Le traçage cyberphysique des personnes et la vie privée

Mathieu Cunche

Le traçage cyberphysique des personnes et la vie privée

Par **Mathieu CUNCHE**
Maître de conférences à l'INSA-Lyon

Depuis l'apparition de l'iPhone en 2007, une grande partie de la population porte en permanence sur elle un « ordiphone », qui a été récemment rejoint dans notre sphère physique personnelle par d'autres appareils connectés (écouteurs, bracelets, capteurs de sport ou de santé, etc.). Ces appareils ont en commun d'inclure une ou plusieurs technologies sans-fil : Wi-Fi, Bluetooth et sa variante basse consommation, le Bluetooth Low Energy (BLE).

Depuis le début des années 2010, on a vu apparaître des systèmes traçant les utilisateurs dans le monde physique *via* la collecte des signaux radio émis par ces appareils sans-fil compagnons. Initié aux États-Unis par l'entreprise Euclid Analytics [(1)], le concept de traçage cyberphysique s'est rapidement développé au point de déclencher des réactions des autorités de contrôle, du législateur et des fabricants d'appareils.

Ce traçage cyberphysique, souvent pratiqué à l'insu des individus concernés, est particulièrement intrusif, et est une menace évidente pour la vie privée. Cette problématique de protection des données personnelles peut être abordée suivant deux axes : premièrement, une approche légale et réglementaire, avec une évolution des règles pour encadrer ces nouvelles techniques de collecte de données personnelles ; et deuxièmement, une approche technologique, avec une réflexion sur l'évolution des standards et la mise en œuvre de contre-mesures.

Traçage cyberphysique : fonctionnement et applications

Le traçage cyberphysique tel qu'on l'entend ici repose sur les technologies sans-fil (Wi-Fi et Bluetooth) intégrées dans nos appareils portables (ordiphones, bracelets connectés, écouteurs, etc.). Ces appareils se comportent comme des balises radio en émettant régulièrement des courts messages qui contiennent un identifiant unique et propre à chaque appareil (on parle d'adresse MAC). Cette diffusion de message est continue, et est présente même quand l'appareil n'est pas connecté ; en effet, l'émission de ces messages fait partie d'un mécanisme qui permet à notre appareil de découvrir les réseaux ou équipements à portée, auxquels il pourrait éventuellement se connecter.

Ces messages de découverte sont émis en clair (*i.e.,* non protégés par un chiffrement), et leur contenu, en particulier l'identifiant propre à l'appareil, peut être capté à distance (parfois à plusieurs dizaines de mètres) par un appareil dédié appelé *sniffer.* En collectant les signaux émis par nos appareils, ces *sniffers* sont en mesure de détecter la présence de personnes et de suivre leurs déplacements (voir Figure 1).

(1) https://archive.thinkprogress.org/meet-the-real-life-tracking-database-that-could-include-you-ddba626eb210/

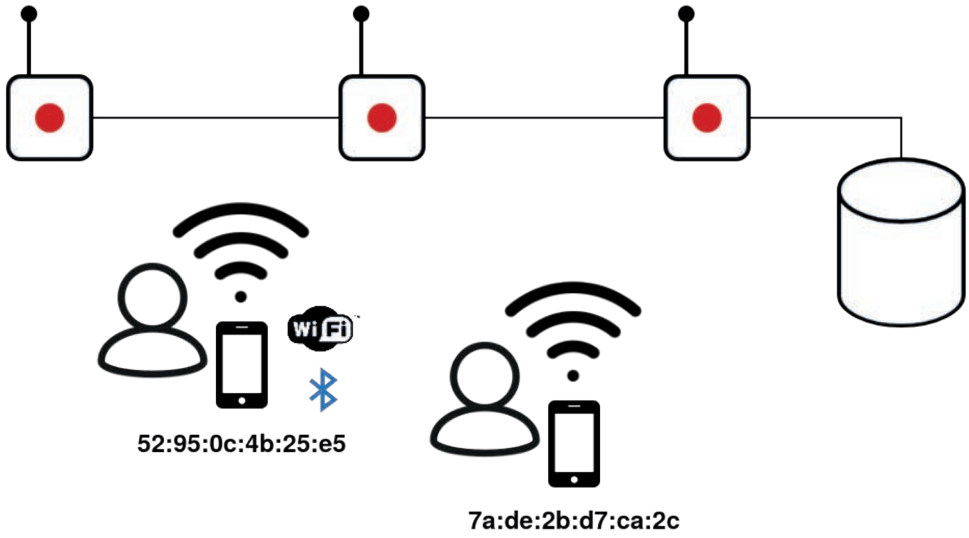

Figure 1 : Système de traçage cyberphysique basé sur le Wi-Fi et/ou le Bluetooth. Les signaux émis par les ordiphones sont captés par des *sniffers*, permettant un suivi des porteurs de ces appareils (Source : D. R.)

Ces systèmes de traçage cyberphysique ont trouvé une diversité d'applications. Par exemple dans le domaine des transports avec l'observation des flux sur les axes routiers [2], ou encore dans les transports en commun comme dans le métro londonien [3]. Un autre domaine d'application est les enseignes commerciales qui utilisent ces systèmes dans le cadre d'applications dites d'*analytics*, donnant lieu à des mesures de la clientèle (nombre de visiteurs, durée et fréquence des visites, etc.). Sur le modèle du traçage en ligne, le traçage cyberphysique permet de profiler les personnes et de leur soumettre de la publicité ciblée sur leurs ordiphones [4] ou dans le monde physique *via* des écrans publicitaires [5].

Enjeux légaux et réglementaires

Le traçage cyberphysique et la collecte de données qui en découle sont soumis à un ensemble de règles, et en particulier au Règlement général sur la protection des données (RGPD), entré en application en 2018. Les données captées par ces systèmes, et notamment les identifiants d'appareils, sont des données à caractère personnel au sens du RGPD. Ainsi, il découle de cette qualification un ensemble d'interdictions et d'obligations liées à leurs collectes et leurs traitements. Ces obligations peuvent être levées si les données sont rendues anonymes, cependant cette tâche s'avère difficile à mettre en œuvre sur ce type de données.

La CNIL (Commission nationale de l'informatique et des libertés) a proposé une liste de règles [6] applicables aux systèmes de « mesure d'audience et de fréquentation dans des espaces accessibles au public ». Elle y rappelle en particulier les exigences en termes d'information des personnes et d'exercice du droit d'opposition et de rectification. Elle précise également l'importance de l'anonymisation et de la pseudonymisation des données, et rappelle les bonnes pratiques en la

(2) https://www.mobilite-intelligente.com/ressources/technologies/localisation/captures-dadresses-bluetooth
(3) https://techcrunch.com/2019/05/22/mind-the-privacy-gap/
(4) https://info.haas-avocats.com/droit-digital/smartphone-et-g%C3%A9olocalisation-un-dispositif-sous-haute-surveillance-de-la-cnil
(5) https://qz.com/112873/this-recycling-bin-is-following-you/
(6) https://www.cnil.fr/fr/dispositifs-de-mesure-daudience-et-de-frequentation-dans-des-espaces-accessibles-au-public-la-cnil

matière. En ce qui concerne la base légale, l'invocation de l'intérêt légitime est considéré comme valable si l'anonymisation intervient à court terme ; ce qui implique que les données pourront être collectées sans le consentement des personnes. Par contre, en l'absence d'une anonymisation à court terme, l'intérêt légitime n'est plus acceptable, et un consentement informé, libre et spécifique est alors nécessaire.

Plusieurs autorités de protection européennes, dont la CNIL, ont pris des décisions au sujet de systèmes de traçage cyberphysique. Ces décisions illustrent les motivations des « traceurs » et présentent ce qui n'est pas acceptable pour les autorités en l'état actuel de la législation. En 2015, la CNIL a refusé un projet d'estimation de flux piétons porté par JCDecaux et Fidzup [7] à cause d'insuffisances au niveau de l'anonymisation des données et de l'information des personnes. En 2018, cette même entreprise Fidzup a été mise en demeure par la CNIL [8] pour son système de profilage et de ciblage publicitaire mobile basé sur des systèmes de traçage cyberphysique déployés chez des commerçants. Cette mise en demeure repose sur l'absence de base légale pour ce traitement de données, et en particulier l'absence de consentement. Aux Pays-Bas, la ville d'Enschede s'est vu infliger une amende de 600 000 euros pour avoir mis en place un système qui permettait de tracer, et non pas seulement de compter, les passants dans le centre-ville [9]. On voit donc que l'absence d'anonymisation à court terme et la base légale sont les motifs principaux de ces interdictions et sanction (dans le cas des Pays-Bas) de la part des autorités de protection.

Un nouveau règlement européen, baptisé *ePrivacy*, pourrait bientôt changer cette situation. Ce règlement vient compléter le RGPD sur le cas particulier des communications électroniques. La problématique des systèmes de traçage cyberphysique *via* des signaux sans-fil y est abordée dans l'article 8 intitulé « Protection des informations stockées dans les équipements terminaux des utilisateurs finaux ou liées à ces équipements », où l'on peut lire :

« 2- La collecte d'informations émises par l'équipement terminal pour permettre sa connexion à un autre dispositif ou à un équipement de réseau est interdite, sauf si :

(cc) elle est pratiquée exclusivement dans le but d'établir une connexion et pendant la durée nécessaire à cette fin ; ou

(dd) un message clair et bien visible est affiché, indiquant les modalités et la finalité de la collecte et la personne qui en est responsable, fournissant les autres informations requises en vertu de l'article 13 du règlement (UE) 2016/679 lorsque la collecte porte sur des données à caractère personnel, et précisant les mesures éventuelles que peut prendre l'utilisateur final de l'équipement terminal pour réduire au minimum la collecte ou la faire cesser ».

Ainsi, en l'état actuel de ce règlement, un affichage informant sur le traçage et les moyens de s'opposer ou de limiter la collecte de données serait suffisant. On note que cette position est beaucoup plus libérale que celle de la CNIL qui exige pour le moment une anonymisation à court terme ou un consentement.

Enjeux technologiques

Si les protections réglementaires ne sont plus suffisantes, la technologie à la source du problème peut nous fournir des solutions pour échapper à ce traçage.

(7) https://www.legifrance.gouv.fr/cnil/id/CNILTEXT000031159401/
(8) https://www.frenchweb.fr/la-cnil-met-en-demeure-deux-startups-de-ciblage-publicitaire/332384
https://www.legifrance.gouv.fr/cnil/id/CNILTEXT000037217124/
(9) https://datanews.levif.be/ict/actualite/la-ville-neerlandaise-d-enschede-se-voit-infliger-une-amende-gdpr-pour-du-tracage-wifi/article-news-1420015.html?cookie_check=1626181080

Adresses aléatoires

Face à cette menace de traçage accentuée par la généralisation des objets portables intégrant Wi-Fi ou Bluetooth, une solution a été proposée. Cette solution, appelée « adresse aléatoire », repose sur la substitution de l'identifiant permanent présent dans les signaux par un identifiant aléatoire et temporaire. Ainsi, l'appareil utilise consécutivement des pseudonymes indépendants qui rendent inopérants les systèmes de traçage cyberphysique.

Fabricants et développeurs d'OS

L'intégration des mécanismes anti-traçage tels que les adresses aléatoires est la responsabilité des fabricants de systèmes d'exploitation (OS) mobiles, comme Apple pour iOS et Google pour Android. De plus, les fabricants sont souvent amenés à adapter le système d'exploitation, et il est de leur responsabilité de veiller à ce que les modifications qu'ils apportent au système n'affectent pas les protections anti-traçage. Ces mécanismes de protection sont aujourd'hui intégrés dans une majorité des appareils récents. Néanmoins, il a pu être observé des failles qui remettaient en cause l'efficacité de ces protections. En effet, l'utilisation d'une adresse aléatoire n'est pas suffisante à elle seule, et son intégration est loin d'être évidente.

Au-delà des mécanismes de protection, il est nécessaire de fournir à l'utilisateur des moyens de contrôle clairs et efficaces. Dans le cadre du traçage *via* Wi-Fi et Bluetooth, il est parfois suggéré d'éteindre les fonctionnalités sans-fil de l'appareil pour échapper au traçage. Cependant, cette opération ne désactive que partiellement les fonctionnalités sans-fil et n'empêche pas le traçage [(10)]. Des efforts sont donc nécessaires pour informer les utilisateurs de cette collecte de données et pour leur fournir les moyens de s'y opposer.

Standardisation

Les technologies telles que le Wi-Fi et le Bluetooth sont définies par des standards techniques sur lesquels les fabricants se basent pour développer leurs produits. Ces documents déterminent donc les exigences sur les fonctionnalités auxquelles doivent satisfaire les appareils voulant apparaître comme conformes à ces normes. Ainsi, ces standards techniques sont en capacité d'imposer la mise en place de mesures de protection à une très large échelle.

Au sein de ces standards, la sécurité des communications est un enjeu qui a été considéré dès leur genèse, et une large part des spécifications est dédiée à la description de mécanismes de sécurité (par exemple WPA – Wi-Fi Protected Access). Comparativement, on retrouve peu d'éléments liés aux problématiques de vie privée telles que les protections contre le traçage cyberphysique. Si l'on s'intéresse au cas de l'adresse aléatoire, son introduction dans le Bluetooth coïncide avec l'introduction du BLE en 2010, tandis que son introduction dans le 802.11 (Wi-Fi) s'est faite beaucoup plus tardivement, en 2018 [(11)]. Depuis peu, les enjeux de protection des données personnelles commencent à prendre de l'importance au sein de ces standards, avec notamment la constitution de groupes de travail [(12)] sur le sujet et la publication d'un document de l'IEEE 802 sur les considérations en matière de protection de la vie privée dans ces standards [(13)].

(10) https://linc.cnil.fr/fr/desactiver-le-wi-fi-android-ne-nous-preserve-pas-du-tracage
(11) https://standards.ieee.org/standard/802_11aq-2018.html
(12) "IEEE P802.11 - Randomized and Changing MAC address (RCM) Study Group (SG)", https://www.ieee802.org/11/Reports/rcmtig_update.htm
(13) "IEEE 802E-2020 - IEEE Recommended Practice for Privacy Considerations for IEEE 802® Technologies", https://standards.ieee.org/standard/802E-2020.html

Conclusions & perspectives

Le traçage des personnes est rendu possible par une adoption croissante d'appareils équipés de technologies sans-fil. Les problématiques de vie privée associées font apparaître des enjeux technologiques, mais aussi légaux et réglementaires. Il est essentiel de considérer ces problématiques le plus tôt possible pour mettre en place des protections adéquates. Ceci est particulièrement important pour les aspects technologiques, car, une fois définis, les standards sont difficilement modifiables et demeurent en vigueur pendant de longues périodes.

Au-delà du Wi-Fi et du Bluetooth, dont il a principalement été question dans cet article, une meilleure prise en compte de problématiques de vie privée est nécessaire dans le développement des futures technologies sans-fil. En effet, Wi-Fi et Bluetooth sont progressivement rejoints par d'autres technologies qui pourraient être à la source de nouvelles menaces pour la vie privée. Par exemple, l'Ultra Wide Band (UWB), qui permet d'estimer les distances entre appareils avec une précision de quelques centimètres, est progressivement intégrée dans les appareils mobiles. L'UWB pourrait donc favoriser un traçage beaucoup plus fin que ce qui est réalisé actuellement par les technologies Wi-Fi et Bluetooth.

Bibliographie

CELOSIA G. (2020), *Privacy challenges in wireless communications of the Internet of Things,* thèse de doctorat, Université de Lyon, INSA-Lyon.

DEMIR L., CUNCHE M. & LAURADOUX C. (2014), "Analysing the privacy policies of Wifi Trackers", *Proceedings of the 2014 Workshop on Physical Analytics*, New York, NY, USA, pp. 39-44.

MATTE C. (2017), *Traçage Wi-Fi : Attaques par prise d'empreinte et contre-mesures*, thèse de doctorat, Université de Lyon, INSA-Lyon.

MATTE C. & CUNCHE M. (2016), « Traçage Wi-Fi : applications et contre-mesures », *GNU/Linux Magazine*, n°84, hors série.

MAVROUDIS V. & VEALE M. (2018), "Eavesdropping whilst you're shopping: Balancing personalisation and privacy in connected retail spaces", *Living in the Internet of Things: Cybersecurity of the IoT – 2018,* pp. 1-10.