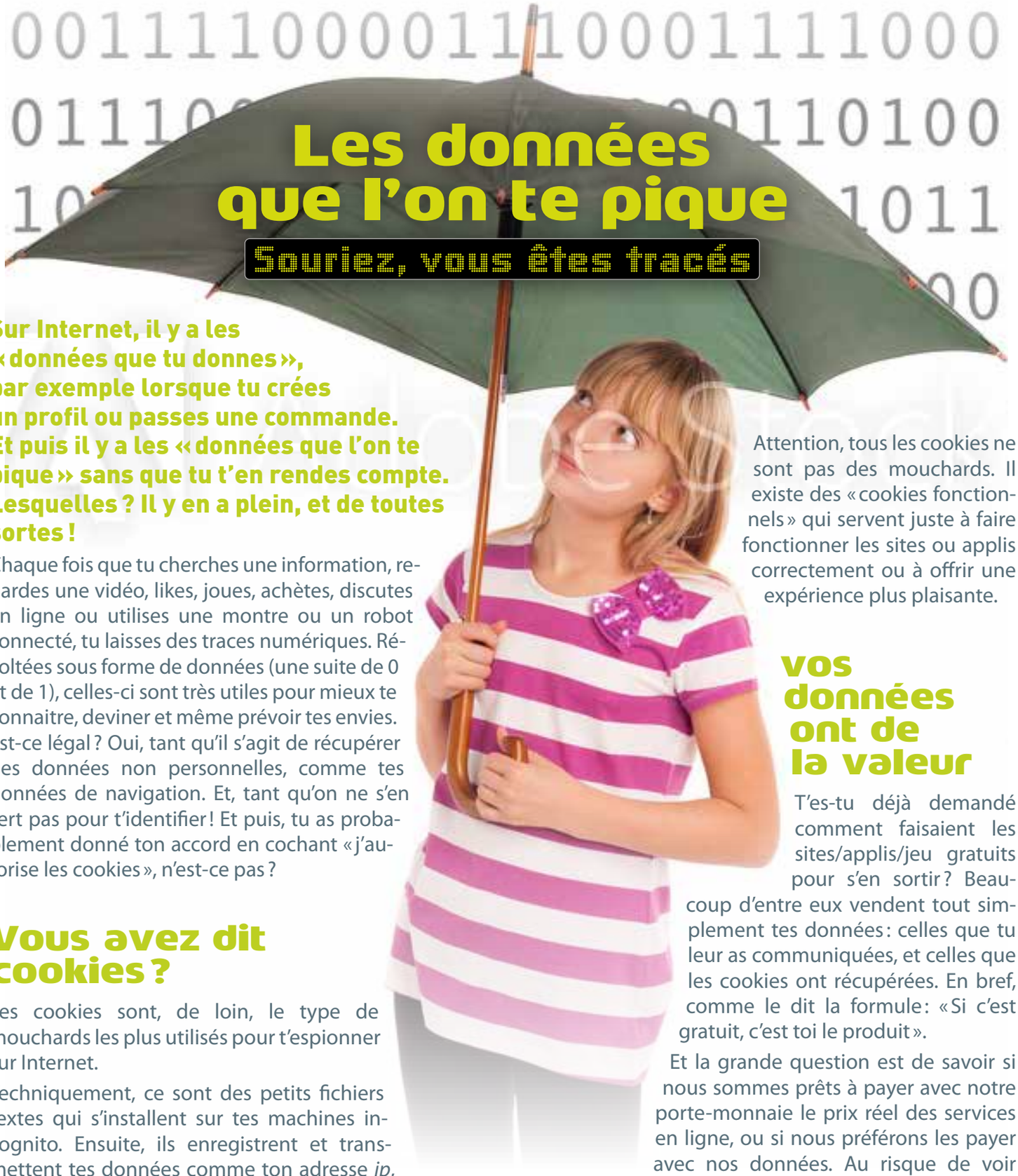
Par Pascale Garreau et Divina Frau-Meigs

Les données que l'on te pique

Souriez, vous êtes tracés



Sur Internet, il y a les « données que tu donnes », par exemple lorsque tu crées un profil ou passes une commande. Et puis il y a les « données que l'on te pique » sans que tu t'en rendes compte. Lesquelles ? Il y en a plein, et de toutes sortes !

Chaque fois que tu cherches une information, regardes une vidéo, likes, joues, achètes, discutes en ligne ou utilises une montre ou un robot connecté, tu laisses des traces numériques. Récoltées sous forme de données (une suite de 0 et de 1), celles-ci sont très utiles pour mieux te connaitre, deviner et même prévoir tes envies. Est-ce légal ? Oui, tant qu'il s'agit de récupérer des données non personnelles, comme tes données de navigation. Et, tant qu'on ne s'en sert pas pour t'identifier ! Et puis, tu as probablement donné ton accord en cochant « j'autorise les cookies », n'est-ce pas ?

Vous avez dit cookies ?

Les cookies sont, de loin, le type de mouchards les plus utilisés pour t'espionner sur Internet.

Techniquement, ce sont des petits fichiers textes qui s'installent sur tes machines incognito. Ensuite, ils enregistrent et transmettent tes données comme ton adresse *ip*, tes visites, tes achats, tes recherches, mots de passe, likes, là où tu cliques, combien de temps tu restes sur une page, etc.

Attention, tous les cookies ne sont pas des mouchards. Il existe des « cookies fonctionnels » qui servent juste à faire fonctionner les sites ou applis correctement ou à offrir une expérience plus plaisante.

Vos données ont de la valeur

T'es-tu déjà demandé comment faisaient les sites/applis/jeu gratuits pour s'en sortir ? Beaucoup d'entre eux vendent tout simplement tes données : celles que tu leur as communiquées, et celles que les cookies ont récupérées. En bref, comme le dit la formule : « Si c'est gratuit, c'est toi le produit ».

Et la grande question est de savoir si nous sommes prêts à payer avec notre porte-monnaie le prix réel des services en ligne, ou si nous préférons les payer avec nos données. Au risque de voir arriver une société où les entreprises comme les états sachent tout sur tout le monde.

Les datas et moi: trois exemples...

1 **Tu achètes en ligne un livre sur la naissance du Rap. Les jours suivants, s'affiche sur ton compte *Instagram* une pub pour une compilation musicale des années 80.**

Décryptage : *un cookie installé sur la librairie en ligne a permis de te classer dans le profil « amateur de rap ». Un vendeur a payé une régie publicitaire récoltant ces profils un peu partout pour que sa pub de compilations leur soit envoyée.*

2 **Sur ton fil info, tu ne reçois que les infos liées aux e-sports et aux sorties de jeux vidéo.**

Décryptage : *à force d'étudier ce que tu lis, ton fournisseur d'info te connait bien et ne voudrait surtout pas t'envoyer sur d'autres pistes… Confortable, mais pas idéal si tu souhaites élargir tes horizons.*

3 **Tu utilises une application sympa. Elle souhaite un bon anniversaire à ton cousin.**

Décryptage : *les fabricants d'applis raffolent de ces données personnelles : contacts, calendrier, photos, données de géolocalisation, messages. Cette appli connait la date d'anniversaire de ton cousin et son mail et comme elle est sympa, elle lui présente ses vœux. Heureusement, parce que tu avais oublié…*

Juste pour vos yeux

Voici, en guise d'exemples, le nombre de mouchards qui s'affichent au compteur quand tu vas sur les sites suivants :

youtube.com

wikipedia.org

disneyplus.com

animedigitalnetwork.fr

jeuxvideo.com

geekjunior.fr

Regarde la petite vidéo réalisée par Savoir Devenir et l'INA

https://www.youtube.com/watch?v=P-3LYICRioQ

9+1 conseils pour naviguer tranquille

1. **Ne pas accepter en vrac tous les cookies ! Regarde la liste des cookies que tu vas accepter !**
2. **Installer sur ton navigateur des extensions « anti-mouchards », comme *Ghostery* ou *Privacy Badger***
3. **Activer l'option « do not track » ou « ne pas pister » disponible sur chacun de tes navigateurs**
4. **Supprimer régulièrement les cookies de ton navigateur, en ne conservant que ceux qui sont indispensables. Cela vaut aussi pour tes applications.**
5. **Penser à désactiver les fonctions de géolocalisation sur ton smartphone**
6. **Utiliser plutôt *Qwant*, un moteur de recherche qui ne trace pas**
7. **Préférer *Firefox*, un navigateur qui ne trace qu'au minimum**
8. **Diversifier tes services web. Par exemple, *Chrome*, *YouTube*, *Google* et *Gmail* appartiennent tous au groupe *Alphabet*. L'entreprise va alors collecter beaucoup d'informations sur toi.**
9. **Visionner ce webdoc :** *donottrack-doc.com/fr/intro*