

# Un été Sud-Ouest

À chaque jour, sa série

Tout au long de l'été, « Sud Ouest » vous offre un moment de détente. **LUNDI** : Sagas familiales. **MARDI** : Maisons d'ici. **MERCREDI** : En dehors des foules. **JEUDI** : Préparez vos mouchards !  **VENDREDI** : Balade œnotouristique. **SAMEDI** : Interdit au public. Passez un bel été « Sud Ouest » !

## Naviguez en paix, nous nous occupons du reste...

Internet a ouvert un gigantesque marché de collecte de données. Nos traces sont devenues le nouvel or noir des grandes firmes

**PRÉPAREZ VOS MOUCHARDS (5/6) :** Comment les nouvelles technologies trahissent nos faits et gestes. **DEMAIN :** Dans la série des balades œnotouristiques, le château Gravas, à Barsac (33).

YANN SAINT-SERNIN  
y.saint-sernin@sudouest.fr

En 2007, le responsable des procédures de sécurité dans l'armée américaine, le commandant Ray Ceralde, avait provoqué un tollé en encadrant l'utilisation d'Internet par les militaires. Parmi les informations susceptibles de compromettre la sécurité opérationnelle, l'officier citait les commandes de pizzas !

À ceux qui estimaient que seul un paranoïaque pouvait assimiler les habitudes alimentaires des militaires à du secret-défense, il proposait une autre lecture de ces informations : le 17 janvier 1991, les pizzerias autour du Pentagone avaient enregistré un pic de commandes venant du bâtiment d'Arlington. Quiconque accédait à ces données commerciales peu protégées et en apparence anodines pouvait en déduire qu'un nombre inhabituel d'agents restait tard ce soir-là. Et que le déclenchement de l'opération Tempête du désert était imminent.

Bienvenue dans l'ère du big data. Aujourd'hui, l'art d'extirper des connaissances de données personnelles grâce à des algorithmes s'est tant développé que les pizzas du Pentagone font figure d'aimables bluettes. Internet, que ce soit par les traces laissées par les internautes ou par les informations qu'ils déposent sur les réseaux sociaux, constitue un gisement de données dans lequel puisent à l'envi les publicitaires, les start-up, les géants du Net... et les agences de renseignement.

### Siphonnage au grand jour

Ce siphonnage se joue en partie en pleine lumière. Les politiques de confidentialité de Google ou Facebook, que presque personne ne lit, sont explicites. Par exemple, Google ne cache pas qu'il scanne les courriels sur Gmail. Facebook ou Instagram précisent que les données déposées sur ces réseaux sociaux leur appartiennent...

Le reste de la collecte fait appel aux cookies et aux mouchards. Les premiers sont des données déposées par un serveur sur nos navigateurs afin de les marquer ; les seconds reçoivent et envoient des informations sur ce que vous faites ou regardez. À l'origine, les cookies permettaient de faciliter la navigation. Mais ils sont aussi devenus des espions capables de tracer nos faits et gestes sur le Web.

### Nos traces numériques sont le vrai prix de la gratuité du Web

Ceux des grands sites comme Google ou Facebook, de par leur omniprésence sur la Toile, rendent possible un traçage massif. Récemment épinglé, Facebook parvenait même à déposer un cookie sur les ordinateurs d'internautes non abonnés au réseau social. Il permettait de les marquer à chaque fois qu'ils visitaient une page contenant le plugin Facebook (le bouton permettant de « liker » une page, présent sur la plupart des sites). Ou comment ces sympathiques icônes peuvent se transformer en chiens de garde rapportant à leur maître l'identité de ceux qui sont passés par là.

### La NSA aime Google

La puissance des cookies de Google n'a pas échappé à l'Agence de sécurité américaine (NSA) et à son équivalent britannique, le GCHQ. Dans les années 2010, tous deux se sont greffés sur le mécanisme de tracking (recherche et traçage) de Google, baptisé « cookie Pref », afin d'identifier et de pirater des cibles.

En 2013, la Commission nationale de l'informatique et des libertés (Cnil) a développé l'application CookieViz permettant de visualiser en temps réel les interactions entre un ordinateur, le site visité et des sites tiers. Appliquée à un site marchand réputé, on constate qu'il est connecté à une quinzaine de sites à qui il envoie des informations sur le visiteur : mesure d'audience, publicité, analyse des pages visitées...

Ces outils de profilage permettent aux sites de s'adapter à leurs visiteurs, notamment pour de la publicité ciblée. Avec des pratiques parfois à la limite de la légalité. Ainsi, sur certains sites de vente de billets d'avion, la Cnil a relevé une modulation du prix pro-



posé en fonction du site précédemment consulté. Un internaute provenant d'un comparateur de prix se voyait parfois offrir un prix d'appel plus attractif, mais avec des frais plus élevés...

### Données contre services

Grâce aux mouchards, certains sites de vente peuvent également connaître le matériel utilisé par les clients. Les utilisateurs d'Apple, réputés fortunés, se voient ainsi proposer des tarifs plus élevés. Plus fort encore : en 2012, en lui envoyant de la publicité personnalisée, la chaîne de supermarchés Target avait appris à un père que sa fille était enceinte avant que lui-même ne s'en rende compte. La chaîne avait tout compris grâce aux modifications de consommation de la jeune femme...

Désormais, nos traces numériques sont une manne pour qui sait les collecter. Publicitaires, commerçants, agences de renseignement, mais aussi assurances, ne tarissent pas d'intérêt pour leur potentiel. Elles sont le vrai prix de la gratuité du Web et de

### L'AVIS DE L'EXPERT

**ÉRIC FILIOL**, ancien agent de la DGSE, directeur du centre de recherche de l'ESIEA (École d'ingénieurs du monde numérique).

« Personne ne peut se dispenser de règles d'hygiène. Snowden a montré à quel point le profilage commercial peut basculer dans la surveillance administrative. Je recommande de bannir Internet Explorer ou Chrome au profit de Firefox en mode navigation privée avec le plugin Ghostery, qui bloque certains mouchards, et Self-Destructing Cookies, qui efface les cookies les plus intrusifs. Il faut régulièrement nettoyer ordinateurs et téléphones. La plupart du temps, alors qu'on croit les avoir détruites,

les données restent quelque part, comme dans les fichiers temporaires de Windows. Le logiciel CCleaner donne des résultats acceptables. L'enjeu n'est pas d'avoir ou non quelque chose à cacher. Il s'agit du droit fondamental à la vie privée. Aujourd'hui, de simples données de consommation peuvent très facilement indiquer votre religion, vos préférences sexuelles, voire vos opinions politiques. Il faut envisager les choses sous l'angle de la responsabilité collective, car cette surveillance fonctionne sur des modèles statistiques que chacun alimente. En me protégeant, je protège aussi les autres. »

son formidable développement : données contre services. Combien votre navigation rapporte-t-elle à cette industrie ? La valorisation des sociétés livre des indices. LinkedIn, la start-up aux 433 millions de CV en ligne, a récemment été vendue 16 mil-

liards de dollars à Microsoft... En 2012, l'application PrivacyFix estimait la valeur des données transmises par un internaute. En un an, selon cette application, un Européen pouvait rapporter entre 10 et 600 dollars à Google.