**LT-14012020-Une enquête révèle comment Tinder & Cie siphonnent nos données**

Soutenue par la FRC, une enquête menée en Norvège montre comment Tinder, Grindr, Clue ou OKCupid amassent des sommes considérables de données en toute illégalité. Le préposé fédéral à la protection des données est interpellé

Ce sont [185 pages d’une étude](https://www.forbrukerradet.no/out-of-control/) au contenu aussi consternant qu’effrayant qui sont publiées ce mardi. Si certains consommateurs européens et suisses se doutaient que certaines des applications installées dans leur smartphone se montraient indiscrètes, ils en ont aujourd’hui la certitude.

Une enquête menée par l’association norvégienne de défense des consommateurs Norwegian Consumer Council, à laquelle se sont associées dix autres organisations similaires, dont la Fédération romande des consommateurs (FRC), documente de manière précise comment des applications populaires telle Tinder abusent de la confiance des internautes. Elles accumulent des masses considérables de données, et les revendent à des tiers à des fins publicitaires, en toute illégalité.

**Lire aussi:** [«L’amour sous algorithme» dévoile le côté obscur de Tinder](https://www.letemps.ch/societe/lamour-algorithme-devoile-cote-obscur-tinder)

Intitulée «Out of Control» (Hors de contrôle), l’enquête démontre «comment les consommateurs sont exploités par l’industrie de la publicité en ligne», écrivent les auteurs de l’étude. Avec de nombreux exemples, le document révèle comment, chaque fois que nous utilisons des applications, des centaines d’entités de l’ombre – comme les appellent les auteurs du rapport – reçoivent des données personnelles sur nos intérêts, nos habitudes et notre comportement. «Ces informations sont utilisées pour établir le profil des consommateurs, qui peut être utilisé pour la publicité ciblée, mais peut également conduire à la discrimination, la manipulation et l’exploitation», affirment les responsables du Norwegian Consumer Council.

**Tinder, si opaque**

L’enquête documente deux problèmes de taille. Le premier a trait à la masse colossale d’informations que récoltent les applications, sans consentement explicite ou implicite, et surtout sans aucune raison valable. Le second est lié au commerce de ces données par ces «entreprises de l’ombre», des agrégateurs d’informations inconnus du grand public qui créent ainsi des profils précis dont raffolent les annonceurs.

**Lire aussi:** [Une enquête révèle comment les smartphones sont pistés de manière inouïe](https://www.letemps.ch/economie/une-enquete-revele-smartphones-pistes-maniere-inouie)

L’étude s’est principalement intéressée à dix applications, dont par exemple Tinder. Téléchargée plus de 100 millions de fois, il s’agit de l’une des applications de rencontre les plus populaires. Tinder appartient à la société de Los Angeles Match Group. Selon l’étude, un utilisateur de Tinder risque de voir ses données partagées avec les… 45 autres applications et services de ce groupe. C’est a priori illégal au vu du Règlement général sur la protection des données (RGPD), d’autant que le consentement explicite du consommateur n’est pas demandé. De plus, l’enquête a démontré que Tinder envoie les coordonnées GPS de l’utilisateur à des revendeurs de données tels AppsFlyer (qui affirme avoir des données sur… 8,4 milliards d’appareils) et Leanplum. Quant au profil publicitaire du consommateur (Advertising ID), il est récolté par AppsFlyer, Branch, Facebook et Salesforce.

**Grindr hors de contrôle**

Un autre exemple choquant est celui de Grindr. L’application de rencontre gay/bi, téléchargée plus de 10 millions de fois, est propriété d’un groupe chinois, mais son éditeur est aux Etats-Unis. L’application avait été au cœur d’un premier scandale en 2018, après une plainte du Norwegian Consumer Council parce que Grindr partageait le statut HIV des utilisateurs avec des tiers. Aujourd’hui encore, montre l’étude, Grindr partage coordonnées GPS, adresse IP et identifiant de publicité avec une dizaine de sociétés externes. Et Grindr affirme qu’il «ne contrôle pas l’usage de ces technologies de *tracking*» et demande à ses utilisateurs d’aller lire les politiques de confidentialité de cette dizaine de sociétés tierces dont l’utilisateur ignore tout…

Tant le système iOS sur iPhone qu’Android créent un identifiant de publicité unique pour chaque smartphone, qui est censé être anonyme. Mais le partager risque de permettre d’identifier une personne. Ainsi, si Grindr transmet vos données GPS et votre identifiant et qu’une autre application transmet votre nom et votre identifiant, les courtiers en données pourront croiser ces données et connaître votre nom et votre localisation.

**Appel en Suisse**

On retrouve les mêmes problèmes avec les applications de suivi de fertilité Clue et MyDays, du programme de maquillage Perfect365, de l’application religieuse Muslim: Qibla Finder, du programme pour enfants *My Talking Tom 2* ou encore du clavier virtuel Wave Keyboard. Il est possible que certains éditeurs de ces applications réagissent dans les jours à venir à ce rapport.

**Découvrez notre dossier:** [La protection des données, affaire personnelle](https://www.letemps.ch/dossiers/protection-donnees-affaire-personnelle)

Que faire face à cette surveillance de masse? Ce lundi, la FRC a interpellé le préposé fédéral à la protection des données via un courrier formel. «Nous lui demandons d’évaluer la légalité de ces pratiques en Suisse et de prendre des mesures le cas échéant, détaille Robin Eymann, responsable de la politique économique à la FRC. Individuellement, il est très compliqué pour un consommateur de pouvoir s’opposer à ce type de pratique. On parle toujours de la responsabilité du consommateur, mais on voit bien qu’il n’a aucun moyen de donner son consentement en étant bien informé car les conditions générales sont très opaques et lacunaires et même quand il refuse le ciblage publicitaire, les applications ne respectent pas sa volonté. C’est donc bien aux autorités d’agir.»

**Paramétrage important**

A priori, les dix applications sont toutes utilisées en Suisse. «D’autres procèdent certainement de la même manière, donc on pointe du doigt dix applications, mais c’est sûrement juste la pointe de l’iceberg», poursuit Robin Eymann.

Le consommateur peut pour l’heure agir via les paramètres de son smartphone pour demander un suivi publicitaire limité. Sur un iPhone, il faut ainsi aller dans «réglages», puis «confidentialité», «publicité» et activer enfin le «suivi publicitaire limité». Une fonction similaire existe sur Android et il semble que le pistage des internautes soit moins grand sur iPhone, selon les auteurs de l’étude. Mais comme ces derniers le font remarquer, les entreprises marketing parviennent souvent à contourner ces paramètres.