JAN WALRAVEN

Le vol du siècle

Comment nous avons perdu notre vie privée et comment la reconquérir

Now Future Éditions

Table des matières

PREMIÈRE PARTIE

On vous suit

DEUXIÈME PARTIE

On vous met dans des cases

TROISIÈME PARTIE

On vous vend

QUATRIÈME PARTIE

On se sert de vous

CINQUIÈME PARTIE

Après le vol

Première partie

ON VOUS SUIT

Chapitre 1er

Un petit poucet numérique

Imaginez la situation suivante. Depuis vos 12 ans, vous n'avez plus jamais été seul. À aucun moment. Dès que le réveil sonne et que vous ouvrez les yeux, un individu se tient à vos côtés, un bloc-notes et un stylo à la main. Aucun de vos gestes n'échappe à ce personnage tout de gris vêtu.

« Levé à 7h04. »

« Tiré la chasse à 7h09. » « Douché entre 7h11 et 7h17 – plus longtemps que la moyenne – avec du savon Nivea. »

« Entièrement habillé à 7h20 – n'a pas mis de slip propre. »

« Mangé deux tartines à la confiture de fraise et lu dans le journal trois articles de sport entre 7h21 et 7h30. »

« Parti à vélo à 7h33 et arrivé à la gare – après un problème de chaîne – à 7h40. »

« Acheté du café à 7h41. »

« Monté dans le train – en retard – à 7h46. »

Et ainsi de suite. Les seuls moments où vous ne voyez pas le personnage gris et taciturne, c'est lorsque vous dormez. Mais son bloc-notes fait état de votre rythme respiratoire et de votre fréquence cardiaque pendant la nuit, ainsi que du fait que vous êtes allé aux toilettes à 3h33. Chaque jour, à minuit, le rapport de la journée écoulée est transmis à une organisation dont vous ne connaissez que le nom et dont vous avez déjà vu le CEO à la télé. Pour le reste, vous ignorez à quoi servent les rapports journaliers.

Vous constatez cependant que le journal contient de plus en plus de sujets sportifs. Que depuis quelque temps, les publicités pour du gel douche, du café et de la confiture se multiplient à la télé. Récemment, vous avez même trouvé au courrier un dépliant publicitaire pour des sous-vêtements Eskimo… Et pourquoi donc le réparateur de vélo vous a-t-il déjà appelé trois fois ce mois-ci pour vous proposer un contrat d'entretien à vingt pour cent de réduction ?

Vous accepteriez, vous, d'être ainsi suivi jour après jour, à tout moment du jour et de la nuit, par quelqu'un que vous ne connaissez ni d'Ève ni d'Adam ? Qui note scrupuleusement tout ce que vous faites, tout ce qui vous fait rire ou vous fâche, les personnes avec qui vous sortez au restaurant, les vêtements que vous achetez, l'adoucissant que vous utilisez, la confiture que vous tartinez, le train que vous prenez et à quelle heure, le goût que vous avez pour le café, les articles de presse que vous lisez…

Non ? Cette idée ne vous plaît pas ? Alors j'ai une mauvaise nouvelle à vous annoncer : le scénario décrit n'est pas de la fiction. D'accord, aucun personnage habillé de gris ne vous accompagne dans la douche, mais vous n'en êtes pas moins épié à tout moment. Sans que vous le sachiez, ou sans que vous en ayez conscience.

Les informations que nous avons confiées ces dernières années à nos appareils numériques, nous ne les confierions même pas à nos meilleurs amis.

Bienvenue dans le nouveau monde, un monde où quelqu'un s'enrichit de chacun de vos gestes. Et ce monde a vu le jour grâce à l'invention la plus révolutionnaire de la seconde moitié du vingtième siècle : l'internet. Jamais il n'a été plus facile de communiquer avec ses proches, ses amis ou des inconnus, partout dans le monde. Une quantité gigantesque d'informations est disponible plus facilement et plus rapidement que jamais. Nous lisons des livres et des journaux en ligne, nous écoutons de la musique en ligne, nous « *streamons* » des films et des séries, nous achetons des vêtements et des cadeaux dans des boutiques en ligne, nous communiquons et discutons en ligne, nous nous disputons en ligne, et nous trouvons en ligne l'amour de notre vie. Nous vivons en ligne, presque toute la journée. Tout cela,

vous le saviez déjà. Pas besoin de vous expliquer par le détail les plaisirs que procure l'internet. Nous pouvons à peine nous en passer, nous sommes scotchés à l'écran de notre *smartphone*, *laptop* ou tablette.

Or toute médaille a son revers. Tout ce que vous faites en ligne est enregistré, stocké, analysé. Partout où vous passez, vous laissez une empreinte numérique, une trace faite de uns et de zéros. Comme le Petit Poucet. Mais nous ne laissons pas nos miettes numériques derrière nous pour retrouver notre chemin. Ces miettes apparaissent dans notre sillage sans que nous en ayons conscience. Comme dans le conte de Perrault, il y a des prédateurs qui picorent ces miettes. Et ces prédateurs, ce ne sont pas des oiseaux affamés, mais des entreprises de tailles diverses dont nous ignorons jusqu'à l'existence, mais aussi des autorités locales et nationales. Grâce à des technologies innovantes conçues à cet effet, elles nous suivent partout où nous nous rendons dans le monde virtuel, mais aussi dans la vraie vie.

Dans la première partie, je m'étendrai sur ces technologies et les données qu'elles collectent à notre propos. Comment sommes-nous filés, et quelles informations intéressent ces ombres ? Et le navigateur internet sur notre *laptop*, notre *smartphone*, les réfrigérateurs et les poteaux d'éclairage intelligents de la rue, que savent-ils de nous, et comment ont-ils obtenu ces informations ?

L'ordinateur très personnel

Avant l'arrivée des *smartphones*, tablettes et autres gadgets intelligents, nous surfions toujours sur internet via notre PC ou *laptop*, un ordinateur personnel grâce auquel nous pouvions entrer en contact avec le reste du monde via l'internet. En 2005, près de la moitié de tous les ménages belges possédait une connexion internet ; en 2017, cette proportion avait atteint 86 pour cent. En 2016, selon les chiffres d'Eurostat, 78 pour cent des utilisateurs belges d'internet utilisaient un *laptop* pour surfer, alors qu'aux Pays-Bas, 64 pour cent des surfeurs se servaient d'un ordinateur fixe. Une grande partie de notre consommation d'internet se déroule donc toujours sur notre PC ou *laptop*, via notre navigateur, qu'il s'agisse de Google Chrome, de Microsoft Internet Explorer et Edge, ou de Mozilla Firefox. Derrière

les écrans de ces navigateurs se déroule la première strate, intéressante, d'un ensemble très complexe de techniques de filature qui sont appliquées en ligne, sans que nous en ayons conscience. Mais comment ces techniques fonctionnent-elles exactement ?

Des miettes

Une première de ces techniques de filature est presque aussi ancienne que l'internet lui-même. Il s'agit des *cookies* qui ne sont rien d'autre que de petits fichiers de texte. Ils ont été développés pour permettre aux sites web de garder des informations sur leurs visiteurs et aussi, en dernier ressort, pour enregistrer le comportement de navigation des visiteurs, à la manière d'un minuscule passeport numérique. Lorsque vous surfez sur un site web, vous vous connectez toujours sur un serveur. Ce serveur envoie ensuite un *cookie* vers le navigateur avec lequel vous parcourez l'internet. Ce *cookie* est stocké dans votre navigateur de sorte que le site web puisse vous reconnaître lors d'une prochaine visite. Si vous surfez pendant quelques heures, votre navigateur contient donc une multitude de ces *cookies*. Sans doute avez-vous déjà fermé ou accepté des centaines de fois, sans réfléchir, la mise en garde que les autorités européennes obligent tous les sites web à afficher à propos des *cookies*.

Ces *cookies* ont aussi leur utilité. Sans eux, un site web ne fonctionnera pas comme le développeur l'a prévu. Les petits fichiers de texte informent par exemple les sites de presse que vous êtes abonné et que vous pouvez avoir accès à la partie payante, ou ils sont utilisés pour retenir quels produits vous avez mis dans le panier d'une boutique en ligne. Si vous supprimiez tous les *cookies* contenus dans votre navigateur, chaque site que vous visiteriez ensuite aurait l'apparence d'un site que vous visitez pour la première fois. Le propriétaire d'un site veut offrir à chaque utilisateur l'expérience le plus personnelle possible, et les *cookies* en constituent le moyen. Bon, d'accord. En même temps, cela signifie que de nombreuses informations vous concernant sont stockées par l'entreprise qui gère ce site web.

Or le propriétaire de ce site particulier n'est pas le seul que votre visite intéresse : un grand nombre d'autres entreprises souhaitent aussi en savoir plus sur votre personne. Elles veulent en outre savoir quels sont les autres sites que vous visitez, à quelle fréquence, et ce que vous y faites ou y cherchez. C'est pourquoi les développeurs ont créé un type spécifique de *cookie* qui ne se limite pas à un seul site, mais qui est au contraire capable de suivre et d'enregistrer les utilisateurs sur de nombreux sites différents. Ces *cookies* de traçage sont des versions élaborées des simples *cookies*. Ils vous suivent à travers tout l'internet, d'un site à l'autre, et retiennent ce que vous faites en ligne.

Lorsque vous visitez un site web, vous y croisez souvent des publicités. Souvent, elles émanent d'une partie tierce qui souhaite promouvoir ses produits ou services. Pour pouvoir afficher cette publicité, votre navigateur doit aussi établir une connexion avec le site de cet annonceur. À ce moment-là, l'annonceur envoie à votre navigateur un *cookie* de traçage qui lui indique que vous avez vu ses publicités. Lorsque vous vous rendez ensuite sur un autre site web, il se peut que ce même annonceur y affiche la même publicité, ou au contraire une publicité totalement différente. Et grâce à ce *cookie* de traçage, l'annonceur sait aussi quand vous pouvez voir sa publicité sur cet autre site web. Il peut donc tenir un registre des sites web que vous avez visités, du moment où vous les avez visités et aussi si vous avez cliqué sur ses pubs.

Il est donc important pour les entreprises publicitaires de pouvoir installer des *cookies* de traçage sur le plus grand nombre de sites possible, histoire de pouvoir vous suivre dans toutes vos pérégrinations virtuelles. Ensuite, plus vous visitez de sites, plus elles en savent sur votre comportement en ligne. C'est notamment grâce à ces *cookies* que vous avez l'impression d'être poursuivi par certaines pubs. Puisque chaque annonceur individuel ne peut pas négocier avec les millions de sites web existants, des réseaux publicitaires ont été créés pour faire le lien entre l'annonceur et le vendeur d'espaces publicitaires. Ces réseaux achètent de l'espace publicitaire sur le plus grand nombre de sites possible pour permettre à leurs clients – les annonceurs – de montrer leurs publicités sur tous ces sites. Ce sont ces intermédiaires qui installent les *cookies* de traçage dans votre navigateur. Lorsque vous voyez une pub dans votre navigateur, vous établissez une connexion

non pas avec les serveurs de l'annonceur lui-même, mais avec le serveur central du réseau publicitaire, lequel enregistre, stocke et analyse votre comportement de navigation.

Un chemin de miettes

Les *cookies* de traçage ne sont plus les seuls outils servant à vous suivre sur Internet, loin de là. Avec l'avènement des bloqueurs de publicité et la possibilité, offerte désormais par la plupart des navigateurs, de bloquer ces *cookies* de parties tierces, les entreprises et réseaux publicitaires ont été obligés de chercher d'autres modes de filature. Et les possibilités sont énormes. Il y a par exemple les balises (*beacons*, en anglais) ou les pixels espions (*tracking pixels*). Au départ, il s'agissait de petites illustrations, invisibles à l'œil nu, intégrées sur un site, par exemple dans la même couleur que le fond du site.

Aujourd'hui, une telle balise ne doit plus nécessairement être une illustration, il peut s'agir aussi d'un petit bout de code informatique ajouté au site. À chaque visite, cette illustration ou un autre morceau d'information est téléchargé au départ d'un serveur et permet au propriétaire de ce serveur de savoir quel utilisateur visite ce site, quand il le fait et depuis quel ordinateur. Entre-temps, une flopée d'extensions et de petits programmes ont été développés pour bloquer les *cookies* de traçage de parties tierces. Un pixel espion permet toutefois aux annonceurs de contourner ce blocage et donc de vous suivre malgré tout. Il constitue aussi une façon moins complexe de suivre le comportement de navigation des utilisateurs. Ainsi, Facebook propose un pixel espion propre à son site. Les entreprises qui souhaitent faire de la pub sur Facebook peuvent ajouter ce petit bout de code informatique à leur site et vérifier ainsi si ces publicités ont des répercussions positives sur leur propre site, par exemple lorsqu'un utilisateur clique sur une publicité Facebook pour ensuite faire un achat dans leur *webshop*. Toutes ces manipulations se font à l'insu des utilisateurs qui, souvent, n'ont pas conscience qu'ils se rendent sur un autre serveur.

C'était aussi le cas de la Turque Elif, jusqu'au jour où la police est venue tout à coup sonner à sa porte. Elif avait déjà perdu son emploi

d'enseignante parce que des traces de ByLock, une messagerie instantanée suspecte aux yeux du gouvernement turc, avaient été trouvées sur son téléphone. Pourtant, Elif n'en démordait pas : elle n'avait jamais utilisé ni téléchargé cette appli. Comment s'était-elle alors retrouvée sur la liste noire ? L'expert en informatique Tuncay Bepkgi a résolu le mystère après avoir analysé des milliers de cas tels que celui d'Elif. Le coupable était un pixel espion. ByLock avait été développé et était utilisé par des partisans de l'intellectuel turc exilé Fethullah Gülen, soupçonné d'avoir fomenté le coup d'État de 2016. Chaque Turc ayant un jour établi une connexion avec les serveurs de ByLock est dès lors considéré comme un traître potentiel à la patrie. Pour brouiller les pistes, les développeurs gülenistes de ByLock ont conçu le plan de « souiller » cette liste noire avec de prétendus partisans. La technologie qui leur permettait de le faire existait déjà. Bepkgi découvrit que les développeurs de ByLock avaient aussi intégré un pixel espion invisible dans d'autres applis, notamment une appli permettant de rechercher les horaires de la prière islamique. Ainsi, chaque fois qu'Elif utilisait l'une de ces applis contaminées, son téléphone téléchargeait le pixel espion et établissait donc à son insu une connexion avec le serveur de ByLock. Résultat : Elif, ou à tout le moins son téléphone, se retrouva sur la liste noire des utilisateurs de ByLock sans jamais avoir utilisé cette messagerie. Grâce à l'enquête de Bepkgi, plusieurs Turcs qui, comme Elif, avait été suspectés d'utiliser ByLock et donc d'appartenir au mouvement de Gülen, ont été blanchis entretemps.

L'histoire d'Elif prouve que le comportement en ligne que nous adoptons à notre insu peut être lourd de conséquences. Le traçage des utilisateurs ne s'arrête pas non plus aux *cookies* et aux pixels. Sans cesse, de nouvelles manières d'identifier, d'enregistrer et de poursuivre les utilisateurs sont mises au point. Ainsi, il est possible aujourd'hui de prendre l'empreinte digitale d'un navigateur : un poinçon unique qui permet d'identifier le navigateur, et donc son utilisateur, lorsqu'il visite un site web. Utilisez-vous Chrome, Firefox ou Internet Explorer ? Vous avez paramétré le français comme langue d'interface ? Vous avez installé un bloqueur de publicité ? Comment votre écran est-il configuré ? Quel est votre système d'exploitation ? En raison de tous ces

paramètres et de nombreux autres encore, votre navigateur affiche des caractéristiques uniques, grâce auxquelles une empreinte numérique unique du navigateur peut être composée pour la grande majorité des utilisateurs. Les sites web peuvent ainsi non seulement identifier les utilisateurs et réduire le risque de piratage, mais aussi suivre les utilisateurs via différents sites web et collecter des informations quant à leurs préférences. Il existe des dizaines d'autres techniques permettant d'atteindre le même but. Certains sites retiennent quelles pages vous visitez et sur quels éléments vous cliquez, mais aussi comment vous faites glisser la souris sur une page. Ces informations permettent de savoir quels éléments vous intéressent davantage que d'autres.

Chaque pas que nous faisons en ligne est observé. À notre insu, des entreprises et organisations scrutent tous nos faits et gestes. Elles veulent savoir ce que nous faisons, et quand. Heureusement, il est possible de savoir quelles sont ces entreprises.

AU BANC D'ESSAI

Suivre et être suivi

Pour me faire une idée de la présence de ces technologies, pour savoir comment elles fonctionnent exactement et quelles entreprises y ont recours, j'ai décidé début 2018 de jeter un œil sous le capot des sites d'actualité HLN.be et Nieuwsblad.be, les sites web les plus populaires de notre pays. Avec plus de 57 millions de visites, HLN.be était le site belge le plus fréquenté en décembre 2017. Le site du *Nieuwsblad* occupait la deuxième place, avec plus de 50 millions de visites. Comme tout l'internet, les visites que reçoivent ces sites sont scrutées par diverses parties. Heureusement, il est possible de retourner les rôles, grâce à de petits programmes qui permettent de voir quelles entreprises regardent par-dessus votre épaule.
J'utilise le programme Lightbeam, développé par Mozilla, la société-mère de mon navigateur Internet Firefox. Lightbeam révèle en temps réel les connexions invisibles établies par le navigateur. Je commence par désactiver les différents bloqueurs publicitaires que j'utilise d'habitude pendant la navigation. Je ne voudrais pas manquer certains traceurs. L'inconvénient est cependant qu'en désactivant ces bloqueurs publicitaires, je donne à certaines entreprises l'occasion d'observer une partie de mon comportement de navigation. Qu'à cela ne tienne.

Je me rends sur HLN.be, la version en ligne de *Het Laatste Nieuws*, le quotidien le plus populaire du pays, et aussitôt, Lightbeam m'indique les serveurs et sites avec lesquels j'établis une connexion et donc avec lesquels je partage des informations sur mon comportement de navigation. Le compteur grimpe rapidement et s'arrête sur un nombre impressionnant. Je n'ai encore visité que la page d'accueil, et mon navigateur a déjà établi une connexion avec 49 sites de parties externes. Lorsque je consulte ensuite l'un des articles principaux sur le site, le compteur poursuit sa progression et comptabilise 16 connexions supplémentaires. Ensuite, je me rends sur le site Nieuwsblad.be. C'est alors que se produit un événement intéressant. Je peux voir non seulement quels traceurs ont enregistré mes visites à HLN.be et Nieuwsblad.be, mais aussi lesquels m'ont suivi lorsque je suis passé d'un site à l'autre. J'ai visité trois pages web sur deux sites différents, et pendant ce temps, mon navigateur a établi une connexion avec 105 sites tiers au total. Avec 18 d'entre eux, mon ordinateur a été connecté aussi bien depuis HLN.be que depuis Nieuwsblad.be. Ces sites savent donc que j'ai visité à la fois HLN.be et Nieuwsblad.be, quand je l'ai fait et dans quel ordre.

Quelles sont donc ces 105 entreprises qui veulent connaître mon comportement de navigation ? Il est évident que les éditeurs des deux sites d'actualité figurent dans la liste. Mediahuis et De Persgroep veulent savoir ce que vous faites sur leurs sites, ce qui leur permet par exemple de les améliorer. Mediahuis, l'éditeur de *Het Nieuwsblad*, mais aussi du *Standaard* et de *Gazet van Antwerpen*, collabore à cette fin, notamment, avec Optimizely. Cette entreprise américaine précise sur son site que grâce à cette collaboration, les visiteurs des sites de Mediahuis cliquent sur un plus grand nombre de bannières publicitaires, que Mediahuis a augmenté ses ventes d'abonnements et peut vérifier aussitôt si les adaptations apportées à ses sites génèrent les résultats escomptés. De cette façon, Mediahuis apprend à mieux connaître le comportement et les besoins de son public. Fin 2016, pour le site d'actualité Apache, j'avais rencontré Annick Deseure, *digital-datamanager* chez Mediahuis. Selon elle, la collaboration avec Optimizely permet surtout à Mediahuis d'« adapter ses sites de façon plus objective et de mieux déployer l'actualité qui intéresse les visiteurs ». Mediahuis veut publier les nouvelles que les lecteurs veulent lire, et doit dès lors savoir sur quels éléments ils cliquent. C'est là qu'intervient Optimizely.

Outre les traceurs de Mediahuis et du Persgroep même, la liste des 105 entreprises curieuses contient les noms de Google et de Facebook, qu'on ne présente plus. Avec leur nombre énorme d'utilisateurs, ces groupes jouent dans une tout autre catégorie. Je reviendrai plus tard sur la

façon dont ils identifient le comportement en ligne de tous les internautes du monde, ou presque. Car parmi cette bonne centaine de traceurs figure toute une série de noms inconnus du grand public, mais qui ne manquent pas d'intérêt pour autant : Chartbeat, Gemius, Rubicon Projet, Gigya…

Prenons donc le temps de les examiner de plus près. Je commence par Chartbeat, qui développe des applications spéciales à la mesure des médias d'actualité. L'entreprise américaine se vante d'être la solution par excellence pour comprendre ce que les utilisateurs font du contenu des sites qu'ils visitent. Qui consulte quelle page ? Mais aussi qui partage quel article sur quel réseau social ? Et le fait-il via son *smartphone* ou non ? « Chartbeat se charge de retracer ce que les gens lisent sur quel site, article et page, pixel après pixel et seconde après seconde », promet l'entreprise sur son site. Plus de cinquante mille sites web dans plus de soixante pays recourent aux services de Chartbeat, ce qui représente au total cinquante milliards de visites de pages web tracées par mois.

Gigya promet quant à elle de transformer les visiteurs anonymes en clients connus. L'entreprise profite pleinement de la nonchalance dont nous faisons preuve. Selon elle, il n'est plus nécessaire de se cacher pour enregistrer notre comportement en ligne. Nous donnons avec désinvolture l'autorisation de partager les données nous concernant en échange d'un peu de confort. Gigya a développé un « *login* social », qui donne l'occasion aux utilisateurs de s'identifier sur un site web via Facebook, Google, Twitter, etc., ce qui leur évite de devoir créer un compte distinct pour chaque site. C'est bien pratique en effet, mais Gigya permet ainsi à une entreprise comme Mediaan, la société mère de VTM et QMusic, d'accéder très facilement à notre profil Facebook et aux données personnelles qui y sont liées, comme notre sexe, notre date d'anniversaire et nos centres d'intérêt. Parallèlement aux informations sur le comportement des visiteurs sur le site de VTM ou QMusic même, les entreprises peuvent établir des profils d'utilisateurs individuels et les tenir à jour en permanence. Lorsqu'un utilisateur met son profil Facebook à jour, il est adapté automatiquement dans le profil d'utilisateur de Gigya. Les données concernées sont nombreuses : elles vont de votre localité et de votre situation amoureuse aux « *likes* » que vous distribuez sur Facebook. En outre, dans cette base de profils d'utilisateurs, il est possible de lancer des recherches sur l'adresse *e-mail*, le nom, etc.

Gemius est une autre de ces entreprises qui combinent différentes sources d'information pour mieux comprendre le comportement des utilisateurs. Pour les internautes belges, cette entreprise d'origine polonaise revêt une grande importance, même si la plupart d'entre eux n'en ont encore jamais entendu parler. C'est qu'elle collabore avec le Centre d'Information sur les

Médias (CIM), qui collecte des données et les fournit au marché publicitaire belge. Tous les Belges connaissent, consciemment ou non, le CIM pour les chiffres d'audience télé et radio qu'il publie. Lorsque les journaux et autres médias ont développé leur présence en ligne et ont souhaité y faire de la publicité, le CIM a dû commencer à collecter aussi les chiffres de fréquentation des sites belges. Les annonceurs veulent des données fiables sur le nombre de visiteurs recensés sur un site et, plus que tout, ils veulent savoir qui sont ces visiteurs, pour pouvoir choisir quels messages publicitaires ils publient sur quels sites. Gemius effectue cette mesure d'audience en ligne pour le compte du CIM. L'entreprise s'est donné pour défi de mesurer et de savoir qui sont les gens derrière les *cookies*. Elle collabore avec des entreprises qui possèdent des données sur le comportement des spectateurs et des auditeurs pour pouvoir combiner les données en ligne avec les chiffres sur l'audience des télés, radios et autres médias, et analyser ainsi des « données multimédias ».

Ensuite, on trouve dans la liste le nom de Rubicon Project qui se présente comme le plus grand marché publicitaire du monde. Il s'agit d'un réseau publicitaire, le fameux intermédiaire entre l'annonceur et l'éditeur. Lorsqu'on surfe par exemple sur HLN.be, on sait par avance qu'on y verra des publicités. Mais on ignore lesquelles. Le choix de ces annonces se décide en quelques fractions de seconde. C'est tout ce qu'il faut à Rubicon Projet pour organiser une espèce de vente aux enchères en ligne. L'espace publicitaire est ainsi vendu à l'annonceur qui en offre le prix le plus élevé. Les offres comptabilisées sur ce marché dépendent entièrement de l'identité du visiteur. Rubicon Projet promet aux acheteurs d'espace publicitaire que leurs algorithmes pourront trouver les consommateurs qui « deviendront probablement leurs prochains clients ». Pour pouvoir relier les publicités aux personnes adéquates, Rubicon Projet doit bien entendu savoir qui sont ces personnes. C'est pourquoi l'entreprise collecte, sur les utilisateurs des sites qui recourent à ses services, des informations telles que l'historique du navigateur, la géolocalisation et les termes recherchés.

Alors que je pensais n'avoir visité que deux sites, j'ai donc établi à mon insu une connexion avec 105 autres sites web. Tous ces sites voulaient donc savoir que j'avais visité HLN.be et Nieuwsblad.be et sur quels éléments j'avais cliqué. Ces 105 entreprises ne sont pas les seules à vouloir en savoir plus sur moi et sur des millions d'autres internautes. Loin de là. Ce n'est que le sommet de l'iceberg.

Un appareil indispensable

Sur internet, nous ne nous limitons plus depuis longtemps à fréquenter les sites d'actualité. Il y a dès lors des centaines d'autres façons de suivre notre comportement en ligne. Sur un *laptop* ou un PC, on visite généralement les sites par le biais d'un navigateur. Mais avec l'arrivée du *smartphone* voici quelques années, notre consommation de l'internet est devenue de plus en plus mobile. Et ce nouveau mode de navigation est également scruté avec attention. Alors qu'il est rare que nous emportions notre *laptop* au magasin ou aux fêtes de famille, notre téléphone de poche ne nous quitte que rarement. Il offre dès lors aux entreprises de superbes possibilités de collecter des informations de meilleure qualité et plus détaillées sur notre vie.

Le *smartphone* est un appareil formidable, les Flamands de moins de soixante ans estiment même qu'il s'agit de la technologie la plus indispensable qui soit. Vingt-deux pour cent de tous les Néerlandais consultent même leur *smartphone* plus de cinquante fois par jour… Difficile, voire impossible de trouver un autre exemple de technologie qui se soit imposé aussi bien et aussi rapidement dans notre vie quotidienne. Bien que les premiers *smartphones* soient apparus sur le marché en 1999 et que le simple *GSM* était déjà bien implanté avant, le marché des téléphones mobiles intelligents n'a véritablement explosé qu'avec l'arrivée de l'iPhone en 2007. L'année suivante, le premier *smartphone* doté du système d'exploitation Android de Google fut lancé à son tour. Dix ans après l'introduction de l'iPhone, près de 80 pour cent de tous les Flamands possèdent un *smartphone*. Aux Pays-Bas, 88 pour cent des internautes surfent surtout depuis un appareil mobile. Adam Greenfield, auteur influent et ancien designer chez Nokia, dit du *smartphone* qu'il est l'« artefact le plus caractéristique de notre époque ». Comme l'écrit Greenfield, on a oublié depuis longtemps combien de choses le *smartphone* a remplacées. Alors que nos portefeuilles et sacs à main regorgeaient d'argent, de photos de famille et d'une multitude de cartes d'identité, de banque et de fidélité, aux côtés d'un *walkman* ou d'un lecteur MP3, toutes ces fonctions et bien d'autres encore ont été remplacées par un seul appareil qui détermine dans une grande mesure la manière dont nous

interagissons avec le monde et les gens qui le peuplent. Chaque jour, nous utilisons une appli de messagerie, plusieurs applis de réseaux sociaux, des applis qui nous permettent de visionner des films ou d'écouter de la musique, d'acheter des objets neufs ou de seconde main, des applis avec lesquelles nous vérifions l'état de notre compte en banque, des applis qui nous permettent de trouver notre chemin ou de consulter la météo, qui surveillent notre santé et notre forme, qui nous permettent de commander du *fast-food*, de chercher un emploi ou l'âme sœur… Pour toutes les fonctions possibles et imaginables, il existe l'une ou l'autre appli. Nous divulguons ainsi une énorme quantité d'informations sur notre comportement, nos habitudes et nos centres d'intérêt. Le *smartphone* est donc une mine d'or en puissance.

Tracé dans la vie réelle

Le soir après le travail, vous faites un saut chez Delhaize pour acheter en passant les ingrédients de votre repas du soir. Dans le train, vous aviez recherché en vitesse une recette via votre *smartphone*, et à présent, il vous faut les bons ingrédients. Vous vérifiez rapidement sur votre *smartphone* ce dont vous avez besoin et à ce moment précis, une notification apparaît sur votre écran : Delhaize vous annonce qu'aujourd'hui, vous bénéficiez en exclusivité d'une réduction de vingt pour cent sur le hachis de bœuf et qu'à l'achat d'un paquet de spaghettis, le second est gratuit. D'un seul clic, vous obtenez un code de réduction qu'il vous suffira de faire scanner à la caisse. Vous laisseriez-vous tenter ?

Sam Amrani pense que oui. Cet entrepreneur britannique de 28 ans a introduit dans la vie réelle ce qui, en ligne, est la norme depuis des années : le traçage. À cette fin, sa petite entreprise Tamoco utilise la technologie qui nous est apparemment la plus indispensable : notre *smartphone*. L'idée lui est venue lorsqu'il travaillait pour Orange. Lorsqu'il proposa au géant de la téléphonie de tirer profit des données de localisation qu'il récoltait sur ses clients, l'entreprise n'y donna toutefois aucune suite. Amrani et son associé Daniel Angel décidèrent alors en 2012 de se lancer eux-mêmes dans l'exploitation

de cette mine d'or. Après quelques essais avec des codes QR, ils trouvèrent en 2016 la formule magique idéale : un vaste réseau de capteurs capables d'enregistrer les signaux des *smartphones*, notamment les réseaux *Wi-Fi* publics d'enseignes « horeca » telles que Starbucks. Cette entreprise dispose de plus d'un milliard de ces « capteurs de proximité » qui, outre le signal *Wi-Fi*, peuvent reconnaître et capter des signaux *Bluetooth* ou *GPS*, ainsi que des informations sur le type de smartphone utilisé ou son niveau de charge. En recoupant toutes ces données, Tamoco peut déterminer au mètre près la position d'une personne dans la vie réelle. L'entreprise a accès aux déplacements de cent millions de propriétaires de *smartphones* dans le monde. Comment Tamoco y parvient-elle ? Tout simplement : grâce aux applis de votre téléphone. Tamoco a conclu des contrats avec un bon millier de développeurs d'applis. Généralement, ce sont des applis qui ont de nombreux utilisateurs mais qui génèrent peu d'argent. Lorsque vous installez l'une de ces applis et que vous approuvez ses conditions d'utilisation, vous l'autorisez aussi à enregistrer des informations de localisation via le réseau de capteurs de Tamoco. Cette dernière vend ensuite ces données aux annonceurs, et les applis touchent une partie du bénéfice. Lorsque vous franchissez ensuite le seuil d'un magasin de meubles, les applis du réseau de Tamoco envoient sur votre téléphone des publicités ou des promotions émanant de ce magasin. Du moins si vous y avez passé plus de cinq minutes… C'est apparemment le temps dont Tamoco a besoin pour connaître votre position exacte. Tamoco a déjà travaillé avec Unilever pour la mise en place d'une boutique éphémère pour les glaces Magnum. Si l'un des cent millions de *smartphones* auxquels Tamoco a accès, a visité cette boutique, il montrera ensuite une publicité pour Magnum. Cette technologie permet aussi à Tamoco d'adresser aux utilisateurs le bon message au bon moment, pour une promotion en cours au supermarché de leur quartier, par exemple.

Amrani et son équipe capitalisent ainsi sur notre manque de temps. Car qui lit toutes les conditions d'utilisation des applis qu'il installe ? On n'aurait plus le temps de faire grand-chose d'autre. Mais lorsqu'on télécharge l'une de ces applis, on donne toujours une série d'autorisations au développeur. Un planificateur d'itinéraire vous demandera

logiquement de pouvoir utiliser vos données de localisation. Mais de nombreuses applis demandent toute une série d'autorisations dont l'utilité n'est pas toujours évidente : comme un planificateur d'itinéraire qui demande à pouvoir accéder à vos photos, ou l'un ou l'autre jeu qui souhaite connaître votre position GPS… Il s'agit généralement d'applis avec des publicités. Ici aussi, les entreprises tentent de collecter le plus de données possible sur leurs utilisateurs. Amrani et son équipe l'ont bien compris. En téléchargeant l'une de leurs applis partenaires, l'utilisateur leur offre ses données de localisation sur un plateau. Amrani et un très grand nombre d'autres développeurs et entreprises ont bien compris les possibilités qu'offre notre utilisation du *smartphone*. Nous sommes notre *smartphone*. Quand on connaît le *smartphone*, on connaît la personne qui se cache derrière.

On est suivi et surveillé lorsqu'on surfe sur internet via son *laptop* ou PC. Et avec l'arrivée du *smartphone*, cette surveillance en ligne est passée à la vitesse supérieure. Autrefois, lorsque nous sortions, nous laissions notre *laptop* à la maison, mais aujourd'hui, nous sommes accros à un appareil équipé d'une multitude de capteurs précis capables de nous suivre et de nous surveiller jusque dans le monde physique. Bien que l'appareil capte de nombreux signaux et est capable de collecter des informations, il y en a de nombreuses autres qui lui échappent. Le moment où nous lançons le lave-vaisselle, par exemple, ou la température à laquelle notre chauffage est réglé, le niveau de remplissage de notre réfrigérateur… Ce sont pourtant des informations qui seraient très utiles à toute une série d'entreprises. Pourquoi dès lors ne pas rendre tous les appareils électroniques aussi intelligents que notre téléphone ? Chaque objet utilitaire représenterait ainsi un nouveau moyen de collecter des informations sur notre vie. Or, c'est exactement ce vers quoi nous nous dirigeons avec le concept de l'Internet des objets (IoT – *Internet of Things*).

Votre maison est en ligne

Voilà deux années consécutives qu'Amazon Echo, qui n'est pas beaucoup plus qu'un haut-parleur avec un microphone, figure parmi

les cadeaux de Noël les plus populaires aux États-Unis et ailleurs. Amazon refuse de divulguer des chiffres exacts mais, fin 2017, l'entreprise annonçait fièrement que des millions de nouveaux appareils avaient été vendus, tout comme l'année précédente. Le haut-parleur se décline en divers formats, et certains modèles étaient en rupture de stock. Avec une part estimée à septante pour cent, Amazon domine le marché et laisse son principal concurrent, Google Home, loin derrière lui. Depuis l'arrivée du *smartphone*, aucun gadget technologique n'avait été aussi populaire.

Les haut-parleurs intelligents, comme ceux d'Amazon et de Google, sont appelés à devenir le point central de la maison intelligente de l'avenir. Une maison intelligente sait ce que ses habitants veulent et leur obéit au doigt et à l'œil. Vous voulez commander une pizza ? Demandez-le à Alexa, l'assistante virtuelle intégrée d'Amazon Echo, qui se charge de vous la faire livrer. Vous souhaitez prendre un bain bien chaud sur fond de musique relaxante ? Alexa diffuse les airs les plus doux. Elle vous fait même la lecture si vous le voulez. Alexa répond à vos questions, cherche des recettes et actionne une minuterie pour la cuisson de vos spaghettis. Elle vous commande un taxi et peut allumer et éteindre vos luminaires intelligents, ou régler votre thermostat intelligent. Elle retrouve votre téléphone si vous l'avez égaré. Elle raconte même des blagues. Et bien entendu, elle vous permet de faire vos emplettes dans le *webshop* d'Amazon. Pour commander l'engin, pas besoin de tourner des boutons ni de glisser votre doigt sur l'un ou l'autre écran tactile. Vous n'avez même pas besoin de vous déplacer puisque le son de votre voix suffit. Amazon Echo est activé lorsque vous prononcez le nom d'« Alexa ». En principe donc, l'appareil est toujours allumé puisqu'il doit pouvoir entendre quand quelqu'un prononce ce nom. Et ce quelqu'un peut vraiment être n'importe qui. Une famille texane a pu le constater à ses dépens le jour où une maison de poupée de 170 dollars lui fut livrée. La fillette de la maison, six ans, avait trouvé Alexa tellement amusante qu'elle lui avait demandé une maison de poupée pour y jouer avec elle. Lorsque la mère reçut le mail de confirmation de la commande, elle sut aussitôt ce qui l'attendait. Un peu plus tard, une luxueuse maison de poupée trônait au salon, à côté d'un paquet de biscuits. L'histoire ne s'arrêta pas là car la télévision locale décida d'y consacrer

un sujet. Et lorsque le journaliste prononça à l'antenne les mots « Alexa commanda une maison de poupée », plusieurs téléspectateurs constatèrent que leur propre Alexa voulait faire de même. Ils ont toutefois pu annuler la commande à temps.

Intelligent mais dangereux

Amazon Echo est à ce jour l'exemple le plus connu d'un appareil intelligent relié à l'internet. Mais de très nombreuses entreprises ont l'ambition de rendre leurs produits intelligents. Le fabricant néerlandais de lampes Philips a ainsi développé Hue, un éclairage intelligent. Hue est compatible avec Amazon Echo, notamment, et il peut être commandé par la voix, mais tout aussi bien à distance, par *smartphone* interposé. On peut également programmer Hue de manière à ce qu'il s'allume automatiquement à des moments déterminés, dans plus de cinquante mille nuances de blanc, par exemple pour vous réveiller à 6h30 en diffusant une lumière chaude. Les modèles les plus coûteux peuvent même être synchronisés avec les films que l'on visionne sur un téléviseur intelligent, de sorte que la lumière s'adapte aux couleurs du téléviseur. Et lorsque vous installez l'appli correspondante sur votre *smartphone*, vous pouvez programmer Hue de sorte que la lumière s'allume lorsque vous arrivez sur le chemin de votre maison, ou qu'elle s'éteigne lorsque vous tirez la porte d'entrée derrière vous. Mais pour cela, il faut que l'appli ait accès à votre position géographique.

Le fabricant de jouets américain Spiral Toys, basé en Californie, a eu l'idée lumineuse de lancer des nounours « intelligents » sur le marché. Des peluches reliées à l'internet, donc. Ainsi, lorsque maman est en voyage d'affaires, ou papa en week-end avec des copains, ils peuvent envoyer un gentil message ou une berceuse à leurs chères têtes blondes. La peluche diffuse alors le message, et pour l'enfant, c'est comme si papa et maman étaient près de lui. Plus de huit cent mille pères et mères ont acheté le nounours en question, mais ils s'en sont mordu les doigts. Non pas parce que leur berceuse ou leurs paroles réconfortantes n'auraient pas atteint leurs enfants, mais parce que Spiral Toys a laissé traîner sur internet, sans la moindre sécurisation, les données

liées à leur compte ainsi que des millions de messages enregistrés : huit cent mille adresses *e-mail* et les mots de passe correspondants, au vu et au su de tout le monde. Plus de deux millions de messages personnels dans une base de données en ligne à peine sécurisée. Un défaut que les parents n'avaient sans doute pas prévu…

Et ce n'est pas le seul exemple d'appareil connecté qui présente un niveau de sécurité défaillant, loin de là. L'ours en peluche intelligent mis sur le marché par Fisher-Price est également affublé d'une erreur de logiciel. Cette erreur a permis à des pirates de se constituer une base avec les données personnelles de tous les enfants qui jouaient avec la peluche. Une Barbie intelligente qui réagit à ce que lui disent les enfants s'est également révélée technologiquement vulnérable. Des chercheurs en matière de sécurité avaient réussi à transformer la poupée en un appareil d'espionnage. Les micros intégrés pouvaient être détournés à distance pour servir d'appareils d'écoute.

Et ce n'est pas tout. En 2016, plusieurs appareils intelligents ont paralysé temporairement le réseau social Twitter et le service de streaming musical Spotify, entre autres sites. Bien entendu, ils ne l'ont pas fait de leur propre initiative. Ils avaient été intégrés par des pirates informatiques dans ce qu'on appelle un « *botnet* », une armée d'appareils reliés à l'internet, en l'occurrence des caméras de sécurité mal sécurisées. Les appareils infectés ont été utilisés par un pirate mal intentionné pour attaquer Dyn, une entreprise qui fournit des services de support à plusieurs grandes sociétés internet. L'attaque, au cours de laquelle seulement dix pour cent environ des appareils infectés avaient réellement été utilisés, a pourtant paralysé longtemps de grandes parties d'internet.

Amazon Echo n'est pas à l'abri d'un déraillement. « Éteignez tous vos appareils Alexa, maintenant ! » Tel est le message qu'une utilisatrice américaine reçut de l'un des collègues de son époux. C'est que ce collègue avait capté des messages personnels enregistrés par Alexa. Amazon confirme l'histoire mais n'a pas expliqué pourquoi Alexa avait fait ces enregistrements et les avait transmis. Le porte-parole de l'entreprise s'est contenté de trouver l'incident « très étrange », mais il a précisé que l'appareil avait sans doute été activé parce qu'il avait capté un mot ressemblant à « Alexa ». Ensuite, il aurait sans doute capté au cours de la conversation une expression ressemblant à

« *send to* » suivie d'un mot ressemblant au nom du collègue en question. Amazon s'en tient donc à un défaut et ne considère pas l'incident comme la preuve qu'Alexa reste continuellement à l'écoute. Le client a toutefois décidé de se défaire de tous ses appareils Alexa.

Tout en ligne

Tous ces exemples en disent long sur les faiblesses, mais aussi sur les possibilités des appareils connectés intelligents. Or, l'internet des objets repose justement sur le projet de rendre tous les appareils intelligents et connectés. Pour pouvoir être intelligents, ces appareils doivent être alimentés avec des informations concernant les utilisateurs et leur environnement. Ainsi, l'éclairage intelligent de Philips doit toujours savoir où nous sommes pour pouvoir allumer la lumière automatiquement lorsque nous rentrons chez nous.

L'afflux d'informations permet aux appareils de fournir un service de meilleure qualité et taillé sur mesure. Pour Dave Limp, responsable du développement de produits chez Amazon, Alexa et Echo sont une forme d'informatique ambiante (*ambient computing* en anglais). Contrairement au PC ou au *smartphone*, ce haut-parleur intelligent est moins relié à une personne en particulier, mais il est encore plus omniprésent, du moins si l'on reste à portée de voix.

D'autres appareils intelligents veulent vous talonner d'encore plus près. Les technologies portables comme les montres intelligentes ou les *fitness trackers* entendent rester à votre poignet 24h/7j pour mesurer ce que vous faites. Ces appareils sont de plus en plus performants, grâce à des capteurs qui enregistrent avec grande précision des données qui peuvent aussi servir dans un contexte médical, dans le cas de patients cardiaques, par exemple.

Les entreprises belges ne sont pas en reste. Bloomlife produit par exemple un petit dispositif que les femmes enceintes peuvent se coller sur le ventre pour mesurer et suivre les contractions via leur *smartphone*. Le géant technologique Apple, lui aussi convaincu de l'intérêt de cette évolution, se lance à son tour sur le marché des données médicales ; non par le biais d'un nouvel appareil, mais au moyen de l'iPhone et de l'Apple Watch. L'entreprise a lancé récemment une

mise à jour de l'appli de santé installée de série sur l'iPhone. Elle s'est associée à plusieurs hôpitaux américains pour permettre aux patients de télécharger et de consulter leur dossier médical complet grâce à cette appli. L'iPhone est déjà pourvu de plusieurs capteurs qui collectent des données précieuses et pertinentes sur le plan médical. Et l'entreprise entend bientôt en ajouter plusieurs autres pour pouvoir enregistrer un nombre encore plus grand d'informations. D'autres entreprises peuvent ensuite développer des applications qui utilisent les données collectées par ces capteurs.

La société belge FibriCheck le fait déjà pour détecter les troubles du rythme cardiaque. Il suffit que l'utilisateur pose son doigt sur la caméra pour mesurer son rythme cardiaque. Les résultats sont transmis automatiquement au médecin qui peut aussitôt les évaluer et, le cas échéant, intervenir. FamilyEye, une autre start-up belge, a développé une espèce de caméra intelligente équipée de capteurs à l'intention des personnes âgées. Ce dispositif est installé au domicile de ces personnes et les filme 24h/7j. FamilyEye est capable de détecter une chute et d'alerter aussitôt les secours, mais peut également être utilisé pour vérifier préventivement à distance si tout va bien chez la personne. C'est une solution bien pratique pour les enfants et petits-enfants qui ne peuvent pas assurer une présence constante auprès de leurs parents ou grands-parents âgés.

Mais une application très utile dans un contexte peut revêtir une tout autre signification dans un contexte différent, comme on a pu le constater en Russie… La *start-up* russe NTechLab a lancé en 2016 une appli que tout le monde pouvait utiliser pour photographier le visage d'un inconnu. La photo pouvait ensuite être reliée automatiquement au profil de cette personne sur VKontakte, l'équivalent russe de Facebook. Or cette appli conçue comme un gadget anodin a pris entre-temps des proportions pour le moins inquiétantes. La technologie sophistiquée de reconnaissance faciale de NTechLab – devenue depuis lors *leader* mondial en la matière – est intégrée depuis la fin 2017 sur tout le réseau de caméras de surveillance moscovite.

Boîte noire

Les données médicales et comportementales collectées par l'intermédiaire des montres intelligentes et autres *tracking devices* intéressent aussi très fort le secteur des assurances, qui collecte et stocke depuis des décennies des *big data*, telles que des données historiques sur les moments et les lieux où se produisent des accidents. Les assureurs utilisent ces informations pour évaluer le risque d'incendie et, partant, pour fixer le montant des primes. Les assureurs utilisent aussi des *open data*, des données librement disponibles, par exemple concernant la criminalité dans certains quartiers. Au cours des dernières années, leurs sources ont été diversifiées par l'arrivée des données en ligne. Les *tracking devices* personnels, comme les montres intelligentes, présentent un intérêt tout particulier. L'assureur belge AG Insurance a déjà expérimenté avec ce qu'on appelle la télémesure (*telemetrics* en anglais), une espèce de boîte noire pour voiture qui enregistre votre vitesse, la brutalité avec laquelle vous freinez, où et quand vous roulez. On n'en est pas encore là, mais imaginez qu'un assureur vous propose d'installer contre une réduction de tarif un tel dispositif de traçage dans votre voiture : cet appareil enregistrera alors en permanence votre comportement de conduite et de déplacement, ces données seront ensuite stockées et analysées.

Avec l'internet des objets, tous nos appareils et équipements deviennent intelligents. Ils sont reliés en permanence avec l'internet et entre eux, et forment ainsi un réseau intelligent censé être à notre service. Ils sont intelligents parce qu'ils sont capables, en fonction des informations qu'ils collectent, de prendre des initiatives. Pensez à un luminaire intelligent qui s'allume lorsque la nuit tombe, ou lorsqu'il reçoit un signal émis par notre *smartphone* qui lui indique que vous êtes presque arrivé chez vous après votre journée de travail. Les appareils intelligents doivent rendre notre vie plus facile, plus efficace et meilleure. Mais pour y parvenir, ils doivent collecter encore plus d'informations, davantage encore que celles rassemblées par notre *smartphone*, ou davantage que celles que nous divulguons par le biais de notre *laptop*. Les solutions que ces appareils intelligents nous

offrent pour résoudre les problèmes de tous les jours doivent être instantanées, et donc la collecte et le traitement des données doivent également se faire en temps réel. Ici et maintenant. Nombre de ces techniques sont introduites très rapidement et s'imposent tout aussi vite dans notre maison ou autour de notre poignet. Mais une fois de plus, l'histoire ne s'arrête pas là. Les appareils ne vous surveillent pas seulement dans votre maison et autour d'elle, puisque même lorsque vous sortez, vous êtes suivi. Bienvenue dans la ville intelligente…

La ville qui entend tout, qui voit tout

Nous avions déjà le PC qui suit nos faits et gestes, le *smartphone* qui sait où nous nous trouvons, avec qui nous parlons, quand nous nous levons et nous couchons, et la maison pleine d'appareils intelligents qui savent tout que nous disons et voient tout que nous faisons. La dernière couche qui s'ajoute à présent à ce système de collecte d'informations est la ville intelligente, soit la Cité des objets connectés, une autre composante de l'internet des objets.

Cette ville de l'avenir promet donc d'être plus intelligente en résolvant les problèmes de la façon la plus efficace possible grâce à la technologie. Les problèmes de mobilité figurent parmi les principaux défis qu'il sera possible de résoudre grâce à des technologies intelligentes. Ce ne sont pas les exemples et les idées qui manquent : des voitures qui seront envoyées automatiquement vers le parking offrant le plus grand nombre de places libres, une appli qui indique aux cyclistes le parcours le moins fréquenté ou des feux de circulation intelligents qui restent plus longtemps au vert pour un groupe d'écoliers.

Mais les développeurs et décideurs envisagent également de recourir à des technologies intelligentes pour résoudre d'autres types de problèmes. Des poubelles sont équipées de capteurs qui émettent un signal lorsqu'elles sont presque pleines afin que les éboueurs puissent déterminer le parcours de ramassage le plus efficace. Aux Pays-Bas notamment, des lampadaires de rue intelligents, équipés de capteurs qui règlent l'intensité lumineuse selon ce qui se passe dans leur environnement, ont déjà fait leur apparition à plusieurs endroits. Grâce à un vaste réseau de caméras et de capteurs intelligents, la ville intelligente

peut aussitôt évaluer la fréquentation dans les rues et, le cas échéant, diriger la foule dans la bonne direction.

Dans chacun de ces exemples, on voit qu'il convient d'abord d'établir la cartographie du problème avant que la ville intelligente puisse proposer des solutions. Or, cette cartographie repose sur la collecte d'une grande quantité et variété de données différentes : via des caméras intelligentes capables de reconnaître des visages et des plaques de voitures, des caméras à infrarouge qui mesurent la température ou des capteurs qui enregistrent les signaux Wi-Fi et Bluetooth des *smartphones* pour mesurer l'intensité du trafic… Dans la ville intelligente, les murs ont des capteurs, impossible d'y échapper. On peut certes être prévenu qu'on est filmé ou que nos données sont collectées d'une manière ou d'une autre, mais lorsqu'il y a des caméras à chaque coin de rue, on ne peut pas échapper à cette collecte de données.

Ainsi n'est-il pratiquement plus possible de circuler dans la ville incognito. En 2017, le « *stadsdichter* » anversois (poète officiel de la ville) Maarten Inghels a tenté d'évoquer ce problème de façon poétique avec son projet « *The Invisible Route* ». L'administration de la métropole anversoise possède quelque trois cents caméras dispersées dans toute la ville, mais certains commerçants et citoyens inquiets ont également équipé leurs façades de caméras de surveillance. Une liste publique de caméras à la main, Inghels est parti sillonner la ville pour dresser l'inventaire des caméras privées. Après plusieurs mois de recherche sur le terrain, il a réussi à tracer un parcours d'environ dix kilomètres : du nord d'Anvers jusqu'au musée du Middelheim dans le sud de la ville, en parcourant le centre dans tous les sens. Une ode à l'invisibilité donc, comme il a lui-même appelé son projet. Même s'il n'a bien entendu tenu compte que des caméras que l'on peut effectivement distinguer. Mais à l'ère du *smartphone*, pas besoin de caméra pour savoir où nous sommes.

Si vous êtes en route, vous êtes vu

Les villes ne sont cependant pas seules à souhaiter savoir ce qui se passe sur leur territoire, loin de là. Fin 2016, le gouvernement

belge a décidé de déployer un véritable bouclier de caméras ANPR (*Automatic Number-Plate Recognition*) intelligentes sur l'ensemble du territoire. Cette reconnaissance minéralogique était censée améliorer la sécurité routière, mais pourrait également servir dans la lutte contre le crime organisé et les groupements terroristes.

Or Kristof Clerix, journaliste d'investigation chez *Knack*, a découvert un détail dont le gouvernement a omis d'informer le grand public : ces caméras prennent d'ores et déjà des images haute définition de la voiture tout entière, y compris donc de ses occupants. De plus, le gouvernement a demandé aux producteurs de prévoir la possibilité d'y intégrer la reconnaissance faciale. Cela signifie que les images enregistrées peuvent être reliées à une base de données rassemblant par exemple des photos d'identité. À terme, le bouclier de caméras sera donc capable de reconnaître les conducteurs et les passagers. Si cette possibilité n'est pas encore active aujourd'hui, le gouvernement n'en met pas moins les producteurs au défi de s'y atteler. Un exemple typique de ce qu'on n'appelle dans le jargon un détournement d'usage (*function creep*, en anglais). Une application intelligente introduite aujourd'hui pour effectuer une tâche déterminée pourra peut-être servir demain à des fins totalement différentes. C'est la pente glissante de la ville intelligente.

Les autorités publiques montrent donc un grand intérêt pour les caméras et technologies intelligentes, mais elles ne sont pas les seules : certaines entreprises privées équipent également la ville et l'espace public avec ce type de technologie. Ainsi, une enquête menée par le quotidien *De Morgen* a-t-elle révélé que JCDecaux, leader mondial du « mobilier urbain porteur de publicité » a installé dans des centres commerciaux belges des panneaux publicitaires équipés de caméras qui filment les passants. Ces « capteurs visuels » comptent le nombre de personnes qui regardent la publicité. Le logiciel permet en outre de déduire, sur la base des expressions faciales, le sexe et même l'âge des personnes concernées.

La collecte des données est de toute évidence le mot-clé de la ville intelligente du futur. L'introduction de données historiques et en temps réel est présentée comme inévitable si on veut résoudre les problèmes rapidement et efficacement. La collecte des données, et ensuite leur analyse, sont censées rendre la ville plus sûre, moins polluante et

plus agréable à vivre. C'est du moins l'argument présenté en Flandre pour miser sur les villes intelligentes, qui collectent et analysent les informations à grande échelle. Dans notre pays, la ville intelligente n'en est qu'à ses balbutiements. Mais les décideurs entendent faire de chaque lampadaire de rue, de chaque poubelle et de chaque feu de circulation un collecteur de données intelligent. À Anvers, cette ambition prend déjà forme.