Protéger nos données

par Sylvain Faure,
Professeur de mathématiques
Collège Henri Pourrat à Ceyrat

Lorsqu'on entend parler de protection des données, on pense tout d'abord aux données exploitées à notre insu. Il nous faut cependant **penser à celles que nous communiquons de notre plein gré sur le réseau mondial**. Il ne faut pas non plus oublier les fichiers que nous avons produits.
Évacuons cette dernière partie en disant que seules les sauvegardes fréquentes garantissent de ne pas perdre nos précieux documents, photos, etc. Les stocker dans le *cloud* garantit une synchronisation continue mais revient la plupart du temps à céder la propriété de nos créations à l'hébergeur (et le service n'est gratuit qu'en-deçà d'une certaine quantité de données)… Faire régulièrement des copies sur des supports de stockages[1] personnels est plus contraignant mais permet de garder le contrôle. Utiliser les deux méthodes selon les besoins est sans doute le plus pratique.
Revenons maintenant à nos données personnelles, qu'elles soient collectées de manière plus ou moins opaque ou que nous les mettions nous-mêmes à disposition...

Une collecte discrète

Vous prendrez bien un cookie ?

Visiter un site web, ce n'est pas comme lire un journal ou feuilleter un magazine, action entièrement maîtrisée par le lecteur ; sur le web, pour afficher correctement les textes et médias, le site a besoin d'informations sur notre appareil.

Au temps - pas si lointain - des accès à bas débit, les informations recueillies permettaient au site d'identifier un internaute déjà venu et ainsi d'utiliser un affichage adapté et plus rapide, ce qui était précieux pour l'utilisateur facturé à la durée de connexion. Pour pouvoir reconnaître un visiteur familier, le site marquait sa machine en y faisant inscrire par le navigateur un petit fichier sur le disque dur. Ces petits fichiers, traces de l'historique de navigation, sont les ***cookies***.

Avec le développement de l'internet, l'apparition des publicités et du commerce en ligne, ces cookies ont pris de plus en plus d'importance. Les cookies tiers sont apparus et se sont multipliés : au lieu d'être créés (sur notre machine) par le site visité, ceux-ci, comme leur nom l'indique, le sont par des sites tiers, des partenaires du site visité. On comprend bien que, dès lors, faciliter l'affichage des pages web n'était plus l'objectif, il s'agissait de **mieux comprendre le comportement de l'internaute**, afin de lui proposer des publicités de plus en plus ciblées susceptibles de déclencher des achats.
Les navigateurs se sont adaptés, proposant la navigation privée. Utiliser une fenêtre de navigation privée permet de ne pas faire apparaître les pages visitées dans l'historique de navigation et d'être sûr que d'éventuels cookies seront effacés à la fermeture de la fenêtre (rappelons que procéder ainsi ne garantit en rien l'anonymat. ; en effet, les sites visités ont accès aux adresses IP des visiteurs et les fournisseurs d'accès archivent celles des sites auxquels ils nous connectent.).
La législation elle aussi a évolué.

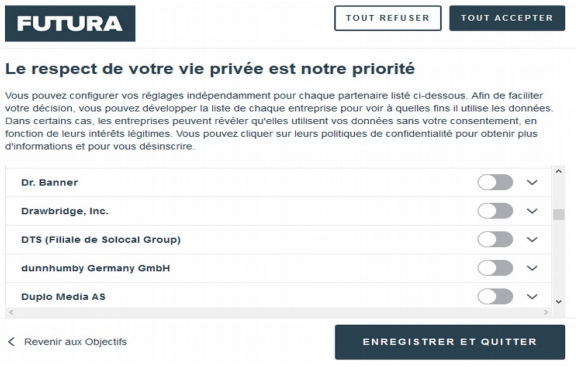
1 Cartes mémoires, clés USB, disques durs, DVD…

RGPD

Le Règlement Général sur la Protection des Données est un règlement européen entré en vigueur le 25 mai 2018, règlement qui s'applique aux entreprises et organisations situées ou non dans l'Union européenne. Outre les différents droits qu'il donne aux citoyens européens, il oblige en particulier les sociétés et organismes qui collectent des données sur ceux-ci à obtenir d'abord leur **consentement explicite** puis à **protéger** les informations recueillies en utilisant des mesures de sécurité.

Malheureusement, tous les acteurs du secteur ne sont pas en conformité avec le RGPD… Il est aisé de voir si un site web l'est ou pas. Il suffit de vérifier que la première fois que l'on visite un site, une fenêtre avec un avertissement du type « *Le respect de votre vie privée est notre priorité* » s'ouvre, invitant à accepter ou refuser les cookies. Pour vérifier si un site déjà visité est conforme, on peut utiliser une fenêtre de navigation privée.
Cependant, l'apparition d'une telle fenêtre ne garantit pas la bonne volonté affichée dans le message. En effet, si le bouton pour accepter est toujours bien visible, le refus des cookies peut s'avérer difficile. Certains sites jouent le jeu (voir l'exemple ci-dessous du site FUTURA) , il y est ainsi facile de tout refuser, et d'en apprendre plus sur l'utilisation des données recueillies et le nombre impressionnant de sites tiers à qui elles sont transmises.

Un exemple de site transparent : le site FUTURA



Pour empêcher ceux qui ne respectent pas la législation de récolter et monnayer des informations sans notre « consentement éclairé », des solutions existent. La plus simple est d'ajouter à son navigateur une extension qui limite la collecte des données de navigation (par exemple : uBlock Origin, Ghostery ou AdBlock Plus) ; de plus, ce type d'extensions bloque ou filtre les publicités, rendant ainsi la navigation plus fluide.

Les données fournies de plein gré

Réseaux sociaux, commerce en ligne...

Les réseaux sociaux hébergent également quantité d'informations personnelles. Les photos partagées un jour de fête « ressortent » parfois des années plus tard notamment par les recruteurs qui consultent les profils des candidats sur les réseaux sociaux. Mais, outre le fait qu'elle peut un jour se révéler compromettante, une photo s'accompagne par défaut de données telles que, par exemple, l'appareil utilisé, la focale utilisée mais aussi l'horodatage et la géolocalisation. Géolocalisation accessible à des applications sur smartphones et qui - à moins de s'y opposer - est archivée (voire publiée) et analysée, y compris par des applications tierces.

Pour utiliser certains services en ligne (consultation de factures, vidéos, musique, etc.) ou pour acheter sur internet, il faut ou bien créer un compte sur le site commercial ou bien utiliser une identification par un site tiers. Dans les deux cas, des informations personnelles sont

transmises (*a minima* pour se faire livrer un colis un numéro de téléphone et une adresse postale), informations fournies de plein gré.
Les sites de commerce ayant peu de clients sont réputés comme étant susceptibles de présenter des failles de sécurité en particulier au niveau de la gestion des mots de passe, ce ne sont pas les seuls. On est pourtant bien obligé d'accorder tacitement notre confiance au site, quel qu'il soit ; ceci étant, on peut limiter les risques en choisissant – comme précaution élémentaire – un mot de passe robuste.

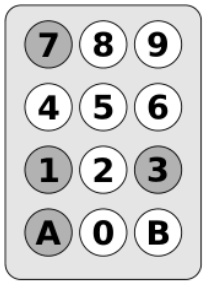
Mots de passe

Le choix d'un mot de passe s'effectue lors de la création du compte, souvent sans réflexion préalable alors qu'il faudrait toujours avoir à l'esprit trois principes :

→ plus un mot de passe est long, plus il est robuste (8 caractères c'est moins bien que 12, 12 c'est moins bien que 16, etc.) ;

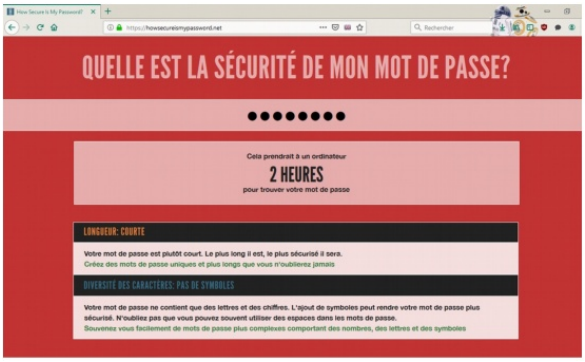
→ plus il est complexe, plus il est robuste (utiliser un mélange de lettres majuscules, de lettres minuscules, de chiffres, de caractères spéciaux et accentués est beaucoup plus sûr que de n'utiliser que des lettres minuscules ou, pire, que des chiffres) ;

→ le mot de passe ne doit pas être facilement devinable (voir ci-dessous).



Supposons que le digicode ci-contre ouvre une serrure en tapant un code formé de 4 chiffres suivis d'une lettre. Initialement, il y a 10 × 10 × 10 × 10 × 2 = **20 000** possibilités et le code est donc difficilement devinable.
Mais à force d'entrer le code, **les traces de doigts** permettent de savoir que seuls les chiffres 1, 3, 7 et la lettre A sont utilisés, l'un des chiffres étant donc répété.
Ainsi, si le 1 est répété, les seules possibilités sont : 1137A, 1173A, 1317A, 1371A, 1713A, 1731A, 3117A, 3171A, 3711A, 7113A, 7131A, 7311A, soit 12 possibilités auxquelles s'ajoutent 12 possibilités pour les codes où 3 est répété et 12 possibilités pour les codes où 7 est répété.
En tout, **36** possibilités seulement et le code d'entrée est devenu aisément devinable.

La connexion au serveur de l'établissement pour lequel le mot de passe est la date de naissance rend facile l'usurpation de compte. Les élèves doivent être sensibles à cet aspect, certains élèves utilisent ainsi très souvent des références à leur prénom et date de naissance pour créer un mot de passe (exemple : richard12*2002).
Il existe des logiciels permettant de générer des mots de passes robustes (et de les stocker). Il suffit juste de s'assurer qu'ils créent le mot de passe en local (sur l'appareil de l'utilisateur) et non à distance.
Une fois les mots de passe trop faibles évités, il faut veiller à leur sécurisation. Ainsi par exemple, si l'on choisit de stocker le mot de passe créé sur l'ordinateur, il conviendra de ne jamais laisser l'appareil être utilisé sans surveillance, à moins de le verrouiller. Certains spécialistes de sécurité informatique conseillent d'écrire le mot de passe sur un papier conservé en lieu sûr, d'autres de le renouveler de temps à autre, pratiques n'ayant pas que des avantages.



https://howsecureismypassword.net/

Perspectives

D'un côté, on nous annonce que la fin des mots de passe est pour bientôt[2] grâce à la généralisation de nouveaux protocoles de sécurité et à la biométrie. De l'autre, il est prouvé que la simple photographie d'une personne faisant le « V » de la victoire, prise à 5 mètres de distance, a permis de tromper un lecteur d'empreintes digitales[3]. D'ici à ce que les mots de passe disparaissent, il reste plus prudent pour l'instant de les sécuriser au maximum.

2 *Dépassés, les mots de passe vont disparaître* sur futura-sciences.com
3 *Protection des données Alerte au piratage biométrique*, *Sciences et Vie* 1195, Avril 2017, p 38-42