Reporterre
le quotidien de l'écologie

A Rennes, des capteurs wifi devaient espionner les passants

15 mars 2017 / Julie Lallouët-Geffroy (Reporterre)

À Rennes, des commerces voulaient mi-février cartographier les déplacements de leurs clients en surveillant les signaux wifi de leur téléphone. La mobilisation de militants des libertés publiques a empêché la mise en place de ce dispositif, mais la pression est forte partout pour capter les données personnelles sans avertir les personnes surveillées.

- *Rennes (correspondance)*

Soucieuse d'enrayer la désertification du centre-ville de Rennes, l'association de commerçants le Carré rennais voulait mettre en place des capteurs des signaux wifi des téléphones pour connaître les déplacements de leurs clients dans leur boutique. Trente boutiques comptaient participer à l'expérience. Il s'agissait d'assurer un maillage du centre-ville pour connaître les habitudes des consommateurs et en tirer des moyens de dynamiser le quartier.

L'annonce de la mise en place du dispositif à la mi-février a inquiété les militants de la protection des données personnelles, qui ont réagi sur les réseaux sociaux et attiré l'attention des élus locaux et de la Cnil, la Commission nationale de l'informatique et des libertés, garante du respect de la loi Informatique et liberté de 1978.

Voyant le tollé venir, le Carré rennais a décidé de jouer la prudence en ne se contentant pas de la déclaration exigée par la Cnil pour installer ces boîtiers, et en demandant une autorisation afin de prouver que l'anonymisation des données personnelles est bien respectée. À l'heure actuelle, la Cnil n'a pas encore rendu son avis.

Au sein même de l'association des commerçants, ces capteurs ne font pas consensus. Son président, Dominique Fredj, a démissionné, mercredi 15 mars, à cause de ce projet. Selon *Ouest-France*, il justifie sa décision en accusant des membres du Carré rennais : *« Ils veulent mettre en place des systèmes de* "tracing" *de nos clients, qui détruiront la relation de confiance qui unit nos commerces de proximité de centre-ville et nos clients et visiteurs. »*

« En tant qu'élu, j'ai pour rôle de protéger mes concitoyens »

Lunar fait partie des militants qui sont montés au créneau. Programmeur de logiciels libres, impliqué dans la conception de logiciels permettant de protéger la vie privée des internautes (comme Tor), il déplore que, aujourd'hui, *« on mette en place des systèmes pour aspirer des données personnelles sans s'interroger sur leurs conséquences et implications. Il n'y a pas de débat public sur le sujet »*

.

Le centre-ville de Rennes.

Laurent Hamon, conseiller municipal EELV aux usages du numérique, enchérit : « *En tant qu'élu, j'ai pour rôle de protéger mes concitoyens. Je ne doute pas de la bonne foi du Carré rennais, mais il faut que ce type de capteurs soit encadré et c'est difficile, car les technologies avancent beaucoup plus vite que la législation.* »

Lunar enfonce le clou en rappelant que *« lorsque l'on met en place un dispositif pour collecter des données, il est rarement retiré par la suite, au contraire, il s'étend »*. Exemple à l'appui : le fichier national automatisé des empreintes génétiques. Créé en 1998, il devait uniquement recenser les personnes condamnées pour des faits de nature sexuelle, mais, en 2003, il a été élargi aux infractions. Résultat : aujourd'hui 1 Français sur 6 serait dans ce fichier, selon un article publié par *Slate*.

« Avec ces dispositifs, où est le consentement ? »

Dès qu'il s'agit de constituer un fichier d'informations, empreintes, signaux wifi ou autres, la Cnil a son mot à dire. Cinq principes régissent ses décisions, au premier desquels la finalité de la collecte de données. La Cnil a la tâche difficile d'assurer l'équilibre entre la liberté des entreprises d'utiliser les nouvelles technologies et de garantir la liberté des personnes de ne pas voir aspirées leurs données personnelles.

Lunar: « Lorsque l'on met en place un dispositif pour collecter des données, il est rarement retiré par la suite, au contraire, il s'étend. »

Laurent Hamon, l'élu municipal rennais, s'inquiète particulièrement de la marge de manœuvre octroyée au citoyen : *« Avec ces dispositifs, où est le consentement ? À quel moment est-il demandé explicitement ? »* Ce type de débat avait eu lieu en 2009, pour que l'internaute coche, ou pas, les cases *« je souhaite recevoir la newsletter de… »*, *« je souhaite recevoir les offres des partenaires de… »* ; un moyen d'obtenir un consentement explicite.

La Cnil n'hésite pas à se positionner sur le sujet, comme le mois dernier, en sanctionnant des sites de rencontres qui utilisaient, sans leur accord, les informations fournies par leurs

clients. L’enjeu actuel est de trouver le meilleur moyen, le moins contraignant, pour obtenir un consentement équivalent à l’échelle d’une ville, d’un festival, d’un magasin… Un casse-tête.

> « C’est à la législation de limiter les entreprises dans leur utilisation des technologies, au nom de l’intérêt général »

Le consentement, qu’on pourrait aussi appeler la dent creuse de la loi informatique et libertés de 1978, est peu présent dans les dispositifs que proposent les start-ups, où seule la promesse d’une étude fine des comportements est brandie ; la collecte de données étant devenue le nouvel eldorado économique.

Pour se prémunir des aspirateurs à données qui se développent un peu partout en France, à Rennes, mais aussi dans des centres commerciaux, le meilleur moyen est d’éteindre l’option wifi de son téléphone ou de renoncer à ce type de téléphonie. *« Mais dans ce cas, on renverse le raisonnement,* explique Laurent Hamon, *ce n’est pas au citoyen de se priver de technologie pour se protéger, c’est à la législation de limiter les entreprises dans leur utilisation des technologies, au nom de l’intérêt général. »*

Laurent Hamon : « Il faut que ce type de capteurs soit encadré et c'est difficile, car les technologies avancent beaucoup plus vite que la législation. »

L'enjeu est d'autant plus important que ces informations pourraient être détournées de leur finalité première. Par exemple, en croisant les relevés du parking d'un hôpital et ceux de votre carte de crédit, on peut déduire si vous êtes atteint d'une longue maladie ou plutôt casse-cou, de quoi refroidir un banquier qui s'apprête à vous octroyer un prêt bancaire. Cet exemple n'est que pure extrapolation dans la mesure où la loi interdit formellement d'opérer de tels recoupements ; néanmoins, certaines affaires démontrent que le suivi d'une personne par ses traces numériques peut avoir des conséquences fâcheuses.

Un enjeu primordial pour la Cnil

C'est ainsi que Lunar évoque le cas d'un Marseillais d'une quarantaine d'années assigné à résidence fin 2015, car suspecté de vouloir empoisonner l'eau potable. Cette décision a résulté d'une mauvaise interprétation des données récoltées. Cet homme était

en arrêt de travail lié à une exposition aux produits chimiques lorsqu'il travaillait dans une station d'épuration. Il se renseignait donc sur ces produits et leurs conséquences sur internet, et s'était rendu sur son ancien lieu de travail.

C'est pour cette raison que l'anonymisation des données, l'effacement du lien entre un téléphone et un individu, est un enjeu primordial pour la Cnil. Le publicitaire JCDecaux s'y est cassé les dents avec les capteurs qu'il voulait mettre en place dans le quartier de la Défense, à Paris. Le Conseil d'État a confirmé mi-février le refus de la Cnil d'autoriser ce système. La CNIL jugeait qu'il ne s'agissait pas d'anonymisation des données, mais de « pseudonymisation », une anonymisation bancale. Les règles établies par la Cnil sont claires sur le sujet, mais sans cesse interrogées au vu des innovations technologiques.

Lire aussi : Le techno-totalitarisme, c'est maintenant

Source : Julie Lallouët-Geffroy pour *Reporterre*

Photos : © Julie Lallouët-Geffroy/*Reporterre* sauf :
. chapô : Flickr (Nicolas Nova/CC BY 2.0)