle, dont nous avons déjà parlé au sujet de la reconnaissance faciale. Le plus pertinent est sans doute celui-ci : l'outil technologique risque de donner aux gens qui l'utilisent un faux sentiment de sécurité, alors qu'il est très loin d'être infaillible, et d'entraîner un relâchement des gestes de protection efficaces (masque, distanciation, aération, etc.). C'est un argument qu'on entendra contre le « passe sanitaire », qui n'a de sanitaire que le nom, étant entendu qu'il ne protège en rien de la contamination, mais ne fonctionne de l'aveu même du gouvernement que comme incitation à la vaccination par la restriction des libertés.

La CNIL publie le 27 avril 2020 un avis sur l'application StopCovid, que nous trouvons un peu faible. Elle demande au gouvernement de démontrer la nécessité de l'outil numérique, alors que le traçage des contacts peut être fait par d'autres moyens, par exemple en interrogeant les personnes contaminées. Mais la commission ne va pas assez loin dans la formulation de cette exigence, et c'est le point le plus intéressant de notre article, son affirmation la plus forte : « L'idée au cœur du droit des libertés fondamentales est que, par principe, il est interdit de limiter nos libertés. Elles ne peuvent l'être que par exception, et uniquement en démontrant qu'une telle limitation est utile à un intérêt supérieur, telle que la santé publique dans notre cas. […] Si aucun élément factuel ne prouve l'efficacité d'une technique qu'elle reconnaît pourtant comme attentatoire aux libertés fondamentales, la mission de la CNIL est de déclarer celle-ci illégale[19]. »

Un an plus tard, StopCovid est devenu TousAntiCovid, et plus personne n'utilise l'application pour le « contact *tracking* ». En revanche, de nombreuses personnes l'utilisent pour produire le QR code de leur « passe sanitaire ». L'application a donc bien confirmé sa vocation policière et administrative, perceptible dès l'origine, et bien éloignée de toute préoccupation d'ordre sanitaire au sens strict. Après quatre ou cinq

vagues de Covid-19, après les vagues de contamination par les variants Delta (été et automne 2021) puis Omicron (hiver 2021-2022), tout le monde a oublié la notion même de traçage des contacts. L'idée paraît vieille et inutile, comme beaucoup d'idées sécuritaires nées pendant la crise du printemps 2020 paraissent aujourd'hui vieilles et inutiles. Les caméras thermiques se sont fait oublier. Aucun drone dans les rues ne surveille le port du masque ou les distances de sécurité. On ne parle plus nulle part de suivre les malades par GPS ou par bornage des téléphones. Quand on passe en revue ces vieux fantasmes de 2020, on a l'impression de traverser un cimetière de jouets encore neufs. Tant mieux.

UNE FRÉNÉSIE LÉGISLATIVE

Les gadgets passent, mais les lois restent – hélas. Saisissant le prétexte de l'urgence d'agir, le gouvernement de la majorité Macron est pris d'une frénésie législative. D'abord, il se donne les moyens, très vite, d'une action exceptionnelle, en faisant voter dès le 23 mars 2020 une loi réglementant l'état d'urgence sanitaire. Prorogée plusieurs fois, cette loi est encore en vigueur au moins jusqu'au 31 juillet 2022. L'état d'urgence sanitaire proprement dit, quant à lui, a duré en France métropolitaine de mars 2020 à juin 2021, et il a été réactivé dans les DOM-TOM à la fin de l'année 2021 (Martinique, La Réunion) et début 2022 (Guadeloupe, Guyane, Mayotte, Saint-Martin et Saint-Barthélemy). Cet état d'urgence renforce le pouvoir exécutif, qui peut prendre un plus grand nombre de décisions par décret.

Malgré son importance vitale, l'organisation de la lutte contre l'épidémie est très loin d'être en 2020 la seule occupation du gouvernement. Édouard Philippe, puis Jean Castex, qui lui succède à Matignon, font voter des lois (sécuritaires), entre deux douzaines de décrets (sécuritaires). Rapide tour d'horizon.

D'abord, l'année est marquée par une avalanche de nouveaux fichiers, ou d'élargissement des fichiers existants, que nous tentons de contester

devant les tribunaux. En mars 2020, le ministère de la Justice décide d'ouvrir le fichier DataJust : il regroupera toutes les décisions de justice qui comportent une notion de dédommagement, ou d'indemnisation des préjudices corporels. C'est un ensemble colossal, qui comporte une grande quantité de données personnelles, voire très personnelles : les noms des personnes impliquées, bien sûr, mais aussi leur situation financière, professionnelle et familiale, ou des indications de santé physique et mentale, etc. Pourquoi agréger toutes ces décisions ? Apparemment, pour voir s'il ne serait pas possible de confier ces millions de jurisprudences et de cas particuliers à un algorithme qui en déduirait, par « apprentissage », la meilleure décision à prendre en fonction des données de la situation : un conseiller ou un juge automatique, en quelque sorte, qui serait statistiquement juste, en fonction des décisions prises dans le passé par les juges humains. Le ministère est très flou sur ce qu'il attend d'un tel algorithme, et se montre bien incapable d'expliquer en vue de quoi il aurait besoin d'autant de données personnelles aussi sensibles. Sur la base des bafouillements du ministère, dont la CNIL relevait aussi le peu de consistance, nous contestons ce fichier devant le Conseil d'État. Notre recours est rejeté en décembre 2021.

En avril 2020, pendant le confinement, le gouvernement élargit les finalités du dossier « Accès au dossier des contraventions » (ADOC), normalement réservé aux infractions routières. Les policiers et les gendarmes avaient commencé à s'en servir pour enregistrer les amendes pour non-respect des règles du confinement : comme la récidive était punie d'une amende plus forte, puis d'une peine de prison, il fallait bien tenir le compte. Comment ? En détournant un fichier… Malheureusement pour les agents, c'est illégal. Après qu'un prévenu a été relaxé pour « malfaçon juridique »[20], le gouvernement prend un décret pour renommer le fichier (« Système de contrôle automatisé » ou SCA) et élargir ses finalités à toutes les amendes[21]. Là encore, le Conseil d'État rejette notre recours en décembre 2021.

Fin 2020, en décembre, trois décrets modifient trois fichiers[22] de « sécurité publique », pour y inclure les « habitudes de vie » et les « activités en ligne », ainsi que les « opinions politiques », là où n'étaient prises en compte auparavant que des « activités politiques ». Nous attaquons également ces décrets devant le Conseil d'État (et nous sommes toujours en attente de la décision).

Du côté des lois, c'est l'escalade. D'abord, en septembre, le gouvernement français introduit dans un projet de règlement européen nommé DSA son sempiternel retrait des contenus en 24 heures[23], qui vient pourtant d'être censuré par le Conseil constitutionnel dans la loi Avia quelques mois plus tôt (juin 2020). En décembre, le gouvernement prend le prétexte de sa lutte contre le terrorisme et la radicalisation islamiste pour s'en prendre aux associations, dans son projet de loi contre le séparatisme. Et surtout, en novembre 2020, le gouvernement présente une nouvelle loi de police, intitulée en toute franchise : « loi pour une sécurité globale ». Nous y reviendrons.

LE HEALTH DATA HUB (HDH) : OFFENSIVE DU BUSINESS SANITAIRE

À l'été 2019, la Quadrature est contactée par un médecin et un ingénieur, qui se sont constitués en association sous le nom d'InterHop. Ils travaillent tous deux pour l'Assistance publique-Hôpitaux de Paris (AP-HP) et s'occupent de la gestion des données de cet énorme groupe hospitalier qui rassemble 39 hôpitaux et accueille 10 millions de personnes chaque année.

Cette activité génère une énorme quantité de données, utilisées bien sûr pour organiser au quotidien les actes médicaux et la facturation, mais qui intéressent aussi beaucoup les praticiens, les entreprises et les organismes de santé. Les deux militants sont inquiets : le gouvernement a décidé, à la suite de la publication du rapport Villani[24], de débloquer un budget colossal pour des projets d'intelligence artificielle, et de mettre dans le même temps les données de santé françaises à disposition des

chercheurs et des entreprises qui souhaiteraient les utiliser, car il faut « faire de la France un pays leader de l'intelligence artificielle ». Une telle base existe déjà depuis 2016 sous le nom de Système national des données de santé (SNDS). Mais, afin d'élargir les données collectées et d'en faciliter l'accès au secteur privé (GAFAM, « medtechs », start-up, assureurs, mutuelles, etc.), un groupement d'intérêt public nommé Health Data Hub (HDH) est créé le 24 juillet 2019.

Le HDH doit regrouper à terme les données de la médecine de ville, des pharmacies, du système hospitalier, des laboratoires de biologie médicale, du dossier médical partagé, de la médecine du travail, des Ehpad ou encore les données des programmes de séquençage de l'ADN[25]. L'accès aux données du SNDS était conditionné à « des fins de recherche, d'étude ou d'évaluation présentant un caractère d'intérêt public ». Pour simplifier l'accès au HDH, on enlève les notions de recherche, d'étude ou d'évaluation. Il suffit désormais de déclarer un traitement « présentant un caractère d'intérêt public ».

Avec le Syndicat des jeunes médecins généralistes (SJMG) et le Syndicat de la médecine générale, nous rédigeons un courrier commun faisant état de nos questionnements sur les modalités de constitution des comités éthiques, qui auront à décider des projets qui auront accès aux données de santé des Français, ainsi que sur les finalités de recherches envisagées, mais aussi sur la solution technique et le modèle économique retenus. Le 31 octobre 2019, nous avons rendez-vous à la Direction de la recherche, des études, de l'évaluation et des statistiques (DREES), une direction de l'administration centrale dépendant conjointement des ministères de la Santé, du Travail et de l'Économie. Nous sommes reçus par la directrice et la sous-directrice du projet, avec un représentant de l'April[26] et un membre du SJMG. L'entretien dure deux heures. L'échange est riche, avec des réponses techniques et argumentées. On en sort plutôt rassurés.

Mais le 19 juin 2020, Jérôme Hourdeaux, journaliste à *Mediapart*, analyse la délibération de la CNIL du 20 avril 2020 concernant le projet HDH[27], depuis son architecture technique jusqu'au contrat

d'hébergement avec Microsoft[28]. Il explique que la CNIL s'inquiète : Microsoft conserverait une copie des clés de chiffrement des données, « ce qui a pour conséquence de permettre techniquement à ce dernier d'accéder aux données ». Aucun rapport avec les données « stockées à froid et chiffrées, donc inaccessibles » qu'on nous avait promises lors de notre entretien sept mois plus tôt. On nous avait expliqué aussi que le système serait cloisonné, et que les différentes technologies nécessaires au fonctionnement du HDH (stockage, machine virtuelle, environnement de travail, outils d'analyse) seraient réparties entre différents prestataires pour éviter les risques de fuite.

Mais c'est Microsoft qui rafle la mise ! La directrice technique du HDH arguant, sans sourciller, que seules les plateformes d'hébergement américaines sont capables de proposer des technologies à la hauteur pour le stockage et le traitement des données de santé françaises. Pourtant, il y a un hic : Microsoft dépend de la législation américaine, passablement permissive concernant l'accès de son administration aux données stockées par les entreprises… InterHop attaque cette décision d'hébergement devant le Conseil d'État, ce qui pousse Olivier Véran, ministre de la Santé, à s'engager à « faire disparaître complètement » les risques posés par l'hébergement du HDH chez Microsoft, et à « adopter une nouvelle solution technique » sous deux ans, dans un courrier adressé à Marie-Laure Denis, présidente de la CNIL, le 19 novembre 2020.

Faute de chiffrement fiable, peut-on au moins anonymiser les données de santé ? C'est une solution évoquée pour apaiser les esprits, mais techniquement inatteignable. Anonymiser de telles données n'a aucun sens : on souhaite pouvoir suivre le parcours d'un malade sur une longue période, comparer l'évolution de la santé sur le long terme, chaque acte médical doit donc pouvoir être corrélé avec le précédent. Cette agglomération est suffisante pour identifier une personne unique dans une base de données.

De manière plus générale, se pose la question de la légitimité de la création de ce *hub*. Dans un pays où les urgences sont régulièrement débordées, où les « déserts médicaux » obligent les patients à parcourir

des dizaines de kilomètres pour se rendre chez un généraliste, et les secours à perdre des dizaines de minutes avant de venir en aide à un accidenté, au moment même où la pandémie de Covid-19 fait déborder les services de réanimation, la priorité serait-elle de dépenser des centaines de millions d'euros pour ouvrir nos données de santé aux start-up de la « biotech » ?

Les hôpitaux ont déjà leurs entrepôts de données, et travaillent avec des chercheurs et des entreprises pour améliorer les parcours et les protocoles de soin. Outre le travail titanesque à réaliser pour homogénéiser les données entre des centaines d'hôpitaux et de CHU, c'est aussi demander aux responsables de traitement de transférer des données obtenues auprès de leurs patients à une entité nationale sur laquelle ils n'ont aucune maîtrise.

Quelle idée sous-tend la centralisation de ces données de santé et leur usage par des start-up ? Une croyance en l'absolue vérité apportée par la machine[29]. En l'infaillibilité des algorithmes. Lors de la remise du rapport Villani intitulé « Donner un sens à l'intelligence artificielle : pour une stratégie nationale et européenne », Emmanuel Macron prononce un discours dans lequel il évoque le monde calculable de Leibniz, parle d'option « presque prométhéenne » et, comble de lyrisme, entrevoit dans un avenir proche la possibilité « à travers des machines apprenantes de pouvoir parcourir beaucoup plus rapidement les chemins du malheur pour choisir le bon chemin beaucoup plus tôt et beaucoup plus rapidement[30] ». Battre Dieu en calcul, rien que ça !

Le rapport Villani ne recule pas non plus devant le lyrisme, mais sa conclusion est beaucoup plus pragmatique. Nous sommes dépassés par la puissance des GAFAM (encore une fois, on retrouve cette idée d'impuissance des politiques, écrite noir sur blanc par les politiques eux-mêmes), mais il nous reste une carte à jouer pour rester dans la course : fournir les données sectorielles sans lesquelles l'IA n'est rien. Et l'organisation du système de santé français permet à l'État d'être assis sur une mine d'or. Emmanuel Macron l'avoue crûment : « Nous avons un véritable avantage, c'est que nous possédons un système de santé […]

très centralisé, avec des bases de données d'une richesse exceptionnelle, notamment celle de l'Assurance-maladie et des hôpitaux. » Puisqu'on n'est pas capable de fabriquer le véhicule, fournissons le carburant ! C'est la piste nommée « *Hospital as a Platform* » par le rapport Villani[31].

Les personnels de santé créeront les données qui seront vendues demain par le HDH. Il est donc évidemment « nécessaire que les professionnels de santé soient sensibilisés et formés pour encoder ces informations de manière à les rendre lisibles et réutilisables par la machine » ! Si le personnel résiste, c'est forcément un problème de culture : il sera donc nécessaire de « procéder à la large diffusion d'une culture de la donnée ». Mais la « culture de la donnée » française et européenne repose sur la loi informatique et libertés (France, 1978) et sur le RGPD (Union européenne, 2018), qui visent justement à protéger cette donnée, et particulièrement la donnée de santé, dite « sensible », au même titre que l'orientation politique ou sexuelle. Maintenant que le contexte technique permet une analyse extrêmement pointue de ces données, il faudrait donc cesser de la protéger, parce qu'elle a une valeur économique importante ?

Début 2022, la loi de création du HDH est votée, les décrets sont passés, mais il manque encore un arrêté, qui définit en particulier la composition du catalogue de données que le HDH pourra exploiter. Il manque aussi une autorisation de la CNIL pour utiliser les données du SNDS[32] – deux éléments cruciaux pour que le projet puisse démarrer. Entre-temps, début 2020, une loi est passée en urgence pour permettre l'utilisation des données liées au Covid-19, et certains projets ont donc pu démarrer sur cette base, dans un cadre dérogatoire lié à la situation sanitaire exceptionnelle. Mais légalement, le HDH n'a toujours pas d'existence, et ses choix techniques, jusqu'à sa justification politique, font toujours débat. La CNIL et la Caisse nationale d'assurance-maladie (CNAM)[33] ont déjà fait part de leur fébrilité sur ce sujet, et la première risque de rendre un avis négatif. En pleine campagne présidentielle, sur un projet pour lequel Emmanuel Macron s'était largement mouillé, sur un thème très « start-up nation compatible », il faut éviter les risques

inutiles. Début janvier 2022, le ministère de la Santé retire sa demande d'autorisation à la CNIL[34]. Le projet de HDH est donc momentanément à l'arrêt.

Les recherches fondées sur des données publiques, dans la majorité des cas récupérées sans que l'usager ne puisse donner un accord libre et éclairé, doivent rester sous le contrôle de la puissance publique. Cela implique de redonner corps à une recherche publique digne de ce nom. Notre système de soin ne doit pas devenir un auxiliaire au service d'entreprises privées et de technologies dont la place n'a jamais fait l'objet d'un débat public. L'histoire nous a largement montré comment les entreprises privées peuvent, dès que l'occasion leur est donnée, oublier le bien commun pour verser dans le capitalisme sordide[35].

La prochaine fois que vous parlerez de décroissance numérique, et qu'on vous accusera de vouloir envoyer tout le monde s'éclairer à la bougie dans des cavernes, vous pourrez répondre que vous envisagez d'abord, et pour commencer : un monde sans caméras de vidéosurveillance automatisée, sans reconnaissance faciale, sans profilage de la démarche ni détection des émotions, sans caméras thermiques et sans données médicales vendues à des assureurs privés, un monde où la police et les services de renseignement ne peuvent pas conserver vos données de connexion et de télécommunications pendant un an dans un entrepôt de données, ni ajouter votre visage dans des fichiers de police quand vous subissez un banal contrôle routier, un monde où votre navigation Internet n'est pas suivie de seconde en seconde par des multinationales pour vous gaver de publicité, ou pour sélectionner ce que vous pouvez lire ou ne pas lire sur les réseaux sociaux, un monde où vos données de santé ne servent pas, à votre insu, à engraisser des entreprises privées.

Mais ce n'est pas le monde dans lequel nous vivons. Dans notre monde, la surveillance est normale, banale, installée. En un an, on a dû s'acclimater aux drones, aux caméras automatiques, aux QR codes pour entrer quelque part – l'année 2020 a inscrit toutes ces technologies dans

notre quotidien. Et voici qu'arrive une nouvelle loi nommée « Sécurité globale ».

6. VERS UN MONDE DE LA « SÉCURITÉ GLOBALE » ?

Au printemps 2020, dans la stupeur du premier confinement sanitaire, il fut question d'un nouveau monde où « plus rien ne serait comme avant ». Dans ce « plus rien », chacun et chacune pouvait mettre ce qui lui tenait à cœur. L'écologiste a pensé qu'on prendrait un meilleur soin de la planète et des animaux. Le militant politique, bercé par la promesse que les travailleurs de la « première ligne » seraient soutenus « quoi qu'il en coûte », a pu croire que la politique d'austérité budgétaire pour les faibles et de crédit public pour les riches était arrivée à un tournant. Chacun a pu rêver tout son soûl, et rencontrer la déception le moment venu. Mais les associations qui militent pour le respect des droits et des libertés n'ont même pas eu cette chance : dès les premières semaines de mars 2020, les autorités françaises ont resserré le poing pour restreindre les libertés.

On pourrait disserter longtemps des raisons structurelles ou opportunistes de ce réflexe sécuritaire. Sur le plan structurel, on peut accuser le néolibéralisme, idéologie de la classe dirigeante, qui soumet l'État aux besoins des grandes entreprises privées et limite son action directe aux tâches « régaliennes », c'est-à-dire le seul maintien de l'ordre : armée, police, justice. On pourrait aussi voir se dessiner une sorte de « division du travail » au niveau national entre les membres de l'Union européenne : à l'Allemagne désarmée l'industrie d'exportation, à la France les techniques sécuritaires et militaires ?

L'essayiste nord-américaine Naomi Klein a théorisé, dans son livre *La Stratégie du choc*, l'idée qu'un pouvoir, même démocratique, n'hésite jamais à tirer parti des périodes de crise pour avancer ses positions, à la faveur de la désorganisation ou de l'inattention de la société, et à tirer ainsi profit de l'affaiblissement des oppositions institutionnelles ou populaires. De ce point de vue, la période de la crise sanitaire causée par l'épidémie de Covid-19 a joué à plein le rôle de diversion et d'opportunité, aussitôt saisie par Emmanuel Macron, la majorité parlementaire et le gouvernement placés sous ses ordres. On l'a vu : l'état d'urgence sanitaire, les drones pour surveiller les rues, les outils de suivi « sanitaire » des populations, les caméras automatisées et les logiciels d'analyse d'images pour contrôler les comportements, la multiplication des fichiers de police, le traitement policier de l'épidémie avec des « passes » et des amendes – tout cela est désormais connu.

Nous avons désormais, à la Quadrature, de très solides raisons de penser que cette hypothèse de l'opportunisme, de la « stratégie du choc » ou de l'effet de surprise, correspond à la réalité. Car les lois sécuritaires qui s'enchaînent ne sont ni des caprices ni des idées décousues. Derrière l'éparpillement apparent des initiatives, il existe en réalité une stratégie concertée. Nul besoin d'invoquer un complot secret ou des volontés secrètes, tout est officiel, et le ministère de l'Intérieur publie sa stratégie dans un document intitulé le « Livre blanc de la sécurité intérieure[1] ».

« Livre blanc de la sécurité intérieure » : l'avenir est déjà écrit

Le « Livre blanc de la sécurité intérieure » est rendu public le 16 novembre 2020 par Gérald Darmanin, ministre de l'Intérieur. Écrit par le ministère, ce long texte de trois cents pages veut « dessiner le pacte de protection et de sécurité des Français, plaçant l'humain au cœur de l'action », ce qui ne veut strictement rien dire, pour peu qu'on essaie de dépasser la surface sonore des phrases. Le livre blanc « s'appuie sur une concertation large et ouverte : experts de la sécurité, élus, préfets, agents

de terrain, chercheurs et universitaires, acteurs de la sécurité privée sans oublier les citoyens eux-mêmes avec la conférence organisée en janvier 2020 » pour définir en réalité son « pacte de protection » de manière unilatérale : il s'agit d'un programme établi par les policiers pour les policiers[2]. Lire ce document, c'est comprendre a posteriori la logique qui relie les lois sécuritaires qui l'ont précédé, et avoir sous les yeux la feuille de route des lois qui suivront. Et en guise « d'humain au cœur de l'action », on trouvera surtout beaucoup d'équipements et de technologies de surveillance à distance.

Un chapitre entier s'intitule « Porter le ministère de l'Intérieur à la frontière technologique[3] » : identité numérique, biométrie, IA[4], analyse des réseaux sociaux[5], prise de plainte en ligne, plateformes de signalement, système d'alertes sur les téléphones des habitants, terminaux mobiles et logiciels de saisie pour les agents sur le terrain, « gilet tactique connecté » et caméra-piéton sur chaque agent, casque et véhicule connectés, cartographie numérique, drones, brouillage radio pour contrer les attaques de drones civils, développement des outils informatiques nécessaires, réseaux internes ou mobiles et serveurs de données[6], collecte et analyse de données, croisement des fichiers (« multi-biométrie »)… Ce chapitre énorme aborde une quantité de sujets vertigineuse qui consacre de manière éclatante le lien intime entre police et numérique.

L'intelligence artificielle, la biométrie et les drones ont droit à des passages indiquant les limites légales actuelles de leur utilisation, et parfois la nécessité de nouvelles lois pour permettre leur plein développement. Travail d'ajustement de la loi aux besoins, à quoi s'emploiera tout aussitôt le projet de loi Sécurité globale.

Le livre blanc parle aussi avec insistance de la constitution d'un « continuum de sécurité », qui convoque l'imaginaire du dôme ou du bouclier, et dans lequel la gendarmerie et la police nationale occupent bien entendu la plus grande place, mais avec le renfort beaucoup plus important des polices municipales et des sociétés privées de sécurité. Ces éléments apparaissent directement dans la loi Sécurité globale, dont le

texte est présenté au Parlement par deux parlementaires de la majorité (LREM) le 20 octobre 2020 : Mme Alice Thourot, avocate et députée de la Drôme, et Jean-Michel Fauvergue, député des Pyrénées-Orientales, commissaire de police et ancien chef du RAID (de 2013 à 2017). Cette loi en faveur des policiers est portée par un policier, pour que tout soit bien clair.

Livre blanc et loi Sécurité globale, les deux textes sont à lire ensemble.

SÉCURITÉ GLOBALE : CE QUE DIT LA LOI

En octobre 2020, nous recevons un appel de l'attaché parlementaire d'une ancienne députée de la majorité : « Vous avez vu le texte de loi qui est bientôt présenté au Parlement ? C'est grave. » Ça tombe bien, les juristes de l'association ont reçu par d'autres voies une première version du texte, et sont justement en train de l'analyser. Cette loi attaque sur tous les fronts.

Une « sécurité globale », voilà un fantasme inquiétant. C'est même littéralement un fantasme totalitaire, celui d'une société figée, d'une fin de l'histoire. Et par ailleurs, ce que la dénomination recouvre est très pauvre, intellectuellement et humainement : il s'agit d'armer un peu plus la police, de lui donner encore des moyens supplémentaires de surveiller, quadriller, contrôler les vies dans l'espace public, qui ne doit plus être qu'un lieu de passage dans le calme. Le couloir de métro, la galerie commerciale et le quartier pavillonnaire comme modèles ultimes de la société.

Nous publions le 29 octobre 2020 une première réaction au projet de loi[7], en nous focalisant sur l'enjeu du moment : dans un contexte de très forte contestation sociale et de sévère répression des manifestations depuis plusieurs années, la loi Sécurité globale introduit plusieurs moyens d'augmenter directement la répression des manifestants, au sol et dans le ciel. Au sol, avec l'autorisation d'envoyer le flux d'images des

caméras-piétons en direct vers le poste de commandement (PC) : c'est évidemment pour coordonner l'intervention policière, mais c'est aussi se donner la possibilité technique d'appliquer aux images des logiciels d'identification biométrique pour repérer des meneurs. Dans le ciel, avec l'autorisation de faire voler des drones vidéo, dont le flux d'images est lui aussi transmis et analysé au PC en direct. Les moyens policiers se militarisent, la manifestation est appréhendée comme un champ de bataille, et l'approche du maintien de l'ordre comme une guerre civile. Contre cette logique insupportable, une forte contestation va s'organiser, au Parlement et dans la rue.

Dès les auditions préalables, nous contestons la partialité des rapporteurs du texte, qui laissent de côté le monde associatif pour n'écouter que les forces de l'ordre. Plus tard, nous dénonçons aussi le comportement de l'un des deux co-rapporteurs du texte, le député Fauvergue (LREM), ancien policier d'élite, dont la morgue et l'attitude agressive envers l'opposition parlementaire frappent les observateurs. Il suffira de l'entendre demander à une députée de l'opposition de « prendre ses gouttes » pour prendre la mesure du personnage[8]… Sûrs de leur fait et assurés de mener la loi à son terme grâce à la majorité à laquelle ils appartiennent, les deux co-rapporteurs montrent sans détour qu'il n'y a pas d'autres options : ce que la police a demandé, la police l'obtiendra.

Rendons grâce à la ténacité d'une poignée de parlementaires d'opposition qui ont su tenir bon, tout au long des débats, et porter la parole de la contestation démocratique contre les articles les plus litigieux et liberticides de cette loi policière. Quels sont ces articles ? Sur les seuls sujets de la Quadrature, le numérique et la surveillance technologique, ils sont au moins quatre.

Nous contestons l'article 20, qui donne le droit d'accès aux images de vidéosurveillance de l'espace public – jusqu'ici réservées à la police nationale et à la gendarmerie – aux agents des polices municipales, et même à certains agents municipaux de la ville de Paris. Nous contestons aussi l'article 20 bis, qui élargit les conditions sous lesquelles les copropriétaires d'un immeuble peuvent transmettre les images de

surveillance des parties communes, en direct, à la police, à des fins d'identification[9]. De même que l'article 20 ter, qui donne aux agents de la SNCF et de la RATP accès aux images de vidéosurveillance de l'espace public.

Nous contestons aussi l'article 21, qui autorise la caméra-piéton des policiers et l'envoi du flux d'images au commissariat ou au centre de commandement. Là encore, parce que nous souhaitons limiter les opportunités de traitement algorithmique des images (reconnaissance faciale ou biométrique), pour identifier et appréhender des personnes sur la seule foi de leur réputation, en particulier dans un contexte de mouvement social ou politique.

Nous contestons évidemment l'article 22, qui autorise les drones policiers non seulement pour des usages de surveillance des biens et des sites, mais pour la surveillance des foules et des manifestations, alors que ces appareils ont désormais une qualité de vidéo suffisante pour identifier des individus et les suivre, avec ou sans traitement algorithmique des images[10].

Mais ce qui va embraser le débat public et donner à la contestation de la loi Sécurité globale une dimension qui dépasse largement l'audience habituelle de la Quadrature, c'est l'article 24. Dans un contexte de grande tension sociale, de manifestations hebdomadaires et de violences policières filmées et diffusées sur les réseaux sociaux, cet article entend interdire la diffusion d'images de policiers en action, sous prétexte que ces images pourraient les exposer à des représailles violentes dans la vie civile.

Les policiers veulent pouvoir travailler sans faire courir de risque à leur famille, ou même risquer des règlements de compte à titre personnel, c'est une chose facile à comprendre et très défendable. La protection des agents en dehors du service est incontestable. Les rapporteurs de la proposition de loi invoquent bien sûr la mort d'un couple de policiers assassinés chez eux, à Magnanville (Yvelines), le 13 juin 2016, par des terroristes islamistes. Ils omettent de dire que ce meurtre terroriste n'a aucun rapport avec la diffusion d'images d'opérations de police sur les

réseaux sociaux. Les rapporteurs et les policiers invoquent aussi les sites de type « *cop watch* » (« surveiller les flics »), qui affichent les visages de policiers s'étant livrés à des violences. Mais c'est masquer une réalité plus vaste.

Sans les images des amateurs, filmant ou photographiant des actions de police, aurait-on entendu parler de la mort de Cédric Chouviat, étouffé en janvier 2020 par trois policiers agenouillés sur sa poitrine, après son arrestation quai Branly, à Paris, parce qu'il avait téléphoné en conduisant son scooter ? Sans les images filmées par des anonymes ou par des professionnels, comment aurait-on documenté les impensables violences qui ont marqué la répression du mouvement des « gilets jaunes » ? En avril 2021, le journaliste David Dufresne, qui a documenté aussi précisément que possible ces violences de la police, dénombrait 353 manifestants blessés à la tête, dont 30 personnes ayant perdu un œil (blessures par balles en caoutchouc), et 5 personnes ayant perdu une main (blessures par grenades explosives)[11]. Dans de très nombreux cas, ces blessures étaient connues grâce aux images tournées au cœur même des manifestations, aussi bien par des manifestants que par des journalistes. L'article 24 est aussitôt et unanimement accueilli comme une volonté d'étouffer les violences policières, de bâillonner les journalistes et les citoyens, et d'empêcher l'exercice d'un droit essentiel pour la préservation de la démocratie.

La corporation des journalistes veille jalousement à la protection de son métier. Hors de question de travailler avec des images fournies par les préfectures, hors de question de ne pas pouvoir travailler au cœur même des mouvements sociaux. Très vite, les journalistes s'organisent, les indépendants comme les membres de grandes rédactions, et donnent au mouvement de protestation, et à l'infâme « Sécurité globale », toute la publicité que leurs moyens leur permettent. Une coordination Stop loi Sécurité globale se met en place : elle regroupe des dizaines de syndicats et d'associations, dont La Quadrature du Net, et lance un appel à manifester le 28 novembre 2020 devant l'Assemblée nationale, où le texte doit être discuté[12].

Cette « marche des libertés » laisse à tous les participants le souvenir d'un grand bol d'air frais. Après des semaines et des mois de confinement, après des mois et des années de manifestations réprimées dans la violence et le sang, c'est une fête. La Quadrature vient en force, avec un grand masque en forme de caméra de surveillance, pour rendre la distribution des tracts plus spectaculaire, et ça marche très bien, la caméra est abondamment photographiée. C'est aussi le vol inaugural de notre « filet à drones », un pauvre filet en ficelles, bricolé en vitesse au Garage, porté par deux grappes de ballons gonflés à l'hélium.

Les ballons colorés et le filet dérisoire font rigoler les gens et donnent un ton potache à la contestation, mais ils nous servent surtout à rappeler sans cesse, de la première à la dernière manifestation du mouvement en janvier 2021, que l'article 24 qui menace la liberté de la presse ne doit surtout pas occulter les autres dangers réels cachés dans le texte de loi, dont l'article 22 sur les drones, ou les quatre articles sur la vidéosurveillance. Les tracts que nous distribuons à chaque manif le rappellent aussi, et tout le rôle capital de Benoît, notre représentant au sein de la coordination Stop loi Sécurité globale, sera de rappeler sans répit aux autres acteurs du mouvement que la loi ne se résume pas à son article 24. C'est alors notre plus grande crainte : que le gouvernement ait introduit l'article 24 comme un chiffon rouge pour détourner l'attention de tous les autres pièges cachés dans le texte, et que l'article soit vite supprimé pour apaiser les journalistes et enterrer la contestation. Nous savons que sans l'appui de la corporation des journalistes et de la caisse de résonance des médias, même la lutte contre les drones n'aura pas la même audience.

Heureusement, la mayonnaise militante prend. Chaque pancarte sur la vidéosurveillance et les drones brandie pendant les manifs contre l'article 24 est une victoire et une joie pour nous. L'association boucle même facilement sa campagne de financement annuel, fin décembre 2020, grâce à un afflux de dons exceptionnel. Nos sujets de travail trouvent un écho dans la société, et ni la surveillance de masse, ni la vidéosurveillance

généralisée ne semblent être devenues des fatalités dans la France de 2020.

En tout cas, la question de la protection des visages de policiers est un point extrêmement sensible pour la hiérarchie policière, et au premier chef pour son ministère de tutelle. En septembre 2020, nous signons et nous relayons une pétition internationale contre la reconnaissance faciale, lancée par l'artiste et militant italien Paolo Cirio[13]. Son travail s'intéresse depuis longtemps aux technologies numériques, au monde qu'elles organisent, aux identités qu'on y tisse, aux libertés qu'elles permettent et à celles qu'elles tuent. Il a contacté la Quadrature après avoir pris connaissance de notre campagne Technopolice, parce qu'il cherchait à mettre sur pied une campagne européenne pour l'interdiction de la reconnaissance faciale et des techniques de profilage biométrique. Solidaires de son travail, nous publions donc sa pétition[14]. Paolo Cirio avait également imaginé une exposition, une campagne d'affichage et un site Web pour sensibiliser à la question de la reconnaissance faciale policière. Sur ces affiches, on pouvait voir des « visages » de policiers casqués et en armure, photographiés dans les innombrables manifestations réprimées durant les deux dernières années : un faux champ de texte invitait les spectateurs à saisir le nom du policier en dessous de son image floue… L'ironie était manifeste et le procédé vieux comme la première contestation : pour montrer la cruauté d'une situation, rien de tel que de l'inverser. Mais le ministère de l'Intérieur protège l'amour-propre de ses troupes et veut surtout leur montrer qu'il les soutiendra jusqu'au bout. M. Darmanin, ministre médiatique, s'empresse donc de menacer sur Twitter l'artiste et le lieu d'exposition qui l'accueillait : « Paolo Cirio : Insupportable mise au pilori de femmes et d'hommes qui risquent leur vie pour nous protéger. Je demande la déprogrammation de "l'exposition" et le retrait des photos de son site, sous peine de saisir les juridictions compétentes[15]. » Le centre d'art déprogramma l'exposition, et le site disparut. Voilà l'ambiance en France en 2020[16].

La loi Sécurité globale est adoptée en avril 2021, avec une série de modifications obtenues en partie par la pression de la rue : l'article 24 est renuméroté et perd l'essentiel de sa substance dangereuse, les drones pourront voler mais avec quelques limitations et quelques conditions[17]. Mais c'est encore trop, ou trop peu, et comme la loi se retrouve devant le Conseil constitutionnel, nous envoyons nos « écritures », élaborées avec d'autres associations (Syndicat des avocats de France, Syndicat de la magistrature, LDH, etc.), pour argumenter en faveur de la censure des articles liberticides[18]. Fin mai 2021, le Conseil constitutionnel censure l'article 24 (devenu 52) punissant la diffusion des images de policiers, interdit la vidéosurveillance continue dans certains « lieux de privation de liberté » (gardes à vue et centres de rétention administrative), ainsi que la surveillance vidéo à partir de drones ou d'hélicoptères : leur nécessité n'est pas démontrée et la loi ne leur mettait pas de limites assez claires. Mais le Conseil constitutionnel formule ses motifs de censure avec une précision qui est souvent, pour un gouvernement têtu, une indication très précise de la marche à suivre pour reformuler ses dispositions dans la loi suivante.

Le gouvernement ne perd pas de temps. Dès février 2021, avant même l'adoption définitive de la loi Sécurité globale, le ministre de l'Intérieur glisse déjà le « délit d'appel à la haine en ligne » à l'encontre des forces de l'ordre dans l'article 18 du projet de loi Séparatisme : l'article 24 affaibli par le Sénat est déjà reformulé dans une autre loi[19]… Passer par la porte et par la fenêtre en même temps, une technique de gouvernement ?

En avril-mai 2021, le gouvernement dépose un nouveau projet de loi « relatif à la prévention d'actes de terrorisme et au renseignement » – que nous surnommons aussitôt « loi Renseignement 2 » : elle complète directement la loi Renseignement de 2015, en pérennisant dans le droit commun des mesures temporaires de l'état d'urgence (facilités de perquisition et de détention) ou diverses mesures expérimentales, comme la surveillance automatisée du réseau par des « algorithmes » surnommés les « boîtes noires ». Mais notre inquiétude est suscitée par des articles

d'apparence anodine. La saisie du matériel informatique des personnes faisant l'objet d'une perquisition par la police (sans intervention d'un juge d'instruction), l'obligation faite aux administrations et aux services sociaux de fournir des informations aux services de renseignement, l'autorisation de larges partages de données entre les services de renseignement, l'extension des boîtes noires aux adresses URL, la confirmation de la conservation des données de surveillance des communications par satellites, plus une disposition floue qui nous fait craindre une attaque contre le chiffrement des communications[20]… Le tout sous couvert de lutte contre le terrorisme, bien évidemment, mais également et au passage pour des motifs tels que le contre-espionnage économique ou la surveillance des mouvements sociaux…

Passée en procédure d'urgence, la loi est discutée à vitesse grand V, nous laissant un sentiment d'épuisement et d'acharnement législatif. Le Parlement, très largement acquis à l'idéologie sécuritaire et au caporalisme de parti qui guide les votes de la majorité, n'ose pas critiquer les pouvoirs exorbitants donnés aux services de renseignement sous couvert de lutte contre le terrorisme, et semble croire sur parole le ministre de l'Intérieur et la délégation parlementaire au renseignement qui répètent sur tous les tons que cette loi est essentielle. Même le Conseil constitutionnel ne voit presque rien à y redire[21]. Il est bien loin le temps où la contestation de la loi Renseignement de 2015 avait été l'occasion de manifestations de rue…

« Loi Séparatisme » et « Loi Audiovisuelle » (printemps-été 2021)

Du côté de la régulation du Web, on doit affronter deux textes de loi en même temps : la loi Audiovisuelle et la loi Séparatisme.

La première, loi « communication audiovisuelle et souveraineté culturelle », supprime enfin la Hadopi – mais pour augmenter et confier ses pouvoirs au CSA, qui devient une nouvelle entité nommée l'Arcom, avec des pouvoirs de régulation et de censure du Web[22].

La deuxième, loi sur le séparatisme, devenue loi sur « le respect des principes de la République », grand fourre-tout de mesures pour détecter ou contrer la radicalisation islamiste, est un prétexte pour mélanger des mesures restrictives des libertés associatives et des mesures de régulation du Web. Son article 18 reprend les éléments de l'article 24 de la loi Sécurité globale (l'interdiction de diffuser des images de policiers identifiables). Son article 19 autorise la fermeture administrative des sites « miroirs » d'un premier site censuré par un juge pour « haine », mesure qu'on retrouve également dans la loi Audiovisuelle pour les sites accusés de « piratage ». Dans les deux cas, la nouvelle Arcom a autorité et gagne de nouveaux pouvoirs.

On compte au moins deux leçons à retenir de ces lois. Première leçon : il s'agit de donner toujours plus de pouvoir à l'administration plutôt qu'à un juge sur Internet. L'idée étant que le juge ne sera pas assez rapide, ni assez efficace, et qu'il faut laisser un peu de marge de manœuvre à l'administration pour réguler Internet. L'Arcom pourra saisir le juge, proposer des mesures aux plateformes, et infliger d'énormes sanctions.

Deuxième leçon : ces lois prétendent s'attaquer aux problèmes d'Internet, à la surpuissance des plateformes, mais ne font en réalité que proposer de plates mesures de modération, de transparence, d'obligations de moyens qui ne remettent jamais en cause le modèle économique sur lequel se fondent ces plateformes. La publicité ciblée, l'économie des données, la captation, la succion même de nos données personnelles pour en faire un business, sont obstinément ignorées. Le RGPD, qui donne précisément un moyen de pression parfait sur l'exploitation non consentie des données personnelles, n'est délibérément pas appliqué, ou exploité.

« LOI DRONES 2 », LA VOITURE-BALAI SÉCURITAIRE (SEPTEMBRE 2021)

En juillet 2021, trois mois à peine après la censure partielle de la loi Sécurité globale par le Conseil constitutionnel, le gouvernement lance déjà, en procédure accélérée, la loi « responsabilité pénale et sécurité intérieure », que nous surnommons aussitôt « Drones 2 ». Voiture-balai de toutes les lois sécuritaires qui l'ont précédée en moins de deux ans, cette loi ornithorynque essaie de reformuler bon nombre de mesures qui ont été censurées. Elle propose en particulier de légaliser les drones policiers, en suivant les recommandations données par la dernière décision du Conseil constitutionnel à ce sujet. Nous ne perdons pas l'occasion de moquer l'entêtement du gouvernement, et de rappeler que les drones ont déjà été interdits quatre fois en deux ans[23]…

Malgré le comique de répétition, le rire est amer. Devons-nous, de guerre lasse, nous résoudre à considérer que notre seul et dernier espace de démocratie sera la saisine du Conseil constitutionnel, organe totalement opaque ? Doit-on être content que face à la mascarade parlementaire, totalement paralysée par la double majorité gouvernementale et présidentielle, le seul contre-pouvoir institutionnel soit… le Conseil constitutionnel ? Si en plus il suffit ensuite au gouvernement de ressortir une nouvelle loi quelques mois après…

UNE « UNION » À LA CARTE ?

L'attitude du gouvernement français à l'égard de ses engagements européens est aussi élastique que sa conception de la démocratie. En même temps que les trois lois dont il vient d'être question, la France mène au sein de l'Union européenne des négociations pour faire avancer deux textes importants. D'une part le DSA, un texte énorme qui encadrera les services en ligne, et notamment les plateformes géantes. D'autre part un règlement pour encadrer l'utilisation de l'intelligence artificielle dans les pays de l'Union. Le gouvernement français pousse dans ces deux textes des propositions sécuritaires et policières identiques à celles qu'il cherche à nous imposer dans son espace domestique. Mieux

encore, il utilise le cadre européen pour tenter de contourner les blocages constitutionnels qu'il rencontre en France et tout bonnement imposer au niveau de l'Union européenne ce qui ne passe pas en France.

Cette volonté était déjà particulièrement visible au moment de la loi Avia « contre la haine », en 2019. Le délai de censure des contenus « haineux » en 24 heures est aggravé, à la fin de la discussion de la loi, par un tour de passe-passe législatif, par l'introduction soudaine d'un délai d'une heure seulement pour la suppression des contenus « terroristes ». Cette mesure est sévèrement censurée par le Conseil constitutionnel. Nous pensions, peut-être par naïveté, qu'une telle gifle suffirait pour convaincre le gouvernement de l'inanité de la mesure. C'était bien mal estimer son audace.

La censure des contenus haineux en 24 heures, confiée aux robots et aux modérateurs des grandes plateformes, se retrouve formulée à l'identique dans le cadre des travaux sur le *Digital Service Act*. La censure des contenus terroristes se retrouve quant à elle dans le « règlement Terro » (« de lutte contre les contenus terroristes »), à l'initiative de la France. Et la mesure repoussée en France fait désormais son chemin dans le texte européen, jusqu'à son adoption finale en mai 2021[24]…

C'est, pour nous, une énorme défaite : dans la lignée de ce qui avait été prévu en France (et appliqué) depuis plusieurs années, la police peut forcer n'importe quel acteur de l'internet (à quelques exceptions) à retirer en une heure un contenu qu'elle considère comme « terroriste ». Le délai d'une heure laisse évidemment, et c'est central ici, prévoir l'utilisation grandissante de la censure automatique, dont les outils sont développés depuis plusieurs années par Facebook, Google, etc.

La France n'hésite donc pas à instrumentaliser l'Union européenne pour imposer le cadre juridique dont elle a besoin pour imposer sa politique sécuritaire domestique. Mais à l'inverse, quand le cadre européen lui déplaît…

LE DROIT CONTRE LES DROITS

Vous vous rappelez sans doute notre contentieux porté devant la CJUE, au sujet de la durée de conservation des données de connexion. Après la très solennelle audience d'octobre 2019[25], la Cour délibère longuement. Elle rend sa décision le 6 octobre 2020 : « Une défaite victorieuse », annonce notre communiqué de réaction à chaud[26]. Victoire, car la Cour affirme bien que la France ne peut plus imposer cette conservation généralisée des données de connexion, mais défaite parce qu'elle fait apparaître un certain nombre de régimes d'exception importants. Nous publions un article qui résume bien l'ambivalence de nos sentiments : bien qu'elle réaffirme des principes juridiques plus protecteurs que le droit français, la décision de la Cour laisse assez de possibilités d'exception pour que nous soyons inquiets pour la suite.

Munis des réponses de la CJUE, nous nous tournons alors vers le Conseil d'État. À son tour, il doit en tirer des conclusions sur la mise en conformité de la loi française. Confiance toute relative cependant, puisque nous jugeons tout de même nécessaire de rappeler publiquement, début avril 2021, la gravité de l'enjeu[27]. Le verdict tombe le 21 avril 2021, et cette fois-ci le titre de notre communiqué n'est d'aucune ambiguïté : « Le Conseil d'État valide durablement la surveillance de masse ». C'est une déception et une défaite énormes pour nous. Nous le savions, il existait des failles dans l'avis de la CJUE, et les petits malins du Conseil d'État, prêts à tout pour soutenir la nécessité d'État de surveiller la population, s'y sont engouffrés : « Le Conseil d'État autorise la conservation généralisée des données de connexion en dehors des situations exceptionnelles d'état d'urgence sécuritaire, contrairement à ce qu'exigeait la Cour de justice de l'UE dans sa décision du 6 octobre 2020 contre la France. Pour arriver à une conclusion aussi brutale, le Conseil d'État a réinterprété la notion de "sécurité nationale" pour l'étendre très largement au-delà de la lutte contre le terrorisme et y inclure par exemple

l'espionnage économique, le trafic de stupéfiants ou l'organisation de manifestations non déclarées[28]. »

La collecte massive et indistincte des données de connexion n'est justifiée que dans le contexte d'une crise exceptionnelle, dit la CJUE ? Fort bien, dit le Conseil d'État, il se trouve que la France est en état d'alerte pour plusieurs raisons… La pirouette cynique plaira tellement que nous entendrons même des parlementaires de droite, de LR à LREM, se réjouir de l'audace et de l'habileté du conseiller d'État qui a dirigé les opérations. N'en doutons plus : l'État français préfère ouvertement l'exercice cynique du droit au respect des droits de ses citoyens.

PEGASUS ET LES « PAS DE LOUP »

Lors des révélations Snowden de 2013, nous avions assisté, un peu ébahis, aux contorsions gênées de nos gouvernants, dont les communications avaient pourtant été captées et enregistrées par les services de « l'allié » américain. On avait vite compris que la France, ayant de toute évidence le même type d'activité, ne pouvait se permettre d'élever l'affaire au rang d'incident diplomatique.

En juillet 2021, Amnesty International révèle, conjointement avec le consortium international de journalistes Forbidden Stories[29], que des dizaines de smartphones appartenant à des personnalités politiques ou médiatiques du monde entier ont été infectés et surveillés au moyen du logiciel espion Pegasus, commercialisé par la société israélienne NSO Group[30].

Un détail compte pour apprécier le sel de l'histoire : NSO Group vend ses outils d'espionnage exclusivement à des États. Autre détail savoureux : on retrouve des traces de Pegasus dans les téléphones de plusieurs ministres et journalistes français. Et, cette fois encore, comme en 2013 : aucune réaction officielle.

Fin novembre 2021, un article publié par *Le Monde* lève un coin du voile. Un article publié aux États-Unis vient d'affirmer que la France était

sur le point de signer un contrat avec NSO Group quand le scandale a éclaté. Le palais de l'Élysée dément aussitôt, en reconnaissant toutefois que l'entreprise avait longtemps et avec insistance courtisé les services français, jusqu'en 2020, et jusqu'au refus catégorique de la France.

Pourquoi ce « non » ? Principalement en raison de la grande porosité du personnel de NSO Group avec les services israéliens et états-uniens. Mais, précise l'article du *Monde* : « Les services de police et de justice ont cependant obtenu que des moyens financiers soient débloqués pour doter les services de renseignement et de justice de l'ensemble des outils nécessaires à un piratage à distance des téléphones. […] À ce jour, les capacités techniques en la matière demeurent loin de celles de Pegasus, et depuis plusieurs années les autorités progressent à pas de loup sur ce sujet miné. Au sein de l'État, on craint d'ailleurs que le scandale autour de Pegasus ne vienne compromettre le développement de cet outil que beaucoup aimeraient voir rejoindre l'arsenal des enquêteurs et des espions français[31]. »

Dès que les services de renseignement français auront développé leur propre outil, les smartphones des habitants du pays seront aussitôt, et dans la plus parfaite légalité, à portée d'écoute, quoi qu'il en coûte.

Si l'effondrement démocratique a largement démarré sous la présidence de Nicolas Sarkozy, et a pu se prolonger sous celle de François Hollande, le quinquennat d'Emmanuel Macron est néanmoins bien lourd : extension des pouvoirs des services de renseignement, nouveaux fichiers de police et bases de données massives, accélération du pouvoir de censure de l'administration, nombreux partenariats avec des entreprises sécuritaires pour démultiplier la surveillance sur Internet ou dans nos rues, utilisation massive de la reconnaissance faciale policière… Il aura directement contribué au basculement, toujours plus rapide, toujours plus profond, vers une société sécuritaire reposant sur la surveillance et la censure, qu'elle soit d'origine étatique ou privée, les deux étant ici souvent mêlées.

CONCLUSION

Les risques liés au numérique évoluent à mesure que l'humanité l'invente et le découvre. Dans ce contexte en constante mutation, nous nous essayons à de nouvelles formes de lutte pour défendre les valeurs que la Quadrature incarne. Sans jamais être certains de l'issue des batailles.

Les sujets sont protéiformes. Les attaques viennent autant d'entreprises privées, petites ou grandes, françaises ou internationales, que des gouvernements. Aucune solution n'est simple et évidente. Il nous faut donc trouver comment mobiliser l'opinion publique, comment l'embarquer dans nos combats, à la croisée du droit, de la technologie et de la politique. Informer et agir, et tenter toujours d'être le plus efficace possible, dans les limites de nos ressources humaines et financières. La lutte ne pourra jamais être menée par quelques militants seulement, elle ne peut se restreindre à une seule, ni même à plusieurs associations.

Augmenter le coût politique d'attaquer les libertés fondamentales est l'un de nos objectifs depuis le départ. Mais l'effort que nécessite cette stratégie est considérable. La censure, la violation de la neutralité du Net, la surveillance des réseaux, la vidéosurveillance algorithmique… : les rendre inacceptables aux yeux de tout un chacun est la seule manière d'obtenir une victoire ferme et pérenne. Transformer des sujets d'experts en évidences culturelles, c'est peut-être l'ultime défi de La Quadrature du Net.

Nous continuerons à aller dans les médias, à participer à des événements associatifs, à répondre aux invitations partout en France et en Europe dès qu'il s'agira de sujets liés aux libertés dans l'espace numérique. Mais c'est surtout sur vous que repose ce travail de conviction. Pour dépasser nos cercles proches et diffuser nos idées, vos idées, dans la société, c'est sur vous que nous comptons. En offrant, par exemple, ce livre à vos amis ! En leur expliquant le danger inhérent à la publicité ciblée ou à la surveillance totale(-itaire) de l'espace public. En rejoignant une association locale. Et surtout, en vous rappelant que la force d'une démocratie repose moins sur un vote une fois tous les cinq ans que sur l'engagement de citoyennes et de citoyens au quotidien, pour contrebalancer le pouvoir d'un État qui peut si facilement dériver.

BIBLIOGRAPHIE

Philippe Aigrain, *Cause commune. L'information entre bien commun et propriété*, Paris, Fayard, coll. « Transversales », 2005.

Philippe Aigrain, *Sharing : culture and the economy in the Internet age*, Amsterdam, Amsterdam University Press, 2012.

Yaël Benayoun et Irénée Régnauld, *Technologies partout, démocratie nulle part. Plaidoyer pour que les choix technologiques deviennent l'affaire de tous*, Limoges, Fyp, coll. « Essais critiques », 2020.

Cory Doctorow, *Little Brother*, Paris, Pocket jeunesse, 2011 (roman).

Michel Foucault, *Surveiller et punir. Naissance de la prison*, Paris, Gallimard, coll. « Bibliothèque des histoires », 1992.

Amaelle Guiton, *Hackers, au cœur de la révolution numérique*, Vauvert, Au Diable Vauvert, 2013.

François Jarrige, *Technocritiques. Du refus des machines à la contestation des technosciences*, Paris, La Découverte, coll. « La Découverte-poche », 2016.

Naomi Klein, *La Stratégie du choc*, Arles, Actes Sud, coll. « Questions de société », 2008 (poche Babel, 2013).

Élodie Lemaire, *L'œil sécuritaire. Mythes et réalités de la vidéosurveillance*, Paris, La Découverte, coll. « L'Envers des faits », 2019.

Jean-Marc Manach, *La vie privée, un problème de vieux cons ?* Limoges, Fyp, coll. « Présence : essai », 2010.

Groupe Marcuse (Mouvement autonome de réflexion critique à l'usage des survivants de l'économie), *De la misère humaine en milieu publicitaire. Comment le monde se meurt de notre mode de vie*, Paris, La Découverte, coll. « La Découverte-poche », 2010.

Cathy O'Neil, *Algorithmes, la bombe à retardement*, Paris, Les Arènes, 2018.

Anne-Sophie Simpere et Pierre Januel, *Comment l'État s'attaque à nos libertés. Tous surveillés et punis*, Paris, Plon, 2022.

Edward Snowden, *Mémoires vives*, Paris, Seuil, 2019.

Olivier Tesquet, *À la trace. Enquête sur les nouveaux territoires de la surveillance*, Paris, Premier parallèle, 2019.

Jérôme Thorel, *Attentifs ensemble ! L'injonction au bonheur sécuritaire*, Paris, La Découverte, coll. « Cahiers libres », 2013.

Félix Tréguer, *L'utopie déchue. Une contre-histoire d'Internet XVe-XXIe siècle*, Paris, Fayard, coll. « À venir », 2019.

Shoshanna Zuboff, *L'âge du capitalisme de surveillance. Le combat pour un avenir humain face aux nouvelles frontières du pouvoir*, Paris, Zulma, coll. « Z a », 2022.

BIOGRAPHIES DES AUTEURS

Mathieu Labonde est responsable administratif et financier de La Quadrature du Net. Après des études littéraires, il a travaillé dans la communication puis dans la presse technique et scientifique, avant d'écrire des romans de vulgarisation pour adolescents et de rejoindre La Quadrature du Net en 2015.

Lou Malhuret est membre de La Quadrature du Net. Spécialiste des questions d'organisation, Lou a également co-fondé le Reset, un hackerspace queer et féministe, et participé à d'autres aventures bénévoles au sein de hackerspaces et d'associations LGBTQI+.

Benoît Piédallu participe aux activités de La Quadrature du Net depuis 2011 et en est membre bénévole depuis 2017. Chef de projet informatique pour le déploiement de logiciels libres, il travaille plus particulièrement sur les dossiers liés aux données personnelles et de santé, ainsi que sur l'IA et la technopolice.

Axel Simon est spécialiste du logiciel libre et open source, et de la sécurité des systèmes d'information. Il travaille à la croisée de ces deux mondes. Il est également membre de La Quadrature du Net, à laquelle il contribue depuis plus de dix ans, dans un premier temps en tant que salarié, puis comme bénévole.

REMERCIEMENTS

Nous remercions toutes celles et ceux qui ont fait de La Quadrature du Net ce qu'elle a été et qui font ce qu'elle est aujourd'hui : activistes, militantes et militants, donatrices et donateurs, partenaires et camarades, journalistes, et même femmes et hommes politiques…

NOTES

. AUX ORIGINES DE LA LUTTE

1 https://www.cairn.info/revue-mouvements-2014-3-page-122.htm

http://www.confessions-voleur.net/confessions/node1.html

2 À ses côtés, on retrouve des noms connus du logiciel libre : Meryem Marzouki, Stéphane Bortzmeyer…

3 Le WCT, qui compte aujourd'hui 50 signataires : https://www.wipo.int/treaties/fr/ip/wct/summary_wct.html

4 https://www.eff.org/fr/cyberspace-independence

5 https://groups.google.com/g/fr.soc.divers/c/GKmAu8w1M9w?pli=1

6 https://ecosphere.wordpress.com/2017/01/08/retour-sur-lamendement-fillon-de-1996/ ;

https://www.conseil-constitutionnel.fr/decision/1996/96378DC.htm

7 http://www.journaldunet.com/solutions/0702/070202-enquete-syndicalisme-informatique/2.shtml

8 https://www.legifrance.gouv.fr/loda/id/JORFTEXT000000801164/

9 Pour répondre à la crainte du « vol de musique », une alliance « Public-artistes » est lancée par des sociétés de gestion des droits d'auteur et des associations de consommateurs. Musiciens, photographes, dessinateurs, producteurs, ou encore plasticiens se mobilisent en faveur d'une autorisation d'accès aux contenus culturels en ligne et d'échanges de ces contenus à des fins non commerciales, en contrepartie d'une rémunération versée aux artistes à l'occasion du paiement de l'abonnement Internet.

10 https://www.fdn.fr/actions/confs/Internet-libre-ou-minitel-2-0/

11 https://www.silicon.fr/adsl-france-telecom-encore-condamne-par-la-justice-europeenne-20134.html

12 https://www.numerama.com/magazine/5692-quand-nicolas-sarkozy-oppose-l-Internet-au-monde-civilise.html

13 https://www.vie-publique.fr/discours/166383-declaration-de-m-nicolas-sarkozy-president-de-lump-et-candidat-lel

14 https://archive.wikiwix.com/cache/index2.php?url=http%3A%2F%2Fwww.laquadrature.net%2Ffr%2Fnode%2F39#federation=archive.wikiwix.com

. HADOPI, OU L'HISTOIRE D'UN PASSAGE EN FORCE

1 Les sanctions seraient pensées en fonction de la gravité des faits et de l'entêtement des contrevenants, les peines allant d'une simple lettre de mise en garde jusqu'à une amende voire à une peine de prison pour les récidivistes, accompagnée d'une coupure de la connexion Internet.

2 « Le Parlement européen torpille la riposte graduée ! », *Next INpact*, 10 avril 2008 : https://www.nextinpact.com/archive/42915-cult-bono-vote-riposte-graduee.htm

3 https://www.journaldunet.com/ebusiness/le-net/1032548-la-reponse-graduee-du-rapport-olivennes-perd-son-grade/ ;

https://www.laquadrature.net/2008/04/10/le-parlement-europeen-rejette-la-riposte-graduee/

4 https://www.laquadrature.net/2009/11/24/paquet-telecom-une-occasion-manquee-pour-les-droits-des-citoyens/

5 Six mois plus tard, à l'été 2009, est embauché Félix Tréguer. Le jeune homme de 22 ans sort alors tout juste de Sciences-po et écrit à l'association pour proposer sa candidature. Il rencontre Jérémie et le courant passe tout de suite : Félix Tréguer est le premier salarié non fondateur de l'association (via FDN2).

6 https://www.laquadrature.net/files/LaQuadratureduNet-Riposte-Graduee_reponse-inefficace-inapplicable-dangereuse-a-un-faux-probleme.pdf

7 Le 21 février 2009 : https://www.laquadrature.net/2009/02/22/lci-plein-ecran-du-21022009-piratage-pourquoi-une-loi-de-plus-wattv/

8 http://mediakit.laquadrature.net/formats/12/7.flv

9 Ce comportement leur vaudra le surnom de « députés godillots », qui devient le nom d'un site Internet permettant aux citoyens de suivre le travail parlementaire de leurs représentants (ces derniers le prendront très mal). https://www.deputesgodillots.info/depute-2-mois-et-60-deputes-godillots.html

10 Décision 2009-580 du Conseil constitutionnel, le 10 juin 2009 : https://www.conseil-constitutionnel.fr/decision/2009/2009580DC.htm.

11 Aujourd'hui Rakuten.

12 Vidéo de l'intervention de John Perry Barlow au e-G8 : https://www.youtube.com/watch?v=JX4ciDBHfNU

13 « e-G8 : Deux visions du Net irréconciliables ? », *20 minutes*, 24 mai 2011 : https://www.20minutes.fr/web/729886-20110524-e-g8-deux-visions-net-irreconciliables

14 Site de la campagne « Internet vs G8 » : http://g8internet.com

. LE COMBAT CONTRE L'ACTA

1 https://www.europarl.europa.eu/doceo/document/TA-7-2010-0058_FR.html

2 En retour, la Grande-Bretagne ne respectait pas le copyright des auteurs américains, dont Edgar Allan Poe.

3 https://www.laquadrature.net/files/flyers/LQDN-20120222_NO_to_ACTA_v1-3.pdf

4 https://upload.wikimedia.org/wikipedia/commons/2/2b/Google_Doodle_Censored_2.png

. CES POLITIQUES QUI N'ONT RIEN COMPRIS

1 Lors des débats Hadopi, à un député demandant comment au juste les citoyens utilisant des logiciels libres seraient censés sécuriser leur accès à Internet (le défaut de sécurisation étant ce que la loi Hadopi se proposait de punir), la ministre explique maladroitement que des pare-feu gratuits existent, citant la suite bureautique OpenOffice qu'utilise son ministère comme exemple : https://www.assemblee-nationale.fr/13/cri/2008-2009/20090211.asp

2 https://www.numerama.com/magazine/12233-pour-albanel-la-quadrature-du-net-c-est-5-gus-dans-un-garage.html ;

https://www.nextinpact.com/archive/49575-quadrature-gus-garage-internet-depeche.htm

3 http://www.politique.net/2009031201-nicolas-sarkozy-a-t-il-deja-envoye-un-e-mail.htm

4 https://www.liberation.fr/france/2009/06/18/fillon-ce-vrai-geek_565464/

5 https://www.liberation.fr/ecrans/2009/04/30/peer-to-peer-moi-je-parle-francais-excusez-moi_958546/ ;

https://www.nextinpact.com/archive/53070-hadopi-p2p-reponses-deputes-bakchich.htm ;

https://www.dailymotion.com/video/k5717nCr79Ob4tZ833

6 Rapport du 23 janvier 2011 téléchargeable sur le site de la Hadopi : https://www.hadopi.fr/ressources/etudes/etude-presentation-de-letude-hadopi-cannes-lors-du-midem-23-janvier-2011. Voir en particulier la page 9 de la synthèse courte (PDF téléchargeable).

7 https://leplus.nouvelobs.com/contribution/2053-campagne-de-pub-hadopi-une-pur-arnaque.html

8 https://www.liberation.fr/ecrans/2011/06/08/hadopi-perdue-en-naze-campagne_953991/

9 https://www.dailymotion.com/video/x94ta5

10 https://wiki.laquadrature.net/Compte-rendu_du_quadr%27ap%C3%A9ro_du_25_mars_2011

11 https://cloud.lqdn.fr/s/EJNneKzm2cfz3nq

12 https://www.laquadrature.net/2012/11/28/datalove-sur-cle-usb-pour-appeler-les-eurodeputes-a-reformer-le-droit-dauteur/

13 https://diybookscanner.org/

14 https://www.bookscanner.fr/le-bookscanner-a-silicon-valois.html

. CES POLITIQUES QUI VEULENT TOUT CONTR LER

1 Voir Grégoire Chamayou, *La Société ingouvernable*, Paris, La Fabrique, 2018 et Bruno Amable, *La Résistible Ascension du néolibéralisme*, Paris, La Découverte, 2021.

2 https://www.laquadrature.net/2009/09/04/il-est-crucial-de-preserver-la-neutralite-du-net/

3 Pour une explication technique courte et claire, voir cet article de Benjamin Bayart, « La diffusion de la télévision linéaire comme service géré », 20 mai 2016 : https://www.laquadrature.net/2016/05/20/La-diffusion-de-la-television-lineaire-comme-service-gere/

4 https://www.laquadrature.net/2009/09/04/il-est-crucial-de-preserver-la-neutralite-du-net/

5 « Mme Kroes, les laisserez-vous contrôler Internet ? », 21 juillet 2011 : https://www.laquadrature.net/2011/07/21/mrs-kroes-will-you-let-them-control-the-net/.

6 « Réponse à la consultation de l'ARCEP sur la qualité de service de l'accès Internet » : https://www.laquadrature.net/2012/02/17/reponse-a-la-consultation-de-larcep-sur-la-qualite-de-service-de-lacces-a-internet/

7 Adrienne Charmet et Agnès de Cornulier ont remplacé Jérémie Zimmermann.

8 https://www.laquadrature.net/2014/04/03/neutralite-du-net-un-grand-pas-en-avant-pour-linternet-libre/

9 « Propositions positives » publiées en juillet 2011 : https://www.laquadrature.net/2016/01/21/

10 https://www.nextinpact.com/archive/44018-filtrage-internet-neutralite-FAI-operateurs.htm

11 « Big Brother : Sarkozy en rêvait, Fillon le fait », 24 juin 2008 : https://www.laquadrature.net/2008/06/06/big-brother-sarkozy-en-revait-fillon-le-fait/.

. LA FIN DE L'INNOCENCE

1 DDoS : *Distributed Denial of Service*. Attaque par déni de service distribué. L'attaquant multiplie le nombre de requêtes adressées à un site Internet, jusqu'à ce que, submergé, le serveur ne parvienne plus à répondre aux requêtes reçues. Le site n'est alors plus disponible pour les personnes qui souhaiteraient le consulter.

2 JSTOR : contraction de *Journal Storage*. Bibliothèque numérique dans laquelle sont archivées nombre de publications universitaires et scientifiques, rendues disponibles en consultation payante. Les universités payent souvent des accès JSTOR aux étudiants travaillant sur des projets de recherche.

3 IRC : *Internet Relay Chat*. Un réseau distribué de chat anonyme en ligne, sur lequel les gens se reconnaissent par leurs pseudos. En quelque sorte, un ancêtre

de MSN ou Slack, mais libre, ouvert, distribué et anonyme.

4 https://reflets.info/articles/opsyria-quand-internet-ne-laisse-pas-tomber-les-citoyens-syriens

5 OpSyria – Itw d'okhin : https://www.francetvinfo.fr/monde/proche-orient/telecomix-des-hactivistes-au-secours-du-peuple-syrien_62941.html

6 https://theworld.org/stories/2012-06-01/battle-hacktivists-anonymous-vs-telecomix

7 https://reflets.info/articles/opsyria-syrian-censorship-logs-season-3

8 https://rsf.org/fr/rapports/entre-surveillance-et-filtrage-la-breche-tenue-des-net-citoyens

9 Il nous parait compliqué de parler de Julian Assange sans aborder les accusations d'agressions sexuelles à son encontre, pour lesquelles il a fait l'objet d'une enquête préliminaire par le parquet suédois dès 2010. Ces accusations ont été utilisées politiquement dans le cadre du harcèlement judiciaire international dont il a été victime. L'enquête a été classée en 2019, peu après son arrestation dans l'ambassade d'Equateur par la police britannique, au mépris de son droit à l'asile politique.

10 Du nom donné par l'administration américaine à ses campagnes militaires à la suite des attentats du 11 septembre 2001.

11 La Tea House se veut un lieu « analogique », qui détonne dans un environnement très numérique. L'objectif est d'en faire un espace de discussion, de pousser les gens à discuter ensemble, autour d'une tasse de thé.

12 Tardis : *Time And Relative Dimensions In Space*. Référence à la machine à voyager dans le temps et l'espace de la série anglaise *Doctor Who*.

13 Tor mettra fin à sa collaboration avec Jacob Appelbaum en juin 2016, à la suite d'allégations d'abus sexuels, qu'il nie. Celles-ci ont eu des répercussions importantes dans la communauté de la sécurité de l'informatique, qui a alors pris conscience des abuseurs potentiels qu'elle peut receler.

. DU PRÉTEXTE À LA PANIQUE ANTITERRORISTE

1 https://www.defense.gouv.fr/content/download/206186/2286591/Livre-blanc-sur-la-Defense-et-la-Securite-nationale%202013.pdf

2 https://www.lemonde.fr/technologies/article/2013/11/26/surveillance-d-internet-inquietudes-autour-de-la-loi-de-programmation-militaire_3518974_651865.html

3 https://www.lemonde.fr/blog/bugbrother/2013/12/10/tout-ce-que-vous-avez-toujours-voulu-savoir-sur-la-lpm-et-que-vous-avez-ete-nombreux-a-me-demander/ ; https://lexpansion.lexpress.fr/high-tech/notre-liberte-sur-internet-est-elle-menacee-par-la-loi-de-programmation-militaire_1327415.html

4 https://www.laquadrature.net/2013/12/13/loi-de-programmation-militaire-les-parlementaires-doivent-saisir-le-conseil-constitutionnel/

5 https://www.assemblee-nationale.fr/14/propositions/pion1907.asp

6 https://www.assemblee-nationale.fr/14/rapports/r2697.asp

7 Voir par exemple https://exegeteamateur.github.io/

. LE TERRORISME PARTOUT

1 https://www.laquadrature.net/2015/01/09/charliehebdo-non-a-linstrumentalisation-securitaire/

2 https://www.numerama.com/politique/31824-sites-terroristes-le-gouvernement-notifie-son-projet-de-blocage-a-bruxelles.html

3 Connue sous le nom d'« article 49.3 »

4 https://www.lefigaro.fr/secteur/high-tech/2015/06/23/32001-20150623ARTFIG00268-loi-renseignement-les-opposants-tirent-leur-derniere-cartouche.php

5 https://www.laquadrature.net/2015/07/23/honte-sur-la-france-le-conseil-constitutionnel-valide-largement-la-loi-renseignement

6 https://www.laquadrature.net/2015/02/18/decret-lpm-la-quadrature-du-net-depose-un-recours-devant-le-conseil-detat/

7 https://exegetes.eu.org/dossiers/abrogationretention/index.html

8 https://www.laquadrature.net/2015/06/05/premiere-victoire-pour-les-citoyens-contre-la-surveillance-la-loi-de-programmation-militaire-devant/

9 https://exegetes.eu.org/dossiers/renseignement/index.html

1 https://section-ldh-toulon.net/deux-ex-lyceennes-anti-CPE-vont.html

2 https://www.lefigaro.fr/actualite/2007/05/16/01001-20070516ARTFIG90039-prelevements_de_salive_le_front_du_refus_s_organise.php

3 https://www.nextinpact.com/article/48209/plus-dun-tiers-francais-sont-fiches-dans-fnaeg

4 https://www.legifrance.gouv.fr/loda/id/JORFTEXT000031473404/

5 https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000031500831/

6 https://www.lemonde.fr/societe/article/2015/11/27/les-militants-de-la-cop21-cible-de-l-etat-d-urgence_4818885_3224.html

7 https://www.liberation.fr/france/2015/11/29/cop-21-malgre-l-interdiction-manifestation-tendue-en-cours-place-de-la-republique-a-paris_1417000/

8 https://www.monde-diplomatique.fr/2019/01/BONELLI/59444

9 https://www.lemonde.fr/idees/article/2017/10/11/conseil-d-etat-quand-les-recours-n-aboutissent-pas-ou-peu_5199605_3232.html

10 https://www.arretsurimages.net/articles/etat-durgence-cop-21-laveu-de-hollande-que-personne-na-releve

11 https://web.archive.org/web/20160624210105/http://necmergitur.paris/

12 https://www.laquadrature.net/2016/05/27/Sale-prin-temps-pour-les-libertes/

13 https://www.laquadrature.net/2016/03/17/crime-organise-terrorisme-etat-urgence-libertes-danger/

14 https://www.assemblee-nationale.fr/dyn/14/dossiers/lutte_atteintes_securite_publique

15 https://www.assemblee-nationale.fr/dyn/14/dossiers/lutte_crime_organise_terrorisme

16 L'historien des sciences Evgeny Morozov développe la notion de « solutionnisme technologique » dans son ouvrage *Pour tout résoudre cliquez ici. L'aberration du solutionnisme technologique* (FYP Éditions, 2014). « Derrière ce mot se cache l'idée que, pour ses thuriféraires, tout aspect de la société n'est en fait qu'un problème à résoudre : la sécurité, le transport, la santé, l'éducation, la politique, l'alimentation… Tout doit être fait pour gommer les défauts du système, atteindre la perfection, augmenter l'efficacité. […] Bref, le solutionniste possède un marteau (le Web, Internet, de puissants ordinateurs…) et tout

ressemble à un clou. La réflexion sur les questions de société disparaît devant l'attrait de la nouveauté. » (« Contre le solutionnisme numérique », *Le Monde,* 24 octobre 2014.)

17 https://www.correze.gouv.fr/Politiques-publiques/Securite-et-protection-des-populations/Securite-Civile/Le-Systeme-d-Alerte-et-d-Information-aux-Populations-SAIP

18 https://www.vie-publique.fr/loi/20767-loi-prorogeant-lapplication-de-la-loi-ndeg-55-385-du-3-avril-1955-relativ

19 https://www.lemonde.fr/societe/article/2016/04/12/comment-la-dgse-a-surveille-thierry-solere_4900451_3224.html

20 GSM : *Global System for Mobile Communication,* « système global pour les communications mobiles » ; RFID : *Radio Frequency IDentification*, « méthode d'identification utilisant les fréquences radio » ; NFC : *Near Field Communication*, « communication en champ proche ».

21 https://exegetes.eu.org/posts/censure-surveillance-hertzienne-incontrolee/

22 https://exegetes.eu.org/dossiers/etatdurgencetempsreel/index.html

. PROTÉGER NOS DONNÉES : LE RGPD EN RENFORT

1 https://www.laquadrature.net/2016/05/17/quadrature_du_net_hors_etat_urgence/

2 https://www.laquadrature.net/2017/12/20/cnil_whatsapp/

3 Le G29 devient le Comité européen de la protection des données (CEPD) à l'entrée en vigueur du RGPD.

4 https://www.laquadrature.net/2018/07/20/teemo_fidzup/

5 Rappelons de nouveau que notre consentement ne doit pas seulement être « explicite » mais aussi « libre » : un bouton « je refuse » doit être proposé et le site doit rester accessible même si on ne clique pas sur « j'accepte ».

6 https://www.laquadrature.net/2017/03/06/ePrivacy_recommandations_LQDN/

7 https://eprivacy.laquadrature.net/fr/

8 https://www.laquadrature.net/2017/11/06/eprivacy_bilan_pe/

9 Un règlement européen est d'application directe dans les législations nationales dès son entrée en vigueur. Une directive européenne doit être transposée dans le

droit national dans un certain délai. Dans le cas du RGPD, plusieurs points peuvent néanmoins être adaptés en droit national, par exemple l'âge minimum pour s'inscrire sur un réseau social (à défaut, une valeur est proposée par le RGPD).

10 En théorie, une directive pose des principes généraux qui doivent être transcrits en droit national. Ces dernières années, les directives sont devenues de plus en plus précises, quand les règlements, s'appliquant directement dans tous les États, contiennent de plus en plus de parties à préciser par chaque État.

11 https://www.laquadrature.net/2018/01/18/pjl_rgpd_amendements/

12 http://www.assemblee-nationale.fr/15/amendements/0592/AN/20.asp

13 La CNIL exige notamment que le service en question imposant le traitement de données personnelles à des fins publicitaires ou le paiement d'un abonnement n'ait pas une position dominante dans son secteur et que des services alternatifs existent.

. MULTIPLICATION DES FRONTS : L'HEURE DES CHOIX

1 https://www.laquadrature.net/elements-pour-la-reforme-du-droit-dauteur-et-des-politiques-culturelles-liees

2 https://www.laquadrature.net/2015/01/20/reforme-du-droit-dauteur-le-parlement-europeen-doit-suivre-le-rapport-reda

3 https://www.laquadrature.net/2018/10/01/les-quadratures-de-nos-vies

4 https://www.consilium.europa.eu/fr/press/press-releases/2017/06/22/euco-security-defence/

. DE LA DÉMOCRATIE NUMÉRIQUE À L'EFFRITEMENT DE LA DÉMOCRATIE

1 http://www.sharing-thebook.com/

2 https://www.republique-numerique.fr/consultations/projet-de-loi-numerique/consultation/consultation/opinions/section-1-ouverture-des-donnees-publiques-1/le-code-source-d-un-logiciel-est-un-document-administratif-communicable

3 https://www.republique-numerique.fr/consultations/projet-de-loi-numerique/consultation/consultation/opinions/section-2-service-public-de-la-donnee-1/

utiliser-les-logiciels-libres-gnu-linux-dans-les-ecoles-et-les-universites

4 http://www.nextinpact.com/news/100511-on-a-compare-loi-numerique-aux-avis-consultation-en-ligne.htm

5 https://www.laquadrature.net/2016/01/06/promouvoir-les-communs/

6 https://www.mediapart.fr/journal/france/120716/loi-numerique-axelle-lemaire-s-explique-sur-les-arbitrages-perdus-et-gagnes

7 https://www.laquadrature.net/2016/07/13/axelle-lemaire-ou-pas/

8 https://en-marche.fr/evenements/cafe-politique-quelle-vie-privee-dans-nos-societes-connectees

9 https://www.contrepoints.org/2021/10/13/408572-collectif-citoyen-sur-la-vaccination-ne-cherchez-pas-il-nexiste-plus

10 https://en-marche.fr/emmanuel-macron/le-programme/numerique

11 https://www.nouvelobs.com/economie/20150107.OBS9413/macron-il-faut-des-jeunes-francais-qui-aient-envie-de-devenir-milliardaires.html

. LA CAMPAGNE GAFAM

1 https://twitter.com/laquadrature/status/944148790684069888

2 Toutes les conférences sont visibles sur https://media.ccc.de/c/34c3

3 https://www.ccc.de/en/

4 https://photos.cloudfrancois.fr/201712-34c3-leipzig/

5 https://www.laquadrature.net/2018/05/21/plaintegafam/

6 https://www.youtube.com/watch?v=VtvjbmoDx-I ; https://startuffenation.fail/

7 D'après leurs déclarations auprès de la Haute Autorité pour la transparence de la vie publique. https://www.hatvp.fr/

8 Article 7, §4, et considérant 43 du RGPD, interprétés par le groupe de l'article 29.

9 En 2017, la CNIL a d'ailleurs condamné Facebook à 150 000 euros d'amende pour avoir réalisé ses traitements sans base légale. Elle considérait alors que « l'objet principal du service [était] la fourniture d'un réseau social [...], que la combinaison des données des utilisateurs à des fins de ciblage publicitaire ne correspond[ait] ni à l'objet principal du contrat ni aux attentes raisonnables des utilisateurs ».

10 Les personnes qui ne s'inscrivent pas sur la plateforme ont quand même un profil sur celle-ci, créé par l'entreprise pour les représenter dans le « graphe social » des inscrits, et permettre au réseau social d'être le plus « complet » possible.

11 Dernière condamnation en date : en septembre 2021, la CNIL irlandaise a condamné Facebook à 225 millions d'euros d'amende pour violation des données personnelles par WhatsApp.

12 https://www.pnas.org/doi/pdf/10.1073/pnas.1218772110

13 https://www.cnet.com/tech/services-and-software/youtube-ces-2018-neal-mohan/

14 Voir notamment son entretien dans le numéro 5 de la revue *Vraiment*, paru le 18 avril 2018.

15 https://www.cnil.fr/fr/la-formation-restreinte-de-la-cnil-prononce-une-sanction-de-50-millions-deuros-lencontre-de-la

16 https://noyb.eu/wp-content/uploads/2018/05/complaint-android.pdf

17 À ce jour, la Quadrature n'a toujours pas accès au texte de la décision luxembourgeoise, que celle-ci maintient secrète. Un recours est en cours auprès de la Commission d'accès aux documents administratifs (CADA).

18 https://www.bloomberg.com/news/articles/2021-07-30/amazon-given-record-888-million-eu-fine-for-data-privacy-breach

19 Malheureusement, l'omerta de la CNPD ne permet pas de savoir si la mise en conformité a eu lieu, ni si les astreintes ont été payées. La Quadrature travaille actuellement à obtenir les informations sur ces décisions dont elle n'a pas été tenue au courant, alors même qu'elle était à l'origine de la plainte.

20 https://www.arretsurimages.net/chroniques/clic-gauche/la-france-un-gafam-comme-les-autres-pour-darmanin

. NAISSANCE DE LA TECHNOPOLICE

1 Vidéosurveillance à Moirans en Isère : https://www.laquadrature.net/2021/03/12/une-videosurveillance-peut-en-cacher-une-autre/.

2 Deuxième interdiction des drones par le Conseil d'État : https://www.laquadrature.net/2020/12/22/interdiction-des-drones-victoire-totale-contre-le-gouvernement/.

3 Claire Legros, « À Marseille, le Big Data au service de la sécurité dans la ville », *Le Monde*, 8 décembre 2017 : https://www.lemonde.fr/smart-cities/article/2017/12/08/a-marseille-le-big-data-au-service-de-la-securite-dans-la-ville_5226528_4811534.html.

4 Émile Durkheim, *Le Suicide*, étude de sociologie publiée en 1897.

5 John Perry Barlow, *Déclaration d'indépendance du cyberespace*, 1996 : https://fr.wikipedia.org/wiki/D%C3%A9claration_d%27ind%C3%A9pendance_du_cyberespace.

6 Célèbre formule due à Patrick Le Lay, alors dirigeant de TF1, qui résumait en 2004 le travail de sa chaîne en ces termes : « Ce que nous vendons à Coca-Cola, c'est du temps de cerveau humain disponible. »

7 Dans un article de novembre 2015, après les attentats à Paris, Olivier Tesquet dresse un rapide historique de la prospérité de cette triste formule, passée de la bouche de Jean-Marie Le Pen dans les années 1980 à celle de toute personnalité politique qui veut se donner un air de responsabilité aujourd'hui : https://www.telerama.fr/medias/la-securite-est-la-premiere-des-libertes-de-le-pen-a-valls-la-formule-s-est-imposee-dans-le-debat-politique,134465.php.

8 « Outil Big Data de la tranquillité publique » : terme utilisé dans un document administratif, le Cahier des clauses techniques particulières (CCTP), que la Quadrature s'est procuré et a rendu public en mars 2018 : https://www.laquadrature.net/files/CCTP_ObservatoireBigData_Marseille.pdf.

9 Claire Legros, *op. cit.*

10 On se souviendra par exemple que, dans les premiers jours du premier confinement sanitaire de mars 2020, les opérateurs téléphoniques avaient pu dire que 17 % de la population de l'Île-de-France avait quitté la ville pour se confiner ailleurs : https://www.lemonde.fr/pixels/article/2020/03/26/confinement-plus-d-un-million-de-franciliens-ont-quitte-la-region-parisienne-en-une-semaine_6034568_4408996.html.

11 Voir par exemple cette présentation de la notion de « *smart city* » sur le site du Centre d'études et d'expertise sur les risques, l'environnement, la mobilité et l'aménagement (Cerema) : https://smart-city.cerema.fr/territoire-intelligent/definition-smart-city.

12 On voit encore la mention de la modification au pied de l'article accessible en ligne.

13 « La surveillance policière dopée aux Big Data arrive près de chez vous ! », 20 mars 2018 : https://www.laquadrature.net/2018/03/20/surveillance_big_data_marseille/.

14 CCTP, consultable sur le site de La Quadrature du Net : https://www.laquadrature.net/files/CCTP_ObservatoireBigData_Marseille.pdf.

15 *Robocop*, film de Paul Verhoeven sorti en 1987 : le fantasme de prévenir le crime ne date pas de 2017 !

16 *Minority Report*, film de Steven Spielberg d'après une nouvelle de Philip K. Dick, 2002.

17 Isabelle Bellin, « Sécurité publique : que dire de la police prédictive ? », *Data Analytics Post*, 28 mai 2020 : https://dataanalyticspost.com/securite-publique-que-dire-de-la-police-predictive/.

. LA TECHNOPOLICE EST DÉJÀ PARTOUT : RETOUR SUR UN FUTUR SANS AVENIR

1 « La "débâcle" de la sécurité privée des JO de Londres », *Le Figaro*, 17 juillet 2012 : https://www.lefigaro.fr/international/2012/07/17/01003-20120717ARTFIG00558-la-debacle-de-la-securite-privee-des-jo-de-londres.php.

2 « La sécurité des JO de Londres vire au fiasco », France Info Sports, 17 juillet 2012 : https://www.francetvinfo.fr/sports/jo/la-securite-des-jo-de-londres-vire-au-fiasco_119645.html.

3 « Londres teste sa sécurité avant les JO », *Libération*, 30 avril 2012 : https://www.liberation.fr/planete/2012/04/30/londres-teste-sa-securite-avant-les-jo_815356/.

4 « Pékin 2008. Des Jeux sous haute surveillance », *Courrier international*, 31 juillet 2008 : https://www.courrierinternational.com/article/2008/07/31/des-jeux-sous-haute-surveillance.

5 Site Web de Big Brother Watch : https://bigbrotherwatch.org.uk/.

6 « NSA slides explain the PRISM data-collection program », *The Washington Post*, 6 juin 2013 : https://www.washingtonpost.com/wp-srv/special/politics/prism-collection-documents/.

7 Olivier Tesquet, *À la trace : enquête sur les nouveaux territoires de la surveillance*, Premier Parallèle, janvier 2020 : http://www.premierparallele.fr/livre/a-la-trace.

8 Interview d'Olivier Tesquet, 21 janvier 2020 : https://www.streetpress.com/sujet/1579625191-reconnaissance-faciale-fichage-generalise-geolocalisation-

surveillance-capitalisme-gafa.

9 Site Web de la société Two-i : https://two-i.com/.

10 Communiqué de l'Association nationale des supporters : https://twitter.com/A_N_Supporters/status/1220692742365425665.

11 Loi de 2016 encadrant « la lutte contre le hooliganisme » : https://www.vie-publique.fr/loi/20971-loi-renforcant-le-dialogue-avec-les-supporters-et-la-lutte-contre-le-hoo.

12 Communiqué de la CNIL, 18 février 2021 : https://www.cnil.fr/fr/reconnaissance-faciale-et-interdiction-commerciale-de-stade-la-cnil-adresse-un-avertissement-un-club.

13 Réponse du gouvernement au sénateur Karoutchi : https://www.senat.fr/questions/base/2020/qSEQ200113854.html.

14 « Le vrai visage de la reconnaissance faciale », juin 2019 : https://www.laquadrature.net/2019/06/21/le-vrai-visage-de-la-reconnaissance-faciale/.

15 Article du site Technopolice paru en juin 2021 : https://technopolice.fr/blog/videosurveillance-biometrique-dans-nos-supermarches/.

16 Antonio Casilli, *En attendant les robots,* Le Seuil, 2019 : https://www.seuil.com/ouvrage/en-attendant-les-robots-antonio-a-casilli/9782021401882.

. DÉCENTRALISER LA LUTTE CONTRE LA TECHNOPOLICE

1 L'essayiste américaine Shoshana Zuboff parle même de « capitalisme de surveillance » : https://www.zulma.fr/livre/lage-du-capitalisme-de-surveillance/.

2 Site Web de l'AN2V : https://an2v.org/.

3 « Nice va tester la reconnaissance faciale lors du Carnaval », *Le Point*, 19 février 2019 : https://www.lepoint.fr/societe/nice-va-tester-la-reconnaissance-faciale-lors-du-carnaval-19-02-2019-2294405_23.php.

4 « Reconnaissance faciale : la CNIL tique sur le bilan de l'expérience niçoise », *Le Monde*, 28 août 2019 : https://www.lemonde.fr/pixels/article/2019/08/28/reconnaissance-faciale-la-cnil-tique-sur-le-bilan-de-l-experience-nicoise_5503769_4408996.html.

5 « Reconnaissance faciale : un recours pour faire barrage à la surveillance biométrique », 19 février 2019 : https://www.laquadrature.net/2019/02/19/

reconnaissance-faciale-un-recours-pour-faire-barrage-a-la-surveillance-biometrique/.

6 Communiqué de la CNIL le 29 octobre 2019 : https://www.cnil.fr/fr/experimentation-de-la-reconnaissance-faciale-dans-deux-lycees-la-cnil-precise-sa-position.

7 « Première victoire en justice contre la reconnaissance faciale », 27 février 2020 : https://www.laquadrature.net/2020/02/27/premiere-victoire-en-france-devant-la-justice-contre-la-reconnaissance-faciale/.

8 « Des micros dans les rues de Saint-Étienne pour assurer la sécurité des habitants », *Le Parisien*, 1er mars 2019 : https://www.leparisien.fr/faits-divers/des-micros-dans-les-rues-de-saint-etienne-pour-assurer-la-securite-des-habitants-01-03-2019-8022531.php.

9 « Mouchards et drones à Saint-Étienne : le maire veut étouffer le débat », 15 avril 2019 : https://technopolice.fr/blog/mouchards-et-drones-a-saint-etienne-le-maire-veut-etouffer-le-debat/.

10 « L'installation très polémique de capteurs sonores est repoussée à Saint-Étienne », France Bleu, 8 mai 2019 : https://www.francebleu.fr/infos/societe/l-installation-de-capteurs-sonores-est-repoussee-a-saint-etienne-1557289707.

11 « Des micros dans la rue : la CNIL tire les oreilles (intelligentes) de Saint-Étienne », *Télérama*, 29 octobre 2019 : https://www.telerama.fr/medias/la-cnil-tire-les-oreilles-intelligentes-de-saint-etienne,n6492439.php.

12 Au sujet des pouvoirs de contrôle et de sanction de la CNIL : https://www.cnil.fr/fr/mission-4-controler-et-sanctionner.

13 « Saint-Étienne : La ville se fait tirer les oreilles et renonce à installer des micros dans ses rues », *20 minutes*, 30 octobre 2019 : https://www.20minutes.fr/societe/2640019-20191030-saint-etienne-ville-fait-tirer-oreilles-renonce-installer-micros-rues.

14 Pour en savoir plus sur les entreprises de la technopolice : https://technopolice.fr/entreprises/.

15 https://data.technopolice.fr/fr/

16 https://carte.technopolice.fr/

17 https://graphcommons.com/graphs/a0367840-d2f9-4f61-8b98-92f7955441c9

18 https://forum.technopolice.fr/

19 Termes de la licence libre CC by-SA : https://creativecommons.org/licenses/by-sa/2.0/fr/.

20 https://technopolice.fr/semobiliser/

21 https://carre.technopolice.fr/

22 https://technopolice.fr/semobiliser/guidesjuridiques/

23 https://technopolice.fr/blog/guide-se-renseigner-sur-la-surveillance-dans-sa-ville/

24 « La *smart city* policière se répand comme une traînée de poudre », 6 juillet 2018 : https://www.laquadrature.net/2018/07/06/nice-smart-city-surveillance/.

25 « Un logiciel pour décoder les émotions des usagers du tramway de Nice », France Bleu, 4 janvier 2019 : https://www.francebleu.fr/infos/societe/un-logiciel-pour-decoder-les-emotions-des-usagers-du-tramway-de-nice-1546621455.

26 « La Californie interdit la reconnaissance faciale sur les caméras des policiers », *Le Journal de Montréal*, 10 octobre 2019 : https://www.journaldemontreal.com/2019/10/10/la-californie-interdit-la-reconnaissance-faciale-sur-les-cameras-des-policiers.

27 « Le vrai visage de la reconnaissance faciale », 21 juin 2019 : https://www.laquadrature.net/2019/06/21/le-vrai-visage-de-la-reconnaissance-faciale/.

28 Voir la fiche de la CNIL sur le fichier TAJ : https://www.cnil.fr/fr/taj-traitement-dantecedents-judiciaires.

29 Chiffres tirés d'un rapport parlementaire « d'information sur les fichiers mis à la disposition des forces de police », octobre 2018, consultable ici : http://www.assemblee-nationale.fr/dyn/15/rapports/cion_lois/l15b1335_rapport-information.pdf.

30 Pour tout savoir sur la naissance, la composition et l'utilisation du fichier TAJ, lisez notre article du 18 novembre 2019, « La reconnaissance faciale des manifestant.es est déjà autorisée » : https://www.laquadrature.net/2019/11/18/la-reconnaissance-faciale-des-manifestants-est-deja-autorisee/.

31 « Nous attaquons la reconnaissance faciale dans le TAJ », 7 août 2020 : https://www.laquadrature.net/2020/08/07/nous-attaquons-la-reconnaissance-faciale-dans-le-taj/.

32 « La Quadrature du Net attaque l'application Alicem, contre la généralisation de la reconnaissance faciale », 17 juillet 2019 : https://www.laquadrature.net/2019/07/17/la-quadrature-du-net-attaque-lapplication-alicem-contre-la-generalisation-de-la-reconnaissance-faciale/.

33 Voir l'article « Tentative d'état des lieux de la reconnaissance faciale en France en 2021 », 21 juin 2021 : https://technopolice.fr/blog/tentative-detat-des-lieux-de-la-reconnaissance-faciale-en-france-en-2021/.

34 « À Istres, la mairie équipe la police de drones pour compléter le dispositif de vidéosurveillance », *Le Monde*, 6 avril 2018 : https://www.lemonde.fr/la-foire-du-drone/article/2018/04/06/a-istres-des-drones-pour-la-videosurveillance_5281508_5037916.html.

35 Voir la fiche de la ville sur le site Technopolice : https://technopolice.fr/istres/.

. QUAND LE NUMÉRIQUE MENACE LES LIBERTÉS

1 Vœux à la presse, 3 janvier 2018 : https://www.elysee.fr/emmanuel-macron/2018/01/03/voeux-du-president-de-la-republique-emmanuel-macron-a-la-presse.

2 « *Fake news* : derrière l'effet d'annonce, Macron esquive le vrai débat », 4 janvier 2018 : https://www.laquadrature.net/2018/01/04/macron_fake_news-2/.

3 « Inefficace ou mal comprise, la loi contre les *fake news* toujours en question », France 24, 19 juin 2019 : https://www.france24.com/fr/20190619-france-loi-fake-news-efficacite-promulgation-lrem-macron-fausses-nouvelles-csa.

4 « Mahjoubi et Schiappa croient lutter contre la haine en méprisant le droit européen », 14 février 2019 : https://www.laquadrature.net/2019/02/14/mahjoubi-et-schiappa-croient-lutter-contre-la-haine-en-meprisant-le-droit-europeen/.

5 Plateforme Pharos de signalement des contenus illicites sur Internet : « Vous pouvez signaler les faits de : pédophilie et pédopornographie, expression du racisme, de l'antisémitisme et de la xénophobie, incitation à la haine raciale, ethnique et religieuse, terrorisme et apologie du terrorisme, escroquerie et arnaque financières utilisant Internet », voir https://www.interieur.gouv.fr/A-votre-service/Ma-securite/Conseils-pratiques/Sur-internet/Signaler-un-contenu-suspect-ou-illicite-avec-PHAROS.

6 http://www.justice.gouv.fr/bo/2019/20190430/JUSD1910196C.pdf

7 CJUE, arrêt du 8 avril 2014 : https://curia.europa.eu/juris/document/document.jsf?text=&docid=150642&pageIndex=0&doclang=fr&mode=lst&dir=&occ=first&part=1&cid=147682.

8 « Demain, la surveillance française devant le Conseil d'État ! », 10 juillet 2018 : https://www.laquadrature.net/2018/07/10/audience_renseignement/.

9 « Recours contre le renseignement : compte rendu de notre audience devant la Cour de justice de l'Union européenne », 11 octobre 2019 :

https://www.laquadrature.net/2019/10/11/recours-contre-le-renseignement-compte-rendu-de-notre-audience-devant-la-cour-de-justice-de-lunion-europeenne/.

10 « Une loi contre la haine anti-Macron ? », 9 mai 2019 : https://www.laquadrature.net/2019/05/09/une-loi-contre-la-haine-anti-macron/.

11 « Analyse juridique de la loi "contre la haine en ligne" », 17 juin 2019 : https://www.laquadrature.net/2019/06/17/analyse-juridique-de-la-loi-contre-la-haine-en-ligne/.

12 « La loi "haine" va transformer Internet en télévision », 1er juillet 2019 : https://www.laquadrature.net/2019/07/01/la-loi-haine-va-transformer-internet-en-tv/.

13 Sur ce sujet, voir l'article de Benjamin Bayart publié en octobre 2018, « Intermédiaires techniques : un éléphant, ce n'est pas une souris en plus gros » : https://www.laquadrature.net/2018/10/10/intermediaires-techniques-un-elephant-ce-nest-pas-une-souris-en-plus-gros/.

14 Une idée développée dans notre article « L'interopérabilité contre la haine », 12 juin 2019 : https://www.laquadrature.net/2019/06/12/interoperabilite-contre-haine/.

15 Une interface de programmation d'information, ou API, est un logiciel dont le rôle consiste à traduire des instructions entre deux interlocuteurs : entre un matériel et un logiciel, par exemple, ou entre deux logiciels. Les plateformes peuvent s'entendre sur une API qui définit des fonctions communes, ou définir un standard commun dont chaque nouvel opérateur pourra s'emparer pour dialoguer avec tous les autres.

16 https://www.laquadrature.net/2019/05/21/pour-linteroperabilite-des-geants-du-web-lettre-commune-de-45-organisations/

17 https://www.laquadrature.net/2020/09/08/lunion-europeenne-doit-imposer-linteroperabilite-aux-geants-du-web/

18 « Première victoire contre la loi "haine" », 11 décembre 2019 : https://www.laquadrature.net/2019/12/11/premiere-victoire-contre-la-loi-haine/.

19 « Loi "haine" : la trahison du Sénat », 18 décembre 2019 : https://www.laquadrature.net/2019/12/18/loi-haine-la-trahison-du-senat/.

20 « Coup d'État sur la loi "haine" », 22 janvier 2020 : https://www.laquadrature.net/2020/01/22/coup-detat-sur-la-loi-haine/

21 Un cavalier législatif est un article de loi qui introduit des dispositions qui n'ont rien à voir avec le sujet traité par le projet de loi.

22 « Vote final de la loi “haine” », 11 mai 2020 : https://www.laquadrature.net/2020/05/11/vote-final-de-la-loi-haine/.

23 Site Web de l’association : https://www.franciliens.net/.

24 Pour trois ans, à titre d’expérimentation.

25 « Le Parlement doit rejeter le flicage fiscal des réseaux sociaux », 5 novembre 2019 : https://www.laquadrature.net/2019/11/05/le-parlement-doit-rejeter-le-flicage-fiscal-des-reseaux-sociaux/.

26 On reproche à un outil similaire utilisé aux Pays-Bas d’avoir été détourné de son usage premier pour discriminer les populations les plus pauvres : https://www.letemps.ch/monde/paysbas-batissent-un-surveillance-pauvres.

. L’ÉTAT D’URGENCE SANITAIRE, NOUVELLE STRATÉGIE DU CHOC

1 « Covid-19 : l’attaque des drones », 4 avril 2020 : https://technopolice.fr/blog/covid-19-lattaque-des-drones/.

2 « Pourquoi le ministère de l’Intérieur vient-il de commander des drones ? », *Libération*, 15 avril 2020 : https://www.liberation.fr/checknews/2020/04/15/pourquoi-le-ministere-de-l-interieur-vient-il-de-commander-des-drones_1785166/

3 « Le ministère de l’Intérieur a-t-il commandé 650 drones pour aider au respect du confinement ? », LCI, 16 avril 2020 : https://www.lci.fr/police/le-ministere-de-l-interieur-a-t-il-commande-650-drones-pour-aider-au-respect-du-confinement-2151170.html.

4 « Nous attaquons les drones de la police parisienne », 4 mai 2020 : https://www.laquadrature.net/2020/05/04/nous-attaquons-les-drones-de-la-police-parisienne/.

5 « Les goélands abattent leur premier drone », 18 mai 2020 : https://www.laquadrature.net/2020/05/18/les-goelands-abattent-leur-premier-drone/.

6 « Drones en manifestation : la Quadrature contre-attaque », 26 octobre 2020 :

https://www.laquadrature.net/2020/10/26/drones-en-manifestation-la-quadrature-contre-attaque/.

7 https://www.laquadrature.net/2020/12/22/interdiction-des-drones-victoire-totale-contre-le-gouvernement/

8 Le Conseil d’État, saisi par la LDH, interdit ces caméras thermiques le 29 juin 2020 : https://www.usine-digitale.fr/article/covid-19-le-conseil-d-etat-interdit-l-

usage-des-cameras-thermiques-dans-les-ecoles.N980456.

9 Fiche de la société Datakalab sur le site Technopolice : https://technopolice.fr/datakalab/.

10 « Coronavirus à Cannes : Surprise ! Dans ces marchés, des caméras vérifient si vous êtes bien masqués », *20 minutes*, 28 avril 2020 : https://www.20minutes.fr/nice/2768871-20200428-coronavirus-cannes-surprise-marches-cameras-verifient-si-bien-masques.

11 « La RATP va tester des caméras intelligentes pour mesurer le taux de port du masque dans la station Châtelet », *Le Monde*, 7 mai 2020 : https://www.lemonde.fr/pixels/article/2020/05/07/ratp-des-cameras-intelligentes-pour-mesurer-le-taux-de-port-du-masque-dans-la-station-chatelet_6039008_4408996.html.

12 « Trop intrusives, les caméras de détection de masques désactivées à Paris et à Cannes », BFM, 22 juin 2020 : https://www.bfmtv.com/tech/trop-intrusives-les-cameras-de-detection-de-masques-desactivees-a-paris-et-a-cannes_AN-202006220163.html.

13 Avis de la CNIL sur les caméras thermiques : https://www.cnil.fr/fr/cameras-dites-intelligentes-et-cameras-thermiques-les-points-de-vigilance-de-la-cnil-et-les-regles.

14 « Crise sanitaire : la technologie envahit l'université », 30 avril 2020 : https://www.laquadrature.net/2020/04/30/crise-sanitaire-la-technopolice-envahit-luniversite/.

15 https://www.ladepeche.fr/2020/04/25/coronavirus-la-societe-toulousaine-sigfox-propose-des-bracelets-electroniques-pour-gerer-le-deconfinement,8862285.php

16 Chaque carte ou chaque puce réseau (Ethernet, wifi, ou Bluetooth) est identifiée par un numéro unique (de 6 octets au format hexadécimal) appelé son adresse MAC, ou adresse matérielle, pour la distinguer de l'adresse lP, par exemple, susceptible de changer à chaque nouvelle connexion.

17 « StopCovid est un projet désastreux piloté par des apprentis sorciers », 25 avril 2020 : https://www.laquadrature.net/2020/04/25/stopcovid-est-un-projet-desastreux-pilote-par-des-apprentis-sorciers/.

18 « Nos arguments pour rejeter StopCovid », 14 avril 2020 : https://www.laquadrature.net/2020/04/14/nos-arguments-pour-rejeter-stopcovid/.

19 Analyse de l'avis de la CNIL, 27 avril 2020 : https://www.laquadrature.net/2020/04/27/la-cnil-sarrete-a-mi-chemin-contre-stopcovid/.

20 « Coronavirus : un fichier de police détourné pour repérer les récidivistes qui violent le confinement », *Le Monde*, 15 avril 2020 : https://www.lemonde.fr/police-justice/article/2020/04/15/un-fichier-de-police-detourne-pour-reperer-les-recidivistes-qui-violent-le-confinement_6036662_1653578.html.

21 « Fichage policier : recours contre le détournement du fichier du système de contrôle automatisé », 9 novembre 2020 : https://www.laquadrature.net/2020/11/09/fichage-policier-recours-contre-le-detournement-du-fichier-du-systeme-de-controle-automatise/.

22 « Décrets PASP : fichage massif des militants politiques », 8 décembre 2020 : https://www.laquadrature.net/2020/12/08/decrets-pasp-fichage-massif-des-militants-politiques/.

23 « La loi Avia revient par la porte de l'UE », 22 septembre 2020 : https://www.laquadrature.net/2020/09/22/aviasback/.

24 « Donner un sens à l'intelligence artificielle : pour une stratégie nationale et européenne », rapport de mars 2018, sous la direction du député Cédric Villani : https://www.vie-publique.fr/rapport/37225-donner-un-sens-lintelligence-artificielle-pour-une-strategie-nation.

25 Pour une liste exhaustive, se reporter à la partie 5 « Patrimoine de données » du rapport de la mission de préfiguration du HDH : https://solidarites-sante.gouv.fr/IMG/pdf/181012_-_rapport_health_data_hub.pdf.

26 Association pour la promotion du logiciel libre : https://www.april.org/.

27 Délibération de la CNIL au format PDF : https://www.cnil.fr/sites/default/files/atoms/files/deliberation_du_20_avril_2020_portant_avis_sur_projet_darrete_relatif_a_lorganisation_du_systeme_de_sante.pdf.

28 « Données de santé : le "oui mais" du Conseil d'État au Health Data Hub », *Mediapart*, 19 juin 2020 : https://www.mediapart.fr/journal/france/190620/donnees-de-sante-le-oui-mais-du-conseil-d-etat-au-health-data-hub.

29 « Health Data Hub : du fantasme de l'intelligence artificielle à la privatisation de nos données de santé », 17 mars 2021 : https://www.laquadrature.net/2021/03/17/health-data-hub-du-fantasme-de-lintelligence-artificielle-a-la-privatisation-de-nos-donnees-de-sante/.

30 « Discours du président de la République sur l'intelligence artificielle », 29 mars 2018 : https://www.elysee.fr/emmanuel-macron/2018/03/29/discours-du-president-de-la-republique-sur-lintelligence-artificielle.

31 Rapport Villani, page 196 : https://www.aiforhumanity.fr/pdfs/9782111457089_Rapport_Villani_accessible.pdf.

32 Page de présentation du SNDS sur le site de la CNIL : https://www.cnil.fr/fr/snds-systeme-national-des-donnees-de-sante.

33 « France : l'Assurance-maladie estime que Microsoft ne peut pas gérer les données de santé », RFI, 19 février 2021 : https://www.rfi.fr/fr/france/20210219-france-l-assurance-maladie-estime-que-microsoft-ne-peut-pas-g%C3%A9rer-les-donn%C3%A9es-de-sant%C3%A9.

34 « Face à la controverse, le Health Data Hub retire "temporairement" sa demande d'autorisation pour héberger des données de santé », *Le Quotidien du Médecin*, 10 janvier 2022 : https://www.lequotidiendumedecin.fr/actus-medicales/esante/face-la-controverse-le-health-data-hub-retire-temporairement-sa-demande-dautorisation-pour-heberger.

35 Nostrum Pharmaceuticals, après avoir multiplié le prix d'un médicament par cinq, se défend en invoquant son « devoir moral de vendre le produit au prix le plus élevé » : https://www.lesechos.fr/industrie-services/pharmacie-sante/etats-unis-un-industriel-augmente-de-400-le-prix-dun-medicament-138722. Novartis, de son côté, a récupéré le résultat d'une recherche financée initialement par le Téléthon, et a décidé de vendre le traitement au prix de 2,1 millions de dollars par patient : https://www.lexpress.fr/actualite/comment-novartis-va-s-enrichir-grace-a-l-argent-du-telethon_2081823.html.

. VERS UN MONDE DE LA « SÉCURITÉ GLOBALE » ?

1 Un document à télécharger au format PDF sur ce site : https://www.interieur.gouv.fr/actualites/actu-du-ministere/livre-blanc-de-securite-interieure ou sur Vie publique : https://www.vie-publique.fr/rapport/277185-livre-blanc-de-la-securite-interieure.

2 « Loi "Sécurité globale" : des auditions parlementaires pro-sécuritaires et à sens unique », 28 octobre 2020 : https://technopolice.fr/blog/loi-securite-globale-des-auditions-parlementaires-pro-securitaires-et-a-sens-unique/

3 « Livre blanc de la sécurité intérieure » (LBSI), pages 201 à 276.

4 Jusque dans des domaines inattendus, comme ce « [ajouter] des capacités d'intelligence artificielle aux logiciels de prise de plainte afin de mieux catégoriser les contentieux » (« Livre blanc de la sécurité intérieure », page 212).

5 « Afin d'améliorer la gestion de l'alerte et la détection rapide de situations dangereuses non signalées aux centres opérationnels, il est possible d'expérimenter l'automatisation de la captation d'informations en sources ouvertes librement accessibles sur les réseaux sociaux » (*Id.*, page 220).

6 Il est à noter que la question des réseaux informatiques internes à la police est abordée sous l'angle de l'augmentation considérable de la quantité d'images de vidéoprotection, qui demandent une très grande capacité de transfert rapide et de stockage (*Id.*, pages 239-240).

7 « Loi "Sécurité globale" : surveillance généralisée des manifestations », 29 octobre 2020 : https://www.laquadrature.net/2020/10/29/loi-securite-globale-surveillance-generalisee-des-manifestations/

8 « Sécurité globale : la police fait la loi », 6 novembre 2020 : https://www.laquadrature.net/2020/11/06/securite-globale-la-police-fait-la-loi/.

9 « PPL Sécurité globale : la police te surveille jusque dans ton immeuble », 18 novembre 2020 : https://technopolice.fr/blog/ppl-securite-globale-la-police-te-surveille-jusque-dans-ton-immeuble/.

10 En octobre 2020, Mediapart rapporte un fait avéré de militants du collectif hospitalier Inter-Urgences suivis jusqu'à leur domicile par des drones policiers : Clément Le Foll et Clément Pouré, « Profitant du flou juridique, les drones policiers bourdonnent toujours », *Mediapart*, 26 octobre 2020 : https://www.mediapart.fr/journal/france/261020/profitant-du-flou-juridique-les-drones-policiers-bourdonnent-toujours.

11 « Deux ans après, que sont devenus les "gilets jaunes" mutilés en manifestation ? », France Inter, 29 avril 2021 : https://www.franceinter.fr/societe/deux-ans-apres-que-sont-devenus-les-gilets-jaunes-mutiles-en-manifestation/.

12 Voir la liste des signataires, des organisations et des soutiens sur le site de la coordination Stop loi Sécurité globale : https://stoploisecuriteglobale.fr/#communique.

13 Site Web de Paolo Cirio : https://paolocirio.net/.

14 « Nous soutenons la pétition pour bannir la reconnaissance faciale en Europe », 22 septembre 2020 : https://www.laquadrature.net/2020/09/22/nous-soutenons-la-petition-pour-bannir-la-reconnaissance-faciale-en-europe/.

15 Tweet de Gérald Darmanin, le 1er octobre 2020 : https://twitter.com/GDarmanin/status/1311688550073724931.

16 « La censure de l'art pour banaliser la surveillance », 8 octobre 2020 : https://www.laquadrature.net/2020/10/08/la-censure-de-lart-pour-banaliser-la-

surveillance/.

17 « Loi “Sécurité globale” adoptée, résumons », 6 avril 2021 : https://www.laquadrature.net/2021/04/16/loi-securite-globale-adoptee-resumons/.

18 « Loi “Sécurité globale” : nos arguments au Conseil constitutionnel », 29 avril 2021 : https://www.laquadrature.net/2021/04/29/loi-securite-globale-nos-arguments-au-conseil-constitutionnel/.

19 « Avatar de l’article 24, le nouveau délit d’appel à la haine en ligne est adopté avec la loi “séparatisme” », *Mediapart*, 11 février 2021 : https://www.mediapart.fr/journal/france/110221/avatar-de-l-article-24-le-nouveau-delit-d-appel-la-haine-en-ligne-est-adopte-avec-la-loi-separatisme.

20 « Loi “renseignement” : le retour en pire », 27 mai 2021 : https://www.laquadrature.net/2021/05/27/loi-renseignement-le-retour-en-pire/.

21 « Loi “renseignement 2” : nos arguments au Conseil constitutionnel », 28 juillet 2021 : https://www.laquadrature.net/2021/07/28/loi-renseignement-2-nos-arguments-au-conseil-constitutionnel/.

22 « Point d’étape des lois “renseignement”, “séparatisme” et “anti-piratage” », 30 juin 2021 : https://www.laquadrature.net/2021/06/30/point-detape-des-lois-renseignement-separatisme-et-anti-piratage/.

23 « Les drones reviennent, nous aussi », 14 septembre 2021 : https://www.laquadrature.net/2021/09/14/les-drones-reviennent-nous-aussi/.

24 « Règlement de censure terroriste adopté : résumons », 7 mai 2021 : https://www.laquadrature.net/2021/05/07/reglement-de-censure-terroriste-adopte-resumons/.

25 Voir https://www.laquadrature.net/2019/10/11/recours-contre-le-renseignement-compte-rendu-de-notre-audience-devant-la-cour-de-justice-de-lunion-europeenne/.

26 « Surveillance : une défaite victorieuse », 6 octobre 2020 : https://www.laquadrature.net/2020/10/06/surveillance-une-defaite-victorieuse/.

27 « Jugement imminent contre la surveillance de masse », 7 avril 2021 : https://www.laquadrature.net/2021/04/07/jugement-imminent-contre-la-surveillance-de-masse/.

28 « Le Conseil d’État valide durablement la surveillance de masse », 21 avril 2021 : https://www.laquadrature.net/2021/04/21/le-conseil-detat-valide-durablement-la-surveillance-de-masse/.

29 Le site Web de Forbidden Stories : https://forbiddenstories.org/fr/.

30 « Projet Pegasus : des révélations chocs sur un logiciel espion israélien », Amnesty International, 8 juillet 2021 : https://www.amnesty.fr/actualites/surveillance-revelations-sur-le-logiciel-espion-israelien-pegasus-nso-group.

31 « Malgré les approches de NSO Group, la France a choisi à la fin de 2020 de ne pas acheter le logiciel espion Pegasus », *Le Monde*, 26 novembre 2021 : https://www.lemonde.fr/pixels/article/2021/11/26/malgre-les-approches-de-nso-group-la-france-a-choisi-a-la-fin-de-2020-de-ne-pas-acheter-le-logiciel-espion-pegasus_6103783_4408996.html.

Édition numérique réalisée par Solenne Vaulot Morel

INTERNET ET LIBERTÉS

Partout où le numérique est venu changer nos vies, le respect de nos libertés fondamentales est un combat.

Pendant que Facebook, Google et compagnie se targuent de protéger nos données tout en les exploitant pour booster la publicité ciblée, les lois sécuritaires s'enchaînent et les expérimentations illégales aussi : des micros dans les rues, des tests de reconnaissance faciale dans les stades ou les transports, des drones aux mains des policiers… La dérive vient des pouvoirs publics autant que des entreprises.

Les membres de La Quadrature du Net sont de ceux qui restent vigilants. Actifs depuis toujours sur les thématiques de droits d'auteur et de censure, ils veillent désormais beaucoup plus largement à la protection de notre vie privée. Par leurs campagnes, ils informent l'opinion. Par leurs recours en justice, aux niveaux français et européen, ils tiennent tête aux GAFAM et aux chantres de la technopolice. Avec, chevillée au corps, depuis les premières heures, l'idée de se battre pour un Internet juste, libre, émancipateur, ouvert et démocratique.

Mathieu Labonde, Lou Malhuret, Benoît Piédallu et Axel Simon sont membres de La Quadrature du Net. Ils retracent ici pour la première fois les luttes de l'association depuis sa création.