« LE SOIR » RÉPOND À VOS QUESTIONS

Deux ans après la première opération « Pourquoi ? », Le Soir a une nouvelle fois sollicité ses abonnés, invités à lui soumettre leurs interrogations sur le monde qui nous entoure.

Pourquoi Meta utilise-t-elle les données cachées des photos et vidéos postées sur ses réseaux ?

Cet article répond à la question de Laurent, de Bruxelles

PHILIPPE LALOUX

Pourquoi Meta utilise-t-elle les données cachées des photos et vidéos que nous publions sur Facebook et Instagram ? » Réponse directe : parce que nous l'y avons autorisé. Ce n'est, certes, pas totalement faux, mais balayer cette excellente question d'un tel revers de main reviendrait à donner de l'eau au moulin de la plateforme qui, depuis toujours, s'appuie sur cet argument pour justifier sa récolte massive de données à caractère personnel.

La collecte de ces données est au cœur du modèle économique des réseaux sociaux, appelé aussi « capitalisme de surveillance ». Cette stratégie consiste à transformer systématiquement les comportements des utilisateurs en matière première gratuite, sous forme de données, pour en faire un produit à vendre à d'autres acteurs (annonceurs, partenaires, etc.). Si leurs services sont « gratuits », c'est que l'utilisateur est le produit et que leur véritable client est l'annonceur qui paie pour accéder à ces prédictions ultra-ciblées.

Surveillance et influence

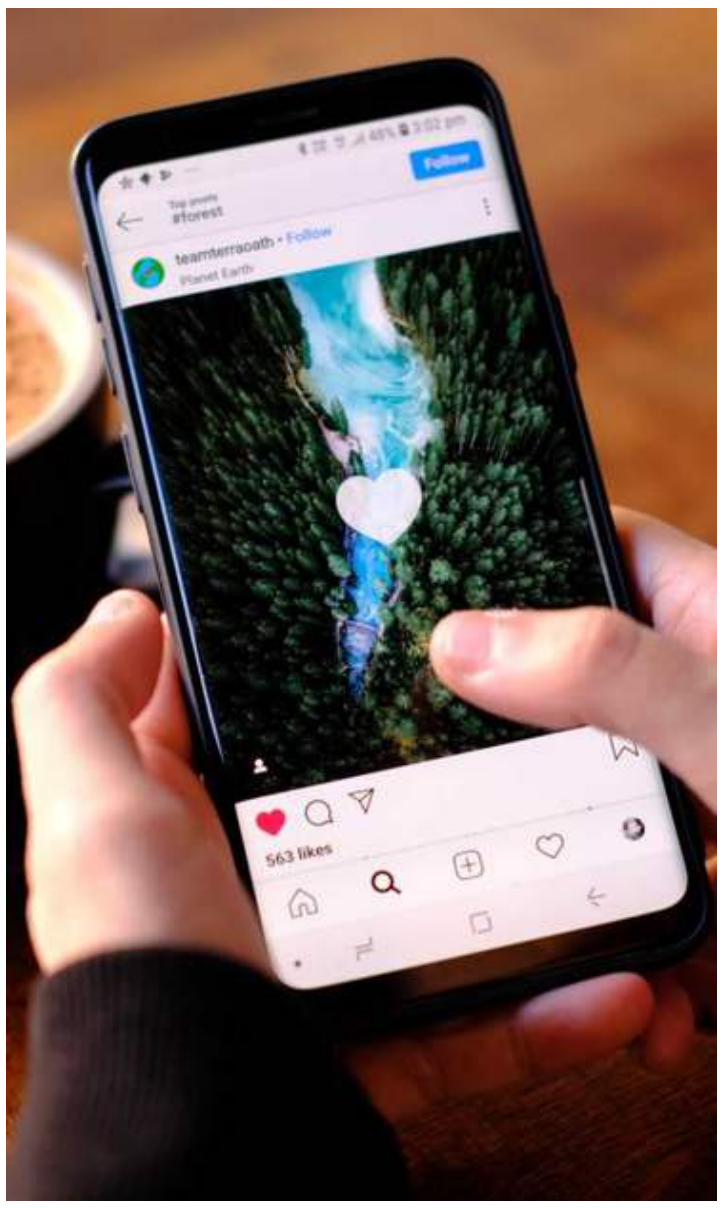
Concrètement, chaque clic, « scroll », « like », trajet, photo ou interaction alimentent des profils comportementaux de plus en plus fins, capables de prédire les envies, les achats, parfois même les opinions des utilisateurs. Ceux-ci communiquent leur nom, numéro de téléphone, adresses e-mail et physique et, dans certains cas, leurs préférences. Ces prédictions sont ensuite vendues aux annonceurs et partenaires qui paient pour cibler « la bonne personne, au bon moment, avec le bon message ». Plus la collecte est massive et continue, plus les prédictions sont précises, et plus le modèle est rentable. Au passage, notre vie quotidienne devient un champ de surveillance et d'influence commerciale quasi permanente.

A noter que, comme l'a confirmé la firme, Facebook collecte aussi des données via des outils (comme le bouton « J'aime ») intégrés sur des millions de sites web et applications tiers. Cela signifie que même si on ne navigue pas sur Facebook, le réseau social sait quels sites on visite et quels achats on effectue. Par ailleurs, depuis mai 2015, même s'il est possible de s'y opposer, Meta utilise aussi, par défaut, toutes les publications, photos et commentaires publics publiés sur ses réseaux pour entraîner son intelligence artificielle.

Parmi cette masse de données aspirées, on retrouve notamment les métadonnées cachées dans la moindre photo ou vidéo prise par un smartphone et publiée sur Facebook ou Instagram. De quoi parle-t-on ? Des données dites « exif », intégrées automatiquement aux fichiers images lors de la prise de vue. On y retrouve la date et l'heure de la prise de vue, les coordonnées GPS (si la localisation est activée), le modèle de l'appareil, les paramètres de la caméra… Autant de données précieuses pour l'utilisateur (par exemple pour retrouver facilement ces photos dans ses albums). Mais aussi pour Meta.

Est-ce que pour autant, tout le monde peut voir ces données (et regarder votre vie privée par le trou de la serrure) ? Non. Tant Facebook qu'Instagram les suppriment de la copie publique, officiellement pour faire de la place sur leurs serveurs (à eux seuls, ces deux réseaux ingurgitent plus de 2.400 photos par seconde). En revanche, Meta y a toujours accès, ainsi qu'à d'autres signaux de localisation (adresse IP, localisation de l'appareil, lieux tagués, etc.).

Avec les réseaux sociaux, notre vie quotidienne est devenue un champ de surveillance et d'influence commerciale quasi permanente. © CANVA.



Des données qui valent de l'or

Pour quoi faire ? Du ciblage publicitaire, avant tout. En sachant où les utilisateurs prennent leurs photos, Instagram et Facebook savent où ils habitent, travaillent et quels magasins ils fréquentent. Cela leur permet, par exemple, de vous montrer des publicités pour le restaurant qui se trouve à 200 m de vous au moment précis où vous y êtes. Si un internaute publie souvent des photos depuis des salles de sport ou des parcs, il sera classé dans la catégorie « sportif », ce qui a une grande valeur pour les annonceurs.

L'heure et le lieu de la prise de vue permettent aussi d'affiner l'algorithme de recommandation de ces plateformes. Bref, ces données valent de l'or. Elles permettent de créer une carte des déplacements de ses utilisateurs, d'identifier leurs centres d'intérêt réels, de vérifier la véracité de leur compte, d'alimenter les fonctions « souvenirs », de comprendre la saisonnalité de leurs achats, de savoir quand ils sont les plus susceptibles de cliquer sur une pub, de déterminer s'ils ont un iPhone dernier cri ou un modèle ancien, d'obtenir des indices sur leur pouvoir d'achat…

La vraie question : l'utilisateur a-t-il donné son consentement pour ces usages ? Si l'on se réfère au Règlement général sur la protection des données (RGPD), une entreprise doit avoir au moins un « fondement légal » pour traiter des données à caractère personnel, parmi celles-ci : le consentement explicite, l'exécution d'un contrat, l'obligation légale, l'intérêt vital, la mission d'intérêt public ou l'intérêt légitime.

Concernant la publicité ciblée, Meta s'est historiquement retranchée derrière la notion de « contrat » et d'« intérêt légitime ». Des bases juridiques jugées « illégales » par les autorités de régulation et la Cour de justice de l'Union européenne, forçant la plateforme à basculer vers le consentement explicite de l'utilisateur. Mais même si l'utilisateur refuse, Meta continue à se fonder sur l'intérêt légitime pour récolter ces données à des fins dites « techniques », comme la sécurité ou la lutte contre le spam. La plateforme pousse donc les bases légales au maximum de ce que les régulateurs tolèrent… jusqu'à se faire condamner.

Comment y échapper ?

Pour échapper à cette récolte forcée de métadonnées, l'utilisateur a deux options. La première, laborieuse, consiste à utiliser des outils de « nettoyage » (comme « Exif Eraser »), qui suppriment toutes les données cachées avant que vous ne téléchargiez l'image sur Instagram ou Facebook. La seconde, radicale, suggère de désactiver la géolocalisation de l'appareil photo, ce qui vous prive d'un précieux outil de recherche, puisque les images n'auront plus de coordonnées GPS intégrées. Quoi qu'il en soit, il n'est jamais inutile d'aller jeter un cil sur les autorisations de localisation d'Instagram et de Facebook dans les paramètres iOS/Android et dans les paramètres de confidentialité Meta.

Il existe néanmoins un moyen imparable d'empêcher Facebook ou Instagram (ou n'importe quelle plateforme) d'exploiter indûment vos données à caractère personnel, y compris les métadonnées de vos photos : ne rien y publier. Ou supprimer toutes vos photos.

Cet article répond à la question de Laurent, de Bruxelles : « Pourquoi Méta utilise les données cachées dans les photos et vidéos postées sur ses réseaux sociaux (surtout Instagram), et à quoi cela sert d'avoir ces données ? »