Vie privée sur le web 3.0: vivre dans une maison de verre?

Le monde numérique apporte bien du confort, mais à un prix parfois élevé. La sphère privée ne va plus de soi. Elle s'estompe désormais, noyée silencieusement dans une connectivité omniprésente. Et elle devient un bien rare.

L'auteur
Thomas Zweifel, Principal IT Consultant, AdNovum

L'utilisation du Social Login est gratuite pour l'utilisateur, mais il la paie avec ses données de profil et d'utilisation.

Chacun le sait: lorsque l'on veut s'inscrire sur un site web, le mot de passe doit être unique, sûr et ne pas être enregistré. Il est dès lors plus pratique de se connecter à l'aide d'un Social Login, comme ceux de Facebook et de Google, disponibles sur de nombreux sites. Ce login centralisé peut à son tour être protégé par une authentification à deux facteurs ou par des mesures de sécurité basées sur le comportement inhabituel de l'utilisateur.

Chaque chose a son prix

L'utilisation du Social Login est gratuite pour l'utilisateur, mais il la paie avec ses données de profil et d'utilisation. En effet, ces données représentent une valeur marchande substantielle et sont précieuses pour les fournisseurs des sites web. Certes, l'utilisateur peut contrôler le transfert et la diffusion de données telles que l'image de son profil, son âge et ses listes d'amis avec le fournisseur du site web. Rien n'empêche cependant la collecte de l'ensemble de ses données d'utilisation. Une collecte qui peut aussi servir l'utilisateur, par exemple pour identifier un comportement inhabituel et empêcher ainsi l'accès abusif à l'un de ses comptes grâce à une analyse comportementale de ses données.

La sécurité et la confidentialité sont également des sujets importants dans le domaine du paiement mobile. En plus du confort de payer avec un smartphone ou d'exécuter des transferts peer-to-peer en temps réel, les utilisateurs peuvent bénéficier de fonctionnalités de sécurité additionnelles comme le capteur d'empreintes digitales pour valider un paiement. Des problèmes de sécurité de longue date sont ainsi résolus: en payant par exemple avec Apple Pay, aucune donnée de la carte de crédit ou de l'utilisateur n'est stockée dans le portemonnaie électronique. Il n'est donc plus possible de procéder à un clonage par copie de la bande magnétique comme avec les cartes de crédit classiques. En revanche, d'autres questions se posent: qui a dorénavant accès aux données et auxquelles exactement? Sont-elles utilisées uniquement pour les opérations de paiement ou également pour le profilage, le marketing ou la recherche?

Courir après les données personnelles

Les fitness trackers, ces petits capteurs d'activité fixés au poignet, recueillent également différentes données, en mesurant par exemple les déplacements et la position, la fréquence cardiaque ou les performances sportives. Ils aident à atteindre les objectifs que l'utilisateur s'est fixés. Il en va de même des nombreuses applications employées pour saisir toutes sortes de données, telles que le sommeil et les informations de nutrition, faisant de l'ensemble de ces solutions une sorte d'entraîneur personnel devenu indispensable. Toutefois, quiconque ayant accès à ces données peut obtenir une image très détaillée de l'utilisateur final grâce à la corrélation de celles-ci.

L'utilisateur doit donc toujours se poser la question de savoir à qui il confie ses données, à qui elles appartiennent, comment elles doivent être protégées, et qui peut les utiliser et les corréler. Il doit donc s'informer et se responsabiliser, surtout dans un domaine où les législateurs peinent à suivre. Ces derniers ne restent pourtant pas inactifs. Le 25 mai 2018 entrera en vigueur le règlement (UE) 2016/679 du Parlement Européen et du Conseil, relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, fixant ainsi pour les utilisateurs finaux et pour les entreprises des droits et des obligations précises. La Suisse va probablement s'inspirer de la norme européenne pour la révision de la loi actuelle sur la protection des données, afin d'en assurer la compatibilité avec le droit européen.

Pas seulement une question de sécurité

Les entreprises se doivent d'estimer à un stade précoce les opportunités et risques qui se posent. Les questions inéluctables sont de savoir quelles sont les technologies sur lesquelles s'appuyer, quelles dépendances elles risquent de créer, quelles sont les exigences réglementaires à surveiller et quels sont les risques de réputation. Elles peuvent cela dit faire un pas en direction de l'utilisateur final en déclarant de manière claire la relation entre leurs services et les niveaux de qualité liés à la protection de la vie privée. Les entreprises suisses peuvent également faire de la publicité en s'engageant pour le respect de la vie privée, en plus des critères de qualité et de sécurité du Swissness. Après tout, que rapporte à un client une excellente solution sur le plan de la sécurité si sa vie privée n'est plus protégée, se retrouvant ainsi simple consommateur dans une maison de verre?