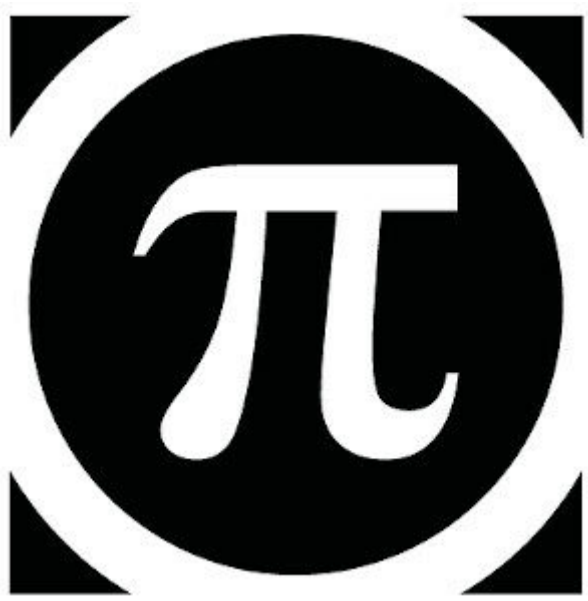
La Quadrature du Net : « En France, la surveillance de la population est extrêmement développée »

Ballast
2 mars 2022

Entretien inédit pour le site de Ballast

Hier, le Conseil d'État français refusait, en référé, de suspendre le pass vaccinal adopté par l'Assemblée nationale le 16 janvier dernier, succédant au pass sanitaire — et ce malgré l'opposition de tous les défenseurs des droits et des libertés individuelles et collectives. Dès le mois d'août 2021, l'association La Quadrature du Net alertait ainsi contre « les dangers » posés par sa mise en place. Précisant : « Cet emballement dramatique des pouvoirs de l'État s'inscrit dans un mouvement d'ensemble déjà à l'œuvre depuis plusieurs années ». C'est de ce mouvement dont nous avons souhaité discuter. Fondée en 2008, La Quadrature du Net est devenue un acteur incontournable de la lutte contre la censure et la surveillance — et plus généralement de la défense des libertés fondamentales dans un monde où le numérique s'étend à tous les domaines d'activité. En pointe lors de la création d'Hadopi[1], elle effectue un important travail de vulgarisation d'enjeux souvent techniques et obscurs. Caméras, smart city, technopolice, lois renseignement, neutralité du Net et pass : tour d'horizon d'un pistage de chaque instant.



Commençons par un dispositif de surveillance devenu central dans nos vies en un clin d'œil : le pass sanitaire/vaccinal. Vous le replacez dans une évolution plus large des technologies qui ont permis l'application de la « *répression par l'exclusion* », jusque-là limitée. Comment expliquez-vous la faiblesse des critiques envers la généralisation d'un tel dispositif ?

Le propre de la « répression par l'exclusion » est d'être difficile à critiquer en masse. Elle se fonde sur une fracture entre personnes jugées désirables ou indésirables par l'État (gens du voyage et migrant·es, typiquement) en espérant que cette fracture et les différences de traitement qui en résultent freinent la solidarité des personnes non-exclues envers celles exclues. Avec des conséquences moins dramatiques, c'est sur ce type de fracture que repose le pass sanitaire pour réprimer par l'exclusion les personnes non-vaccinées, qui ne bénéficient pas toujours d'une grande solidarité. À droite comme à gauche, on ne manque pas d'excuses pour ne plus participer aux manifestations anti-pass : moqueries ou haine contre les personnes qui ont peur des nouvelles technologies (vaccins comme 5G) ; culpabilisation des personnes non-vaccinées ; refus d'être associé à des personnes de classe inférieure ; puis refus d'être associé à l'extrême droite qui, fatalement, est venue profiter de l'isolement politique dans lequel les militant·es anti-pass avaient été laissé·es. Pourtant, les systèmes de répression par l'exclusion sont au cœur de l'idéologie d'extrême droite et des politiques menées par le gouvernement, que ce soit contre les pauvres, les étranger·es ou toute personne déviant des normes réactionnaires. Le pass sanitaire, en montrant comment les nouvelles technologies peuvent décupler ces pratiques de contrôle et d'exclusion, devrait être une cible dans la lutte contre les idées d'extrême droite.

Loi sécurité globale, loi renseignement, lois antiterroristes… Il ne passe pas un an sans qu'une nouvelle loi vienne élargir l'usage des drones, des caméras de surveillance, de la reconnaissance faciale, des perquisitions administratives ou encore du partage des renseignements entre services. Le quinquennat Macron

se distingue-t-il des précédents ?

« Le pass sanitaire, en montrant comment les nouvelles technologies peuvent décupler ces pratiques de contrôle et d'exclusion, devrait être une cible dans la lutte contre les idées d'extrême droite. »

Le rôle de Macron est probablement très faible dans ces évolutions. Sur ces sujets, ce sont les services de renseignement et la police qui ont toujours défini la marche à suivre — elle-même souvent la conséquences d'évolutions internationales : les Français tentent depuis plus de dix ans de rattraper leur retard technologique sur la NSA. Il a fallu attendre 2013 et les divulgations d'Edward Snowden pour que le gouvernement prenne la peine de légaliser les programmes de surveillance massifs et secrets développés par le renseignement français. S'agissant de la reconnaissance faciale, c'est la Chine qui semble inquiéter les polices européennes : hors de question pour l'Occident de perdre l'hégémonie technologique de l'oppression et de se faire distancer par l'empire du Milieu ! D'autant que les enjeux industriels sont immenses et que l'industrie française (Thalès, Atos, Idémia, Evitech…) promet, si on lui en donne l'argent et les lois nécessaires, de faire de la France un pays à la pointe de la surveillance biométrique[2]. Cette escalade sécuritaire est la conséquence naturelle de notre système économique, de la structure de notre État et de facteurs géopolitiques — autant de choses qui existaient bien avant Macron et risquent hélas de lui survivre.

En France, un des contre-pouvoirs clefs est la Commission nationale de l'informatique et des libertés (CNIL), créée en 1978 et réformée en 2004. Vous critiquez souvent ses prises de position, ou plutôt leur absence. Faut-il la réformer ou la supprimer ?

La CNIL, malgré des moyens encore faibles face à l'ampleur des traitements de données personnelles qui sont réalisés, a déjà un certain nombre de ressources pour mettre de sérieux freins au développement de la technopolice — l'alliance des nouvelles technologies aux pouvoirs de police : ce qu'elle ne fait encore que trop rarement. C'est à la population de mettre la pression pour la faire changer de posture. Récemment, certains signes laissent penser que cette mobilisation commence à payer : la CNIL a rendu quelques décisions contre de nouvelles technologies de surveillance. Même si ces décisions interviennent souvent après que le travail ait été fait par la population (si la CNIL a bien fini par interdire les drones, par exemple, elle l'a fait plusieurs mois après nos actions victorieuses devant le Conseil d'État), c'est probablement un bon début.

Continuons dans cette voie tout en nous souvenant qu'il sera difficile d'espérer une pleine protection de la part de la CNIL et qu'il est donc nécessaire que la population continue de s'organiser pour se défendre elle-même.

[Stéphane Burlot]

Le règlement général sur la protection des données (RGPD), adopté en 2016, est censé offrir un des cadres les plus sûrs du monde en termes de protection des données personnelles. Côté utilisateur, il s'est surtout traduit par une multiplication des messages plus ou moins clairs nous demandant d'accepter des cookies pour « améliorer notre expérience ». Quel bilan en tirez-vous ?

En 2016, nous étions très mitigés s'agissant du RGPD. À nos yeux, il ne changeait pas grand-chose par rapport au droit européen antérieur qui, depuis 1995, offrait une vague protection de nos données personnelles. En 2018, toutefois, au moment où le texte allait entrer en application, il a profité d'une très forte et surprenante médiatisation. Nous avons donc rangé notre pessimisme pour surfer sur la vague et tenter de pousser des interprétations juridiques capables de subvertir le modèle économique du capitalisme de surveillance. C'est pourquoi nous avons déposé, avec 12 000 personnes, des plaintes collectives contre Google, Apple, Facebook, Amazon et Microsoft dans le but de les empêcher de faire du ciblage publicitaire en Europe. Trois ans plus tard, le résultat est mitigé : Amazon vient de recevoir une amende record de 746 millions d'euros au

Luxembourg suite à notre plainte, avec obligation sous astreinte d'arrêter la publicité ciblée sans notre consentement. Amazon a fait appel de la décision et n'a pas encore changé son comportement. Les quatre autres plaintes sont bloquées en Irlande, où les entreprises sont situées et où l'autorité semblable à la CNIL ne parait pas pressée de travailler. Comme pour la CNIL en France, le seul blocage semble être politique : derrière un protectionnisme de façade, peu d'États européens souhaitent se mettre à dos les GAFAM qui sont de puissants alliés en matière de censure, de développement technologique ou de propagande politique. Mais comme pour la CNIL, la population peut faire pression sur ces institutions plus ou moins indépendantes, et nous ne désespérons pas de quelques belles surprises à venir.

Sur le plan des données personnelles, on oppose souvent le modèle occidental — où des grands groupes privés sont les premiers à en organiser la collecte et à en profiter — au modèle chinois — où c'est l'État qui s'en sert pour développer des politiques de fichage et de *social ranking*. Une telle dichotomie permet-elle de penser les similarités et différences entre Chine, États-Unis et Europe ?

> ***« L'Asie ne doit servir ni de repoussoir dystopique ni de rivale économique : nous y voyons surtout des populations subissant des technologies similaires à celles que nous subissons en Europe. »***

Nous n'opposons pas de modèle prétendument occidental à un modèle prétendument chinois (où le secteur privé joue d'ailleurs un rôle fondamental) car il nous semble que ce discours permet surtout aux gouvernements européens de dissimuler la surveillance de masse qu'ils ont déjà installée, tout en leur offrant le prétexte pour en installer davantage afin de rattraper un prétendu retard vis-à-vis de la Chine. En réalité, en France, la surveillance de la population est extrêmement développée, qu'elle soit réalisée par l'industrie privée ou par l'État — qui tient à jour des fichiers sur la population, gérés par l'administration sans le contrôle de la justice, afin de savoir quelles personnes sont correctement intégrées dans la société ou, au contraire, posent des risques politiques et doivent ainsi se voir refuser l'accès à certaines professions ou à un titre de séjour.

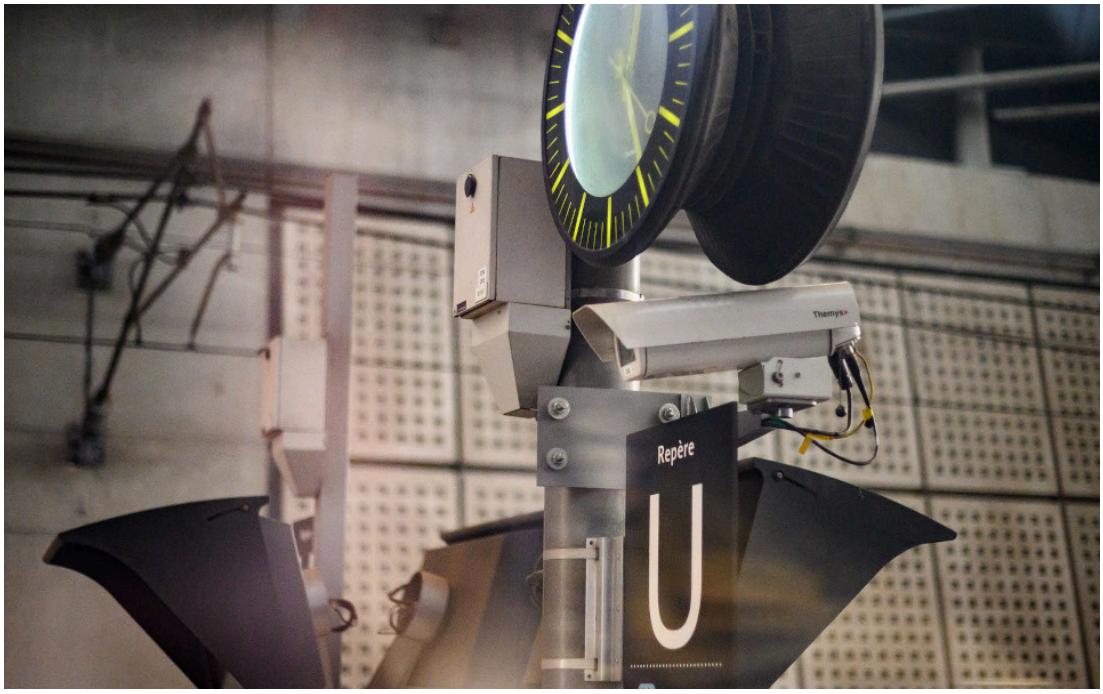
Que sont précisément ces fichiers ?

Voyez par exemple le fichier TAJ[3] ou le fichier PASP[4]. Le *social ranking* lui-même est directement inspiré des systèmes de *credit ranking* (évaluation de solvabilité) développé

aux États-Unis. La reconnaissance faciale est l'héritière de l'anthropométrie française : une technique policière de mesure du corps développée au XVIII[e] siècle. Aujourd'hui, fortes de ces échanges culturels, les industries occidentales et asiatiques collaborent pour développer leurs technologies policières, chacune expérimentant ses outils dans les pays de l'autre. On a récemment vu Huawei déployer gratuitement sa reconnaissance faciale dans des lycées à Marseille et Nice, pendant que la France organisait des expérimentations similaires à Singapour. Elles se servent chacune de l'autre comme prétexte pour avoir le soutien de son État et de sa population. L'Asie ne doit servir ni de repoussoir dystopique ni de rivale économique : nous y voyons surtout des populations subissant des technologies similaires à celles que nous subissons en Europe, et avec lesquelles nous aurions tout intérêt à tisser des solidarités.

Pour lutter contre l'emprise des grandes entreprises américaines, les GAFAM, le développement d'alternatives « souveraines » européennes voire françaises est souvent avancé comme la solution. Pourtant, avoir un Google parisien ou un Facebook berlinois changerait-il fondamentalement un modèle basé sur la collecte massive de données personnelles vendues à des annonceurs ?

Peu de monde souhaite véritablement l'apparition d'un Google parisien ou d'un Facebook berlinois. Le gouvernement français vante les mérites de Google et de Facebook dès que l'occasion se présente et n'aurait aucun intérêt à ce que ceux-ci disparaissent ou s'éloignent. Google et Facebook ont gratuitement repris à leur compte tout le travail de police de l'Internet, et le gouvernement a exprimé à de nombreuses reprises en être très satisfait (son seul problème concerne Twitter qui est moins coopératif que les deux autres). Pour le gouvernement français, remplacer Google et Facebook par des équivalents européens risquerait non seulement de les substituer à des acteurs moins efficaces, mais aussi de soumettre ces nouveaux acteurs aux lois et aux débats publics européens auxquels les GAFAM peuvent échapper en bonne partie. Le seul avantage pour le gouvernement serait d'avoir de gros acteurs français plus proches de ses services de renseignement, mais cette raison ne semble pas actuellement suffire pour entreprendre les démarches risquées et titanesques qui seraient nécessaires à l'apparition d'un Google ou d'un Facebook français — le gouvernement semble préférer la solution confortable du statu quo. Du côté de la population, comme vous l'avez bien souligné, celle-ci a bien plus intérêt à voir le modèle de surveillance publicitaire disparaître plutôt que changer de propriétaire. Cette solution est d'autant plus souhaitable que, juridiquement, le RGPD la rend tout à fait réaliste[5].



[Stéphane Burlot]

Vous êtes plutôt critiques des initiatives, qu'elles viennent du gouvernement ou de la Commission européenne, qui visent à lutter contre la propagation des *fake news* et des propos haineux sur le Web, et particulièrement sur les réseaux sociaux. Faut-il réguler le contenu diffusé sur ces plateformes, au risque, donc, de censurer ?

Nous ne pensons pas que Google et Facebook puissent véritablement offrir des espaces de libertés d'expression : quand ils le font, ce n'est que de façon incongrue et temporaire. Au contraire. La raison d'être de ces entreprises est de créer des espaces d'expression inégale où sont favorisées les industries qui les financent pour diffuser leur propagande publicitaire au détriment du reste de la population — l'inverse de la liberté d'expression. Google et Facebook sont des modèles de censure par nature, de sorte qu'ils n'ont pas attendu que des lois le leur demandent pour censurer des propos contraires à leurs objectifs commerciaux. Les lois de censure (qu'elles prétendent lutter contre la haine ou contre le terrorisme) sont moins une menace pour les grands réseaux sociaux (qui ne s'en trouvent pas vraiment altérés) que pour les alternatives décentralisées déployées par la population. On ne peut que souligner l'échec colossal du CSA et de la justice pour lutter contre la propagation des idées de haine dans l'espace public. Par contre, ces lois présentent un tel poids qu'elles ont pour effet, si ce n'est pour but, de décourager en Europe le développement d'alternatives populaires, seules à

même d'offrir sur Internet de véritables espaces d'expression où les uniques formes de censure ou de modération sont celles choisies par la population autogérée.

Tout ne se passe pas à l'échelle européenne ou nationale. Vous interpellez souvent des villes, de gauche comme de droite, pour leur goût immodéré pour la vidéosurveillance et tout autre outil qui contient les mots « *smart* » ou « big data ». Marseille est la dernière en date. Comment expliquer cet engouement pour des dispositifs dangereux pour la vie privée, et à l'efficacité d'ailleurs souvent contestée ?

> ***« L'utilisation de caméras dans l'espace public n'est quasiment plus remise en cause au sein du champ politique et médiatique. Pourtant, il est bien au cœur de la technopolice. »***

L'échelle locale est très intéressante à regarder s'agissant du déploiement de la technopolice. C'est d'ailleurs le nom que nous avons donné à une campagne lancée en 2019 qui fait aussi écho à l'invasion des technologies et l'accélération grandissante du tout-numérique dans les espaces urbains. Nous nous sommes aperçus que de nombreux dispositifs technopoliciers étaient d'abord déployés localement, dans différentes villes. Ces dispositifs incluent l'écoute urbaine, la vidéosurveillance automatisée (c'est-à-dire l'ajout d'une couche logicielle sur des caméras classiques avec détection de comportements anormaux, de maraudage, etc.), la reconnaissance faciale, des hauts parleurs couplés aux caméras, jusqu'aux logiciels de police prédictive. Les municipalités sont motrices dans la mise en place de ce qui est souvent présenté comme n'étant « que » des expérimentations. À l'origine de tous ces dispositifs, il y a le déploiement de la vidéosurveillance, à l'initiative des collectivités locales et incité par des financements publics. L'utilisation de caméras dans l'espace public n'est quasiment plus remise en cause au sein du champ politique et médiatique. Pourtant, il est bien au cœur de la technopolice : c'est sur cette infrastructure et sa croissance incessante qu'elle repose. Et si la vidéosurveillance s'est imposée comme solution, c'est le fait d'un enchevêtrement d'intérêts convergents entre les élus locaux et les industriels. Si les municipalités installent toujours plus de caméras, c'est parce qu'elles peuvent facilement capitaliser sur ces dispositifs. L'extension et le renforcement des dispositifs sécuritaires constituent ainsi des ressources que les élus peuvent exploiter politiquement : c'est ce qu'on observe à Nice, où Christian Estrosi ne cesse de crier à tue-tête que sa ville est la plus vidéosurveillée de France et, par conséquent, la plus sécurisée ! Lorsqu'un événement a lieu — du dépôt d'ordure sauvage à un attentat, en passant par un cambriolage —, l'annonce de l'installation de nouvelles caméras ou de reconnaissance faciale donne

l'impression de faire quelque chose de concret, une mesure réalisable rapidement qui prétend résoudre un problème.

Qu'en est-il des industriels que vous mentionnez ?

Pour les acteurs privés, la technopolice représente un marché très lucratif. Que ce soit pour les industriels de la défense, donc militaires, comme Thalès, le champion français (vente d'arme, de drone, etc.), des entreprises historiquement du numérique, de l'énergie ou des start-up. Pour les entreprises d'armement, rien d'étonnant à ce qu'elles abreuvent aussi le marché de la sécurité intérieure en technologies de surveillance : le marché civil représente une perspective de débouchés à la R&D militaire — comme le géographe Stephen Graham le montre avec l'exemple des drones. Le marché de la sécurité n'est autre que la transformation et la traduction de technologies militaires vers celles du maintien de l'ordre afin de trouver des débouchés nationaux. En dehors des entreprises proprement sécuritaires, le marché de la surveillance intéresse aussi d'autres acteurs, attirant des entreprises spécialisées dans d'autres secteurs. Des entreprises des TIC [technologies de l'information et la communication] tentent ainsi de d'inscrire dans ce marché : IBM à Toulouse pour équiper une trentaine de caméras de vidéosurveillance de la métropole d'un logiciel de vidéosurveillance automatisée ; Cisco à Marseille et Nice pour équiper les lycées de portiques de reconnaissance faciale. Enfin, les start-ups ne sont pas en reste. Certaines se sont créées spécifiquement pour le marché de la sécurité urbaine tandis que d'autres, comme Two-I, initialement spécialisée dans la reconnaissance d'émotions, se sont au contraire reconverties. Aujourd'hui, elle met au point des algorithmes de reconnaissance faciale, testés sur les supporters du stade de foot de Metz, ainsi qu'une plateforme d'hypervision permettant le pilotage à distance de la ville. Si le recours aux nouvelles technologies dans le but d'automatiser, de rationaliser et de rendre plus efficace la sécurité urbaine est si présent dans les grandes villes, c'est parce qu'il s'inscrit dans le nouveau récit néolibéral. Le recours à l'imaginaire d'une « *smart city* » montre à quel point les métropoles ont intégré la rationalité du New Public Management en appliquant ce capitalisme numérique à l'aménagement et à la gestion territoriale. En bref, si les municipalités sont si promptes à avoir recours à la technopolice et aux dispositifs de surveillance, c'est parce qu'elles y ont tout intérêt, économiquement comme politiquement.

[Stéphane Burlot]

Que ce soit au nom de la protection de l'environnement, de la participation des citoyens avec les « *civic tech* » et bien sûr de la sécurité, la multiplication des données — et donc de ses sources (capteurs, applications mobiles, caméras) — est censée apporter de nombreuses réponses aux défis que vont connaître les grands centres urbains dans les décennies à venir. Rejetez-vous en bloc le concept de *smart city* ou peut-on imaginer une « ville intelligente » sans entrer dans la surenchère technologique et sécuritaire ?

C'est une nouvelle « fiction urbaine », une manière pour le capitalisme numérique de s'attaquer à la gestion de l'espace urbain. La transformation des métropoles deviendrait soudain possible : les nouvelles technologies permettraient à des mégalopoles de pallier à la crise écologique tout en étant plus démocratiques et horizontales. Tout ça repose sur une croyance : à travers la maîtrise et le contrôle toujours plus fin et total des ressources, il serait possible de faire des économies d'énergie et d'être plus efficace dans l'allocation de celle-ci au sein des villes. Et, en bonus, cette numérisation verrait l'avènement d'une « citoyenneté augmentée », où les habitant·es toujours connecté·es seraient de véritable acteurs d'une ville toujours plus démocratique. C'est ce que le géographe Guillaume Faburel nomme la « prophétie technologique », soit le progrès technologique pour toute réponse aux problèmes sociaux. Ces fictions reposent notamment sur l'aménagement de multiples capteurs dans le paysage urbain : des

caméras de vidéosurveillance, des capteurs sur les poubelles pour savoir quand elles sont pleines, des indicateurs de la pollution de l'air, des détecteurs de mouvement pour les lampadaires automatisés, etc. Cette automatisation, doublée d'une surenchère de nouvelles technologies, est inscrite dans l'ADN des *smart cities* : leur fameuse « intelligence » proviendrait de la collecte et de l'analyse des données produites par ces capteurs. En outre, la notion de *safe city* — soit une ville intelligente et sûre — est apparue, bien que différemment mis en avant selon les métropoles. Ce concept, né de la bouche des industriels, illustre le passage à l'automatisation de la sécurité urbaine et à la technopolice. La *smart city* et la *safe city* sont les deux faces d'une même pièce. Que ce soit pour une gestion soi-disant écologique de la ville ou bien pour mener de manière plus efficace la chasse aux pauvres, ce sont les mêmes infrastructures technologiques qui sont utilisées, les mêmes acteurs privés et le même marché économique sont convoqués.

Vous avez un exemple ?

> ***« Que ce soit pour une gestion soi-disant écologique de la ville ou bien pour mener de manière plus efficace la chasse aux pauvres, ce sont les mêmes infrastructures technologiques qui sont utilisées. »***

Le cas des lampadaires est assez parlant. Plusieurs villes mettent en place des lampadaires connectés, dotés de détecteur de mouvement, qui s'allument lorsqu'une personne passe, dispositif justifié par un argumentaire pseudo-écologique. L'ajout de capteurs permet en réalité d'intégrer les lampadaires dans les schémas de sécurité des villes — que ce soit pour installer une caméra dessus, pour augmenter la luminosité lorsque les policiers ont détecté quelques chose et cherchent à éclairer un événement ou encore pour y ajouter une recharge de téléphone ou une antenne 5G. Dans les faits, ça contribue encore une fois à éjecter les personnes les plus précaires des centres-villes : un lampadaire qui ne s'allume que lorsqu'il y a du passage invite à considérer l'espace public comme un endroit où transitent des flux, non comme un potentiel espace de vie. La ville intelligente contribue à un solutionnisme technologique qui cache de vraies issues, celles qui ne sont pas tenues par la technocratie au pouvoir mais construites par et pour les gens. Quid des lampadaires avec un interrupteur pour les allumer ou les éteindre ? La fable d'une ville intelligente est en train d'évoluer. Il ne s'agit plus uniquement de cibler les métropoles : désormais, ce sont des « territoires connectés » qui sont visés. Une manière d'apposer un maillage numérique à toutes les échelles

possibles.

L'empreinte écologique du numérique devient de plus en plus préoccupante. Elle fait l'objet de nombreuses analyses et propositions. Le journaliste Guillaume Pitron pose par exemple la question de prioriser certains flux selon leur utilité sociale au nom de la sobriété énergétique. Ce fonctionnement viendrait toutefois remettre en cause un principe que vous défendez, celui de la neutralité du Net. Comment concilier ces deux préoccupations ?

Cela pose la question du sens politique et social que nous, en tant que société(s) connectée(s), voulons donner à Internet aujourd'hui. La neutralité du Net pose comme principe que les fournisseurs d'accès à Internet traitent tous les flux de communication de la même manière, sans bloquer, ralentir ou faire payer l'accès à certains contenus plutôt qu'à d'autres. Il s'agit d'un terrain où s'affrontent divers idéaux politiques et divers intérêts économiques, en prenant pour objet cette infrastructure technique, complexe et pleine de potentialités qu'est Internet. La neutralité peut recouvrir plusieurs dimensions politiques. L'une d'entre elles s'appuie sur une vision d'Internet en tant que bien commun, libre et accessible à tous et toutes de la même manière. C'est un bel idéal qui, dans les faits, rencontre un certain nombre d'obstacles : au niveau du fonctionnement des divers protocoles de communication, de la gestion des infrastructures, selon les moyens matériels personnels des gens qui se connectent ou en fonction de leur maîtrise des codes pour naviguer « librement » sur Internet. La neutralité du Net recouvre donc de multiples dimensions, à la fois technique, politique, économique et sociale.

[Stéphane Burlot]

Et l'empreinte écologique ?

Guillaume Pitron met un coup de projecteur sur la dimension écologique d'Internet. Ce qu'il nous semble interroger par ses travaux, c'est cette image d'Internet construite comme un espace virtuel (le cyberespace), libre et égalitaire par excellence, espace de tous les possibles complètement découplé des réalités physiques. Or il rappelle à raison qu'Internet, tel que nous le connaissons aujourd'hui, se construit grâce à des technologies et à des infrastructures coûteuses en énergie comme en matériaux rares et polluants, dont l'extraction et le traitement affectent de manière inégalitaire territoires et populations. Dans un même temps, certaines des valeurs dominantes qui gouvernent le développement des réseaux stipulent que tout doit être accessible partout à tout moment, de manière quasi instantanée, quel qu'en soit le coût écologique. Ce rapport au temps et à l'espace est caractéristique de nos sociétés modernes capitalistes. On pourrait faire, dans une certaine mesure, un parallèle avec la capacité de voyager jusqu'à l'autre bout du monde à très grande vitesse grâce au réseau de transport aérien. Cette « liberté de circuler » repose sur l'utilisation d'avions très gourmands et émetteurs de CO_2 polluants : aujourd'hui, nous qui avons accès à cette technologie et conscience des enjeux écologiques, nous sommes amené·es à réfléchir en quels termes il nous paraît juste et légitime de prendre l'avion pour nous déplacer. De la même manière, nous pouvons réfléchir à nos pratiques de communication, aux manières de concilier

l'ensemble de nos valeurs politiques : aussi bien la liberté et l'égalité d'accès et d'échange que la protection de l'environnement. Sans remettre en cause la neutralité du Net, on pourrait défendre ses usages purement médiatiques, de communications entre humains, avec des machines plus simples, plus lentes, et des réseaux gérés en bien commun. Réglementer les usages d'Internet peut être tout à fait compatible avec cette neutralité : celle-ci n'est pas affectée par le fait que nous n'ayons, par exemple, pas le droit de harceler. La neutralité du Net, à nos yeux, est importante car elle permet de mettre les gens à égalité, de faire en sorte que tout le monde puisse participer à la chose publique. D'éviter également de culpabiliser ou de pénaliser injustement les populations. C'est pourquoi nous n'avons pour l'instant traité le problème écologique que par le biais des industries, en attaquant le système publicitaire des GAFAM au cœur de la surconsommation.

Photographie de bannière : Stéphane Burlot

---

1. La Haute Autorité pour la diffusion des œuvres et la protection des droits sur internet, crée en 2009, est chargée de lutter contre le piratage d'œuvres protégées par le droit d'auteur à travers la riposte graduée. Début 2022, elle fusionne avec le Conseil supérieur de l'audiovisuel (CSA) au sein de l'Autorité de régulation de la communication audiovisuelle et numérique (Arcom).[↩]
2. La surveillance biométrique utilise des caractéristiques physiques et biologiques pour identifier les individus : reconnaissance faciale, empreintes digitales ou rétiniennes, etc.[↩]
3. Fichier de traitement d'antécédents judiciaires, mobilisé lors d'enquêtes judiciaires ou administratives.[↩]
4. Fichier de prévention des atteintes à la sécurité publique, portant sur les personnes susceptibles d'êtres impliquées dans des actions de violence collective. Il concernait 60 000 personnes en 2020.[↩]
5. Le RGPD interdit le fait de conditionner l'accès à un service à notre consentement d'y être surveillés, ce qui est la façon dont la surveillance publicitaire nous est actuellement imposée [ndla].[↩]