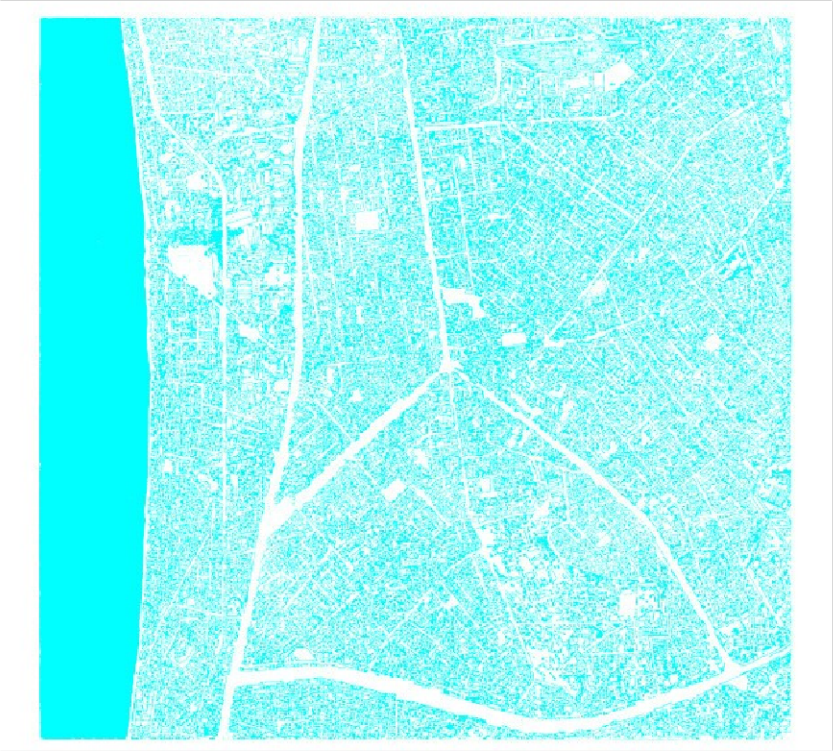
DU BROUILLARD DE L'INCERTITUDE



À L'ASSURANCE DES NUAGES

Il fut un temps où on traçait les gens sur base des empreintes qu'ils et elles laissaient sur leur passage. Mais le réchauffement climatique et la bétonisation ne laissent que peu de neige ou de boue à examiner. On préfère donc aujourd'hui se tourner vers les nuages, ou plutôt vers le cloud, pour inspecter les traces laissées dans le cyberespace. D'ailleurs, à l'heure où nous vivons de plus en plus « en distanciel » et que nous ne sortons plus de chez nous sans notre smartphone, pouvons-nous encore distinguer le « réel » du « virtuel » ? Exploration du pistage à l'ère numérique…

Instauration du passeport sanitaire, violation du secret médical par la transmission automatique d'informations personnelles concernant tests, quarantaines ou autres doses de vaccination, drones survolant les parcs pour inciter les gens à respecter la distanciation sociale, les pousser à rester chez eux voire évaluer le nombre de convives au réveillon de Noël : on peut dire que les technologies numériques ont apporté leur contribution à l'atmosphère détestable de flicage qui s'est installée dans le sillage de la pandémie de coronavirus. Néanmoins, il est une technologie de surveillance dont on a très peu entendu parler, à savoir le Wi-Fi.

« Comment ça le Wi-Fi ? pourriez-vous demander. Google ? Facebook ? Les géants du Net ?
— Oui certainement, vous répondrais-je. Mais le problème ne réside pas uniquement dans notre activité sur Internet. Il réside aussi dans les signaux que les smartphones envoient pour se connecter.
— Ah, vous voulez parler de l'application Coronalert, pour prévenir les « cas contacts » ? Mais n'utilise-t-elle pas plutôt le Bluetooth ?
— Si, en effet. Je l'ai oubliée dans mon introduction, peut-être parce que n'ayant pas rempli les promesses annoncées, les autorités l'ont discrètement enterrée… Mais non, je parle bien de la surveillance par Wi-Fi.
— Alors je ne vois pas de quoi vous voulez parler !

— C'est bien le problème ! Voyons ça… »

Il était une fois le smartphone. Couteau suisse numérique du XXIe siècle, ses atouts sont sa fabuleuse puissance de calcul, la formidable ergonomie de son écran tactile mais surtout la lucarne que celui-ci ouvre sur le monde. Pour que cette dernière fonction soit pleinement remplie, la connexion est de mise. Pas d'appel, de messagerie, de météo ou de likes et encore moins de challenge TikTok tant qu'il n'y a pas de signal.

Tout téléphone portable envoie donc régulièrement un signal pour se faire connaitre de l'antenne télécom la plus proche[1]. S'il s'agit d'un smartphone dont la fonction Wi-Fi est activée, il va de surcroit envoyer des requêtes pour tenter de repérer le boitier internet de votre maison, de votre lieu de travail ou de quelque lieu où vous vous seriez déjà connecté·e. Capter ces signaux est un jeu d'enfant. Pas besoin de matériel lourd réservé uniquement aux services de renseignement. Non, quelques lignes de code suffisent à convertir le premier ordinateur portable venu en mouchard. Les informations ainsi recueillies sont plus ou moins riches en fonction de l'appareil utilisé. Les téléphones récents disposent de systèmes d'anonymisation automatique pour limiter la fuite de données personnelles. Mais les téléphones vieux de quelques années peuvent diffuser allègrement leur identifiant unique (adresse MAC), et les noms des derniers réseaux auxquels ils se sont connectés.

À un niveau plus expérimental, une technique alternative consiste à placer de nombreux capteurs dans une pièce où sont diffusées des ondes Wi-Fi. La présence et le déplacement de corps humains viennent perturber la répartition de ces ondes dans l'espace. Les variations d'intensité des signaux peuvent réciproquement être inter-

1 À noter que les opérateurs télécom ont longtemps été légalement contraints de conserver ces données durant un an. Merci à celles et ceux qui ont lutté pour qu'un jugement européen fasse casser cette loi. Cependant, la France a déjà annoncé qu'elle contournerait cette décision, à voir donc comment la Belgique réagira… Affaire à suivre !

prétées pour déterminer le nombre et l'emplacement des personnes présentes.

Mais qui utilise les ondes pour nous tracer et dans quel but ?

La première fois que j'ai entendu parler de cette technologie, c'était il y a quelques années, lors d'un déménagement. Le conducteur de la camionnette contribuait autant à meubler mon salon que la conversation. Il me confia avoir passé sa journée de la veille à travailler (au noir) à dissimuler des capteurs dans les plafonds des magasins du centre commercial City2. Les mouchards devaient mesurer les flux de passant·es et ainsi permettre au gestionnaire du centre d'adapter les loyers des différentes cellules commerciales.

Dans le secteur de la vente, c'est ce qu'on appelle la *footfall analytics* ou l'analyse de fréquentation. Elle est généralement basée sur l'analyse des ondes, mais elle peut aussi reposer sur celle d'images caméra ou sur une combinaison de ces deux méthodes. L'objectif déclaré est de mieux comprendre les habitudes des client·es en vue de faire grimper le chiffre d'affaires. En plaçant plusieurs capteurs Wi-Fi ou caméras, on peut facilement observer si un·e client·e passe plus de temps au rayon légumes ou au rayon biscuits, ou encore repérer un comportement jugé suspect, peut-être celui d'un·e voleur·se.

Si en prime on arrive à faire installer aux client·es quelque application mobile, il devient possible de prolonger la surveillance en dehors du magasin, d'alimenter les fameux *clouds* en une kyrielle de données, mais surtout de proposer de la publicité ciblée qui pourra s'adapter continuellement aux comportements observés. C'est bien ce qui s'est passé dans les centres commerciaux bruxellois gérés par AG Real Estate, où la gestion des données Wi-Fi était confiée à la société Fidzup, qui traitait celles-ci sans consentement préalable. Mise en

demeure par la CNIL pour cette pratique contrevenant au Règlement général sur la protection des données (RGPD)[2], la société Fidzup a été contrainte de se mettre en règle mais a fini par devoir mettre la clé sous la porte.

Un représentant d'une société qui place ce type de dispositifs dans des chaines de magasins me racontait avoir été une fois froidement accueilli par les employé·es du magasin où il venait l'installer : ces dernier·es avaient bien compris que l'analyse ne s'appliquait pas qu'aux client·es mais aussi aux vendeur·ses. Un mauvais « taux de conversion » – soit un ratio trop faible entre le décompte de client·es entré·es dans le magasin et le nombre de tickets imprimés pendant vos heures de travail – et hop ! voilà que le système pouvait enregistrer une nouvelle sortie du magasin, définitive celle-ci. Ou comment se faire virer par une box Wi-Fi…

Nouvelle confrontation avec l'exploitation des ondes Wi-Fi en 2019, lorsque l'asbl Constant a organisé une balade dans le Marché de Noël de Bruxelles pour attirer l'attention sur l'utilisation de cette technologie dans l'espace public[3]. On y apprenait que c'était une expérience menée en partenariat par un laboratoire de polytechnique de l'ULB (OPERA-WGC) et Brussels Major Events (BME), une asbl satellite de la Ville de Bruxelles, qui prend en charge l'organisation des grands évènements de la capitale, tels que le Nouvel An ou Bruxelles-les-Bains. Lors de ces évènements, l'intérêt n'est assurément plus de fixer les loyers, mais de « gérer la foule ». S'il y a un incident qui hante les nuits des organisateur·ices d'évènements à Bruxelles, c'est bien « le drame du Heysel » de 1985, lors duquel un mouvement de foule avait provoqué la mort de dizaines de personnes et en avait blessé plusieurs centaines. L'idée est donc d'évaluer le nombre de personnes présentes à un évènement de masse, de

2 Lire le *Footfall Almanac*, p. 42 et le rapport de la CNIL, p. 71.

3 Cette balade concluait l'exploration menée par Kurt Tichy et Alex Zakkas, dont on peut retrouver le travail à l'adresse http:/all-syste.ms/now

manière à mieux canaliser la foule voire fermer les accès en cas de dépassement du seuil choisi.

Comme tout le monde n'a pas forcément sur soi un smartphone dont le Wi-Fi est allumé, un facteur multiplicatif est appliqué sur base de tests effectués en croisant différentes techniques de comptage. À en croire les ingénieur·es en charge du projet, il n'y a néanmoins pas le moindre souci à se faire du côté de la vie privée, car les données sont directement anonymisées, au point qu'un bureau d'avocat·es ayant examiné leur procédure a certifié sa conformité avec le RGPD. Dans la mesure où tous les expert·es en matière de données relatives à la vie privée insistent sur le fait que l'anonymisation est un leurre et qu'il est préférable de parler de « pseudonymisation » en gardant en tête qu'il est généralement possible de réidentifier les données, le scepticisme est de mise face aux déclarations des ingénieur·es. Mais il est vrai que la technique mobilisée ici, composée d'opérations successives de hachage et de chiffrement, et ce directement au niveau de la capture de l'information, avant même son envoi vers les serveurs de conservation des données, semble effectivement assez sérieuse. Et en l'absence d'autres données personnelles associées à l'identifiant anonymisé, il n'y a effectivement pas de possibilité de réidentification.

La prudence reste de mise, comme l'illustre la société d'analyse vidéo ACIC : elle propose une formule « Privacy » qui floute les visages des personnes sur les images de vidéosurveillance. Mais la fonction peut être désactivée par qui dispose des droits d'administration, de manière à pouvoir fournir des images « désanonymisées » à la police en cas de besoin. Dans la mesure où l'expérience menée à l'ULB s'avère porter ses fruits, elle pourrait faire l'objet d'une commercialisation dans les prochaines années : que répondront les ingénieur·es quand la police conditionnera l'achat de leur système à la possibilité de se réserver un accès privilégié aux données brutes ?

Déconfinement de la surveillance

Lorsque la pandémie de coronavirus s'est atténuée et que les magasins ont pu rouvrir, la ville de Bruxelles a contacté BME pour réfléchir à la meilleure manière de gérer la foule dans le centre-ville. BME, à son tour, s'est reportée sur l'équipe de chercheur·ses d'OPERA-WGC et très vite, la décision a été prise d'installer des capteurs Wi-Fi le long de la rue Neuve de manière à limiter l'affluence et à faire respecter les distances préconisées pour enrayer la propagation du virus. Lors du déconfinement, un dispositif de barrières, bandes de circulation piétonne et feux de signalisation aux entrées de la rue matérialisaient le dispositif. Aujourd'hui, la régulation se fait plutôt sous la forme de recommandation : les chalands peuvent consulter le site rueneuvebruxelles.be pour s'informer sur les moments plus calmes de la journée durant lesquels il serait préférable de faire son shopping. Mais les capteurs sont toujours présents.

L'épidémie a favorisé ouvertement le déploiement de techniques de *footfall analytics* dans l'espace public, mais la tendance, pourtant bien réelle, est moins visible dans les espaces privés. En effet, bien que ces techniques soient méconnues du grand public, elles sont déjà fort répandues dans les commerces. Le site carto.technopolice.be recense différentes technologies de surveillance et de contrôle présentes dans l'espace public. Y sont principalement répertoriées les caméras de surveillance classiques, « intelligentes » ou à reconnaissance de plaque d'immatriculation, mais aussi les antennes télécom et les dispositifs de *footfall analytics*. On retrouve donc la rue Neuve sur la carte, ainsi que les principaux centres commerciaux. Si l'on sait que les pictogrammes devant indiquer la présence de caméras de vidéosurveillance sont rarement dûment installés, au moins les caméras sont-elles visibles… tandis que les dispositifs de comptage peuvent être relativement discrets. Lors de la balade de l'association Constant au Marché de Noël, bien que connaissant leur présence, nous n'avons pas été en mesure de les repérer physiquement. Il est

donc possible que la carte de Technopolice sous-estime grandement l'ampleur du phénomène. Et de fait, la société Amoobi – spin-off du laboratoire de l'ULB susmentionné – indique par exemple sur son site compter parmi ses client·es rien de moins que IKEA, MediaMarkt, Brico, Carrefour, Delhaize, Aldi, et j'en passe[4]. La question n'est donc pas tant de savoir si les espaces urbains échappent à ce type de surveillance mais plutôt *lesquels* y échappent.

Au rayon futurologie

Les ingénieur·es d'OPERA-WGC ne se contentent pas de décrire ce qui est mais ambitionnent aussi de prédire ce qui sera. Les données collectées sont analysées au cours de la journée de manière à dégager des modèles, ce qui a permis de développer des algorithmes de prédiction d'affluence. Ainsi, s'il est 9 h du matin à l'heure d'écrire ces lignes, le site rueneuvebruxelles.be prévoit des pics de fréquentation entre 13 et 17 h. Sans l'appui de tels algorithmes, nous allons nous aussi nous risquer à esquisser la direction que pourraient prendre les ondes Wi-Fi à l'avenir…

À la STIB par exemple, un système compte déjà le nombre de franchissements de portiques dans les stations et des recommandations sont ainsi formulées sur les lignes et les heures à préférer. Mais ce n'est qu'un début. La société réfléchit depuis longtemps à des méthodes plus fines pour analyser la fréquentation de ses services et stations. Aucune solution existante sur le marché n'a encore satisfait ses dirigeant·es. Elle a donc récemment annoncé le lancement d'un gigantesque chantier nommé « muntsroom », en partenariat avec Agoria, le lobby des industriels des nouvelles technologies, et à grand renfort de fonds régionaux et européens. Le projet a pour objectif de développer « une solution permettant de visualiser les flux de personnes 24 heures sur 24 et 7 jours sur 7 (comptage, direction,

4 En raison de difficultés d'exploitation des données issues des ondes (réflexion, réfraction…), la société Amoobi se concentre aujourd'hui sur l'analyse d'images issues de caméras.

vitesse), de faciliter l'analyse partagée des données et de mettre les données sur les flux de personnes à la disposition d'un large éventail d'utilisateurs »[5]. Le marché sera attribué en décembre 2021.

Par ailleurs, OPERA-WGC et Brussels Major Events ont aussi collaboré sur un projet de recherche avec la société Proximus. En tant qu'opérateur télécom, Proximus quadrille le territoire d'antennes GSM. Comme on l'a vu, ces antennes permettent de localiser les téléphones. Avec la succession des générations de téléphonie, les puissances d'émission augmentent, ce qui nécessite d'ajouter toujours plus d'antennes, réduisant d'autant la taille des cellules. Le déploiement de la 5G à haute fréquence n'annonce donc rien de bon de ce côté-là. De plus, les opérateurs téléphoniques sont généralement aussi des fournisseurs d'accès à internet (FAI). Tel saint Pierre aux portes du Paradis, ce sont eux qui ouvrent la voie vers le *cloud*. C'est le cas de Proximus, qui propose aussi un bien mal-nommé « public wi-fi » pour permettre à ses client·es de se connecter d'à peu près n'importe où. Ce service exploite en fait les boitiers internet des particulier·es qui diffusent un signal accessible à tou·tes les abonné·es Proximus en plus du Wi-Fi local. Avec une infrastructure réseau tentaculaire, un registre clientèle permettant de relier facilement les identifiants des appareils à des individus en chair et en os, un chiffre d'affaires autorisant de somptuaires dépenses en recherche et développement, la société est bien positionnée pour déployer une surveillance massive sur le territoire belge.

J'ai pointé les enjeux de vie privée liés aux données personnelles, mais ces technologies nous en apprennent aussi sur l'évolution des modes de gouvernement. Elles favorisent l'avancée vers un monde où il n'y a plus ni droit, ni obligation, ni interdiction générale de faire ceci ou cela – de circuler rue Neuve ou de se rendre à un concert, de se faire tester ou vacciner. Non, dorénavant, la situation sera analysée en temps réel et l'autorisation pourra être accordée ou refusée au cas par cas, en fonction de l'impact attendu de toute action sur la

5 Voir le rapport sur le site de la STIB.

courbe de croissance, de santé ou de quoi que ce soit qu'il s'agira d'optimiser selon l'agenda du moment. Si nous ne regretterons pas la rigidité procédurale qui pouvait caractériser jusqu'ici l'action étatique, il n'est pas certain que l'instabilité permanente dans laquelle nous plongeons soit beaucoup plus respirable.

Peut-on échapper à la surveillance ?

Individuellement, il est bien sûr possible de laisser son téléphone à la maison ou de désactiver le Wi-Fi et le Bluetooth de notre smartphone avant de sortir de chez nous, de manière à disparaitre des radars. À l'inverse, certain·es hacker·euses proposent plutôt d'inonder les systèmes de surveillance de toutes sortes d'informations plus ou moins farfelues pour que les vraies données se retrouvent noyées dans le « bruit »[6]. Il existe aussi des systèmes d'exploitation sous licence libre, qui s'attachent à améliorer la sécurité informatique des appareils et à limiter les possibilités de surveillance. Des « ateliers d'autodéfense numérique » sont régulièrement organisés pour partager les savoirs et les pratiques sur le sujet[7]. Ces moments permettent surtout ne pas rester seul·e face aux difficultés qu'on rencontre immanquablement dès qu'on s'écarte des solutions toutes faites. Ces ateliers peuvent aussi s'organiser au sein de collectifs, d'associations ou autres, de manière à poser collectivement la question : comment souhaitons-nous nous organiser et communiquer ensemble ? Avec quelles conséquences pour nos vies quotidiennes ? Nos socialités ? Notre environnement ? Dans quelle mesure tel choix nous rend plus libres ou plus dépendant·es ? Il est alors possible de toucher au caractère politique de ces questions et de réaliser qu'elles méritent d'être posées à toutes les échelles. Cependant, tant que les entreprises et les gouvernements courront après les données pour mieux

6 À ce sujet, lire le travail de Helen Nissenbaum & Finn Brunton, *Obfuscation*, C&F, 2019.

7 Ces ateliers sont généralement répertoriés sur des sites comme hackeragenda.be ou agendadulibre.org

nous profiler et nous gérer, il nous faudra tenir le rythme. Mais sans disposer des mêmes moyens, pourrons-nous tenir la distance ? Il apparait par exemple que des modes de surveillance basés sur la détection des odeurs corporelles sont actuellement à l'étude, témoignant une fois encore de l'absence de limite à ce qui peut faire l'objet d'une mesure et d'une analyse. Allons-nous enfiler des combinaisons d'astronaute pour nous protéger de tout type d'intrusion ?

Ou bien ne vaut-il pas mieux mettre un terme à la société de surveillance ?

***

Merci aux responsables de ACIC et OPERA-WGC qui ont bien voulu répondre à mes questions.

***

Cet article a été initialement publié dans une version légèrement différente sous le titre « Pistage dans le cyberespace » dans le numéro 53 du journal Culture & Démocratie.

***

Illustration de couverture : Benjamin Monteil

Résister à la surveillance totale de nos villes et de nos vies

En Belgique, on entend toujours plus fréquemment parler de « Smart City » ou de « ville intelligente », d'innovations technologiques censées accélérer les flux numériques et leur traitement (5G), d'outils toujours plus sophistiqués et automatisés comme les caméras intelligentes… Il serait absolument nécessaire d'investir massivement dans ce secteur, la capitale européenne ne pouvant évidemment pas se permettre de rater le virage technologique !

Derrière les discours technophiles mettant en avant les bénéfices liés à ces technologies qui devraient globalement améliorer la qualité de vie des individus, que cela soit sous l'angle de la santé, de la sécurité, de la mobilité, etc., se cache en réalité des intérêts économiques colossaux et une volonté de contrôle social toujours accrue.

Le déploiement de ces outils sécuritaires visant à quadriller, surveiller, classer, punir dans le but d'orienter et de réguler les comportements se fait bien souvent dans l'indifférence la plus totale, grâce à la complicité liant l'industrie et les décideurs politiques ; ces derniers étant dans le meilleur des cas coupables par négligence ou naïveté, lorsqu'ils ne sont pas eux-mêmes à l'origine de l'adoption de ces gadgets liberticides (caméras ANPR reconnaissant les plaques d'immatriculation, reconnaissance faciale, drones survolant l'espace public et notamment les manifestations, compteurs énergétiques intelligents, etc.).

Face à ce constat, nous sommes plusieurs à regretter le manque d'information et de débat concernant les implications sécuritaires de l'adoption de ces outils technologiques. Nous déplorons l'absence d'une véritable critique de cette surveillance urbaine toujours plus massive. C'est pourquoi nous avons décidé de répondre au projet « Technopolice » initié en France par *La Quadrature du Net* et de l'étendre à Bruxelles, voire à la Belgique.

Notre objectif est de rendre ainsi visibles les menaces liberticides que représentent ces outils de contrôle en région bruxelloise, en centralisant l'information les concernant sur une même et unique plateforme accessibles à tout·e·s. Au travers de ce travail informatif, nous souhaitons donner à chacun·e la possibilité d'appréhender ces enjeux, de bâtir des outils et des stratégies de résistance contre la surveillance, afin que le déploiement de ces outils policiers s'enraye, que la militarisation de l'espace public soit mise en échec et qu'in fine, la technopolice trépasse !

Contre cette dystopie que préparent ceux qui prétendent nous gouverner, nous appelons à une résistance inflexible.

TECHNOPOLICE.BE