• VIE PRIVÉE

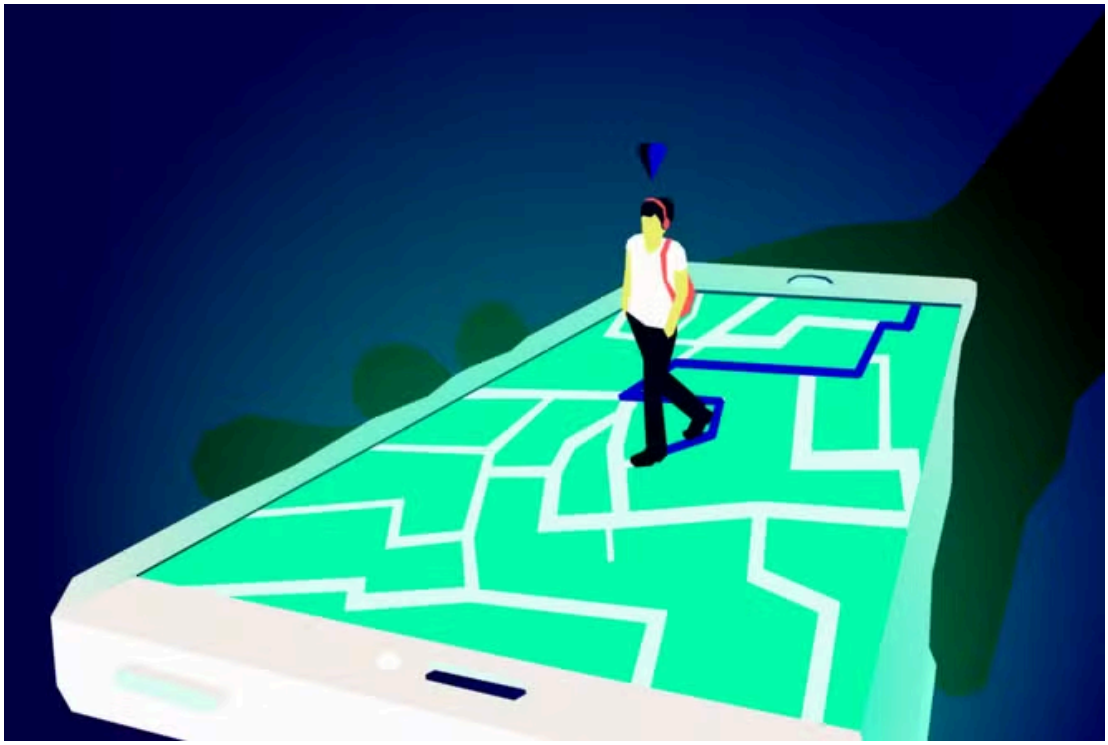
Le pistage des internautes par des applications mobiles (et comment s'en protéger) en quatre questions

Comment savoir qui récupère mes données personnelles et à quelle fin ? Que dit la loi ? Est-il possible de limiter l'accès à mes données ? « Le Monde » répond aux questions que posent les « super fichiers » des courtiers en données.

Par Adrien Sénécat et Martin Untersinger

Publié aujourd'hui à 08h00, modifié à 08h58 • Lecture 3 min.

Article réservé aux abonnés



QUENTIN HUGON / « LE MONDE »

C'est un gigantesque fichier, qui rassemble des informations sur plus de 47 millions d'internautes, issues de près de 40 000 applications mobiles. Et il ne s'agit là que d'un fragment de la base de données géolocalisées de l'entreprise américaine Datastream Group, partagé à des fins commerciales. L'enquête du *Monde*, en partenariat avec huit médias internationaux, montre l'ampleur du pistage des internautes à partir d'applications du quotidien comme Le Bon Coin, Candy Crush ou Vinted. Des pratiques qui posent des questions légales, éthiques, mais aussi pratiques pour tout utilisateur de smartphone.

Lire l'enquête | Données personnelles en vente libre : les « data brokers », une industrie hors de contrôle

• Quelles règles s'appliquent à la collecte et à l'utilisation de mes données personnelles ?

Les données publicitaires issues des applications mobiles étant des données personnelles, la loi européenne en la matière s'applique. Elle donne aux citoyens des droits, comme celui de s'opposer à ce que leurs données soient utilisées ou celui de demander leur suppression. Elle donne aussi des

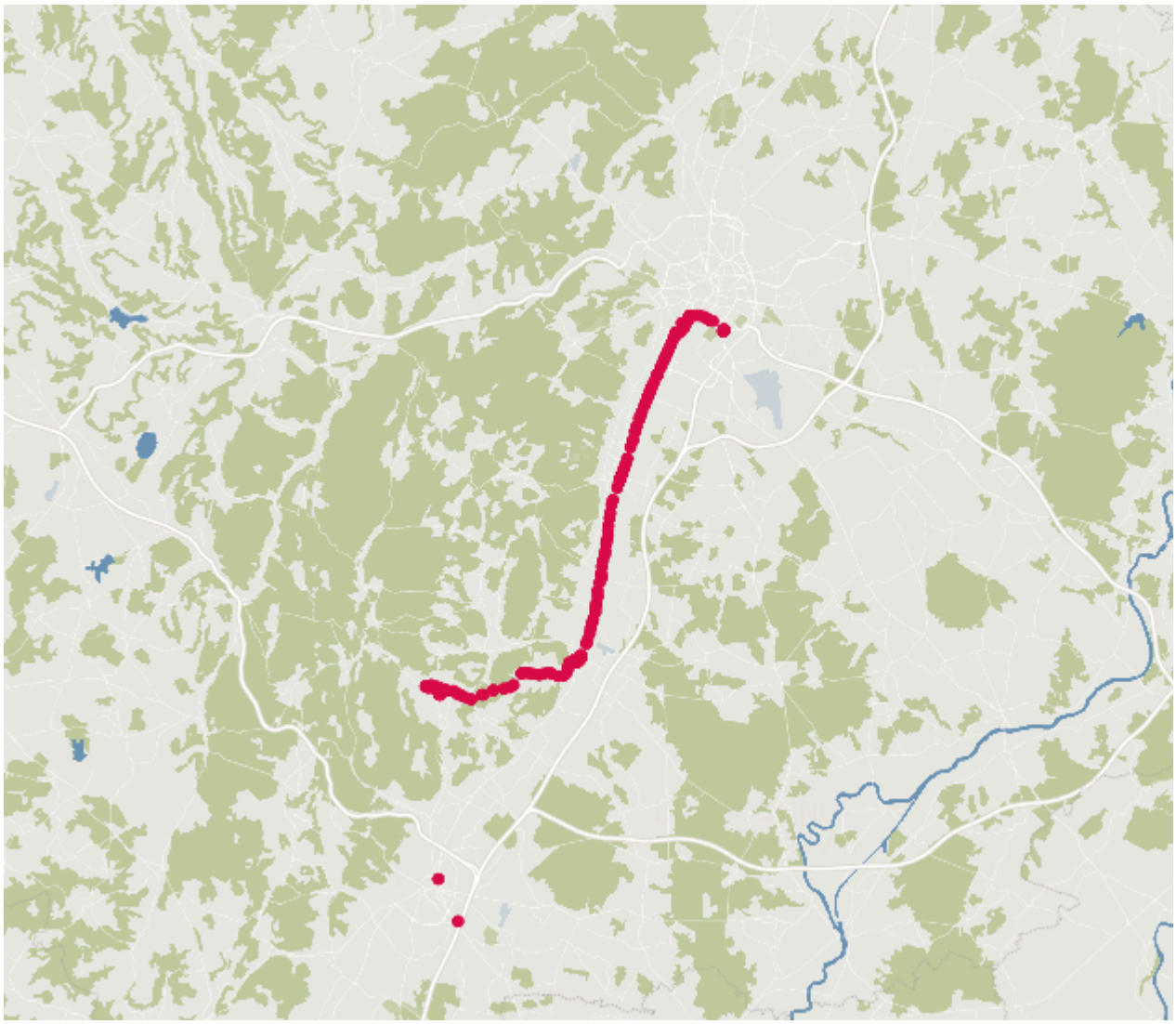
devoirs aux entreprises : collecter un minimum de données, les stocker de manière sécurisée, les supprimer dès que possible…

Le fait que ce soit des données publicitaires rend, par ailleurs, obligatoire le consentement des utilisateurs : celui-ci doit être libre (l'application ne doit pas cesser de fonctionner s'il ne consent pas, par exemple), éclairé (ce qui suppose que les informations sur la collecte de données soient disponibles et claires) et explicite (la seule utilisation d'une application ne peut l'impliquer, par exemple).

Ce qu'il est possible de surveiller avec ces données

Un trajet | Un domicile | Un lieu public

Dans de nombreux cas, les données de localisation permettent de retracer les trajets entiers des mobinautes, comme ici entre Nuits-Saint-Georges et Dijon, en Côte-d'Or.



Source : Le Monde

• Comment savoir quelles informations sont collectées et à qui elles sont partagées ?

C'est possible, mais très complexe – et limité. Les informations déclarées par les éditeurs d'applications posent, en effet, plusieurs problèmes. Les notices de confidentialité présentes sur les magasins d'applications, qui doivent en principe renseigner sur le sort fait aux données de leurs utilisateurs, sont ainsi souvent parcellaires. Il est donc déconseillé de s'y fier pour faire son choix. De même, on peut lire les politiques de confidentialité de chaque application, ainsi que la liste des partenaires publicitaires avec qui les données personnelles peuvent être partagées. Mais la tâche s'avère monumentale, tant ces textes sont longs et détaillés.

La liste des permissions accordées à chaque application en matière d'accès aux données, accessible dans les paramètres du téléphone, permet plus directement de savoir quelles sont les principales sources de données d'une application – et d'en désactiver une partie. La plateforme Exodus permet, en outre, de savoir quelles sont les permissions d'une application Android avant même de l'installer. Certaines données, notamment l'adresse IP, qui peut être utilisée pour géolocaliser un internaute de manière imprécise, sont cependant collectées quels que soient les choix de l'utilisateur.

Lire le décryptage | Sur l'App Store et Google Play, les mensonges des applications sur leur usage des données personnelles

• Est-il possible de limiter les données que je partage ?

Oui, à la marge et de plusieurs manières :

1. **En refusant certains traitements de données.** Sur Android et iOS, chaque application demande un certain nombre d'autorisations pour accéder aux données (en particulier la géolocalisation) : la première ligne de défense est donc d'examiner avec soin les autorisations des applications utilisées et de n'accepter que pour les cas les plus utiles.

2. **En désactivant la géolocalisation.** Pour les utilisateurs d'Android, Vincent Toubiana, chef du service laboratoire d'innovation numérique de la Commission nationale de l'informatique et des libertés (CNIL), conseille d'*« ajouter le paramètre de localisation dans les "Quick Settings", ce qui permet d'activer ou désactiver la localisation pour tout le téléphone très rapidement ». « Si la géolocalisation du téléphone n'est pas activée, les applications n'y auront pas accès »*, résume-t-il.

3. **En limitant le nombre d'applications.** Plus largement, *« il faut éviter les applications qui demandent trop de permissions, comme une lampe torche qui demande accès à mes contacts et à ma géolocalisation »*, explique Nacéra Bekhat, cheffe du service de l'économie numérique et du secteur financier à la CNIL. Mathieu Cunche, professeur d'informatique à l'Institut national des sciences appliquées de Lyon et à l'Institut national de recherche en sciences et technologies du numérique, suggère même de limiter au maximum l'utilisation d'applications sur son téléphone et de privilégier l'utilisation du navigateur du téléphone, plus respectueux de la vie privée.

4. **En restreignant le suivi publicitaire.** Il est aussi possible de remettre à zéro son identifiant publicitaire, voire de désactiver le suivi publicitaire, mais plusieurs experts interrogés regrettent que les publicitaires disposent d'autres moyens de pister les utilisateurs d'applications. *« Un des principaux problèmes est que les fonctionnalités de contrôle et de transparence des grandes*

plateformes sont insuffisantes pour limiter cette dissémination massive et large de données personnelles », explique Narseo Vallina Rodriguez, chercheur à l'Imdea Networks Institute, à Madrid, et spécialiste des enjeux de protection des données mobiles.

• Puis-je demander à faire effacer mes données ?

Oui : le droit européen sur les données personnelles prévoit explicitement un droit d'opposition et de suppression des données personnelles. L'utilisateur peut en faire la demande directement auprès de l'acteur publicitaire qui manipule ses données (à condition de le connaître) ou directement auprès de l'application où elles ont été récoltées. Cette dernière aura l'obligation légale de transmettre la requête aux entités auxquelles elle a fourni ces données.

Les « Data Brokers Files », une enquête internationale

Cette enquête a été lancée à l'initiative de nos partenaires de *Netzpolitik.org*, qui ont obtenu un échantillon de la base de données de l'entreprise Datastream Group, partagé avec de potentiels clients. On y trouve des informations sur plus de 47 millions d'appareils mobiles dans 137 pays du monde pour la journée du 2 juillet 2024, dont un million en France.

Au total, 380 millions de coordonnées géographiques, d'un degré de précision variable, collectées par 39 499 applications, figurent dans ce

Adrien Sénécat et **Martin Untersinger**

Mixeurs plongeants
Les meilleurs mixeurs plongeants

Fours micro-ondes grill
Les meilleurs fours micro-ondes grill

Voir plus