Lire les documents, puis répondre aux questions suivante sous la forme d'un seul paragraphe argumenté.

Questions : Quelles données personnelles sont collectées par les entreprises du numérique ? Comment sont-elles connectées ? La collecte de données personnelles anonymes est-elle une menace pour la vie privée ?

« L'Œil du 20 heures » et France Info. ***« TrackingFiles » : quand les données de géolocalisation de dizaines de millions de Français se retrouvent en vente.*** **francinfo, 04/03/2025**
`https://www.franceinfo.fr/internet/securite-sur-internet/enquete-trackingfiles-quand-les-donnees-de-geolocalisation-de-dizaines-de-millions-de-francais-se-retrouvent-en-vente_7101777.html`

Chaque portable possède un identifiant publicitaire unique, appelé « advertising ID ». Lorsqu'on ouvre une application, s'il y a un emplacement pour une publicité, une notification est envoyée à une sorte de salle d'enchères virtuelle, dans laquelle se trouvent des régies publicitaires. En un clin d'œil, le plus offrant affiche une publicité dans l'application. Mais dans cette transaction de quelques millisecondes, l'utilisateur laisse des traces.
Ainsi, l'identifiant publicitaire est envoyé aux régies publicitaires, ainsi que la localisation du téléphone. Ces données sont ensuite rachetées par des *data brokers*, des courtiers spécialisés dans les données personnelles, pour les revendre, par exemple à des fins marketing. Parfois, ce sont aussi les applications elles-mêmes qui les revendent, après avoir récolté des données sur leurs utilisateurs.
[…]
[Les fichiers des courtiers en données obtenus par les journalistes] concernent près de 12 millions de téléphones et plus d'un milliard de points GPS. […] [Ces données] sont en théorie anonymes, car uniquement liées à l'identifiant publicitaire. Pourtant, il est aisé de recouper les centaines de points pour retrouver des informations, permettant de savoir à qui appartient le téléphone.

Cory Doctorow. ***Delta's AI-based price-gouging.*** **Pluralistic, 30/07/2025**
`https://pluralistic.net/2025/07/30/efficiency-washing/`

Les courtiers en données possèdent toutes les sortes de données sur vous, des informations « légitimes » concernant tous les lieux visités en voiture, en passant par chaque endroit par lequel votre radio ou vos écouteurs *bluetooth* sont passés, ou encore tout ce que vous avez acheté, jusqu'à chacun des sites web parcourus et toutes les recherches que vous avez effectuées. Ils achètent aussi des données qui vous ont été carrément volées par un logiciel espion installé sur votre téléphone. Toutes ces données peuvent être rassemblées dans un unique fichier que vous n'avez pas de droit d'examiner, et encore moins de corriger.
[…]
McDonald a investi dans la *start-up* néozélandaise Plexure, qui propose d'aider les restaurants à faire gonfler les prix de votre commande habituelle les jours de paye, quand vous pouvez vous permettre de payer plus. Et il y a les trois grosses applications « Uber des infirmières », qui utilisent les données de surveillance pour calculer les salaires des infirmières, proposant un taux horaire inférieur aux personnes endettées, en supposant qu'elles seront trop désespérées pour refuser une offre au ras des paquerettes. Et alors que ces applications décident de la valeur de votre travail, les systèmes tarification par la surveillance décident de la valeur de votre argent, en vous faisant payer plus qu'un autre consommateur par ailleurs identique, pour un produit identique, ce qui signifie qu'un de vos dollars vaut moins que celui de l'autre consommateur.