1168

Internet : la vie privée en danger ?

Frédéric Dempuré, ancien chargé d'enseignement à l'université de Poitiers

Depuis la sortie de *Windows 10* la presse se déchaîne sur la firme de Redmond au motif que le dernier système d'exploitation (OS) de *Microsoft* n'aurait de cesse de nous espionner. Une accusation en partie fondée mais néanmoins un peu injuste. Car si *Windows 10* est en effet programmé pour regarder derrière notre épaule, il a fallu qu'il joue des coudes pour s'y faire une place tellement il y avait foule. Petit tour des programmes indiscrets et des actions à mener pour tenter de les faire taire.

« Quand c'est gratuit, c'est toi le produit »

Inutile de tourner autour du pot. Tout le monde peut comprendre que créer un programme informatique, même aux fonctions simples, nécessite des compétences, du matériel et du temps, donc de l'argent. Un retour sur investissement est ainsi, fort logiquement, attendu. L'achat en ligne n'étant pas le modèle économique le plus populaire sur Internet, des solutions alternatives de paiement indirect se sont développées. Et parmi elles, s'est imposée la publicité ciblée, c'est-à-dire celle adressée à une personne en tenant compte de son mode de vie et de ses habitudes de consommation. Sans parler du *Big data*, le nouvel Eldorado des géants du Net, dont la matière première n'est autre que les données personnelles des internautes et des mobinautes (personnes connectées via un smartphone). En résumé, comme aiment à le répéter les spécialistes du marketing en ligne « quand c'est gratuit, c'est toi le produit ». Qu'on se le dise.

Le cas *Windows 10*

Si *Windows 10* est un petit fouineur, contrairement aux autres, il n'en fait pas mystère. Il suffit ainsi de se plonger dans ses conditions d'utilisation pour savoir à quelle sauce l'on va être mangé. En gros, par défaut, la firme de Redmond va récupérer différents types d'informations afin, notamment, d'améliorer les services qu'il nous rend. Sont ainsi transférés sur les serveurs de *Microsoft* ou d'entreprises partenaires, les historiques de navigation, les mots de passe permettant de se connecter à des services en ligne ou encore les listes de favoris et les choix de personnalisation du système d'exploitation. Toutes ces données vont nourrir le système d'auto-complétion (système de suggestion de sites déjà visités) de la barre de recherche d'*Edge*, le nouveau navigateur ou encore nous permettre d'avoir toujours le même environnement de travail, quel que soit le terminal utilisé. *Cortana*, l'assistant virtuel est lui aussi un grand pourvoyeur de données personnelles. Ainsi, pour fonctionner correctement,

© MERIEL JANE WAISSMAN - ISTOCK

c'est-à-dire mieux comprendre nos attentes, voire les anticiper, il doit bien nous connaître (habitudes, localisation, préférences, goûts, listes de contacts et d'amis…). Des informations que l'assistant nous réclamera lors de son installation mais aussi qu'il complètera, au fil du temps, en se nourrissant des traces laissées par notre utilisation de *Windows 10*. Bien entendu, ces différentes données seront utilisées par *Microsoft* ou ses partenaires pour, *a minima*, nous adresser des publicités ciblées.

Et les autres OS ?

Dans cette affaire de nids d'espion, Apple joue également un rôle. L'éditeur du deuxième OS le plus utilisé en France a récemment essuyé la colère de ses utilisateurs. En octobre dernier, suite au lancement de son OS X Yosemite, certains utilisateurs ont affirmé que le moteur de recherche unifié du système d'exploitation *(Spotlight)* transmettait notamment à *Apple* (mais pas seulement) « les données de localisation de leurs utilisateurs et les termes de leurs recherches ». S'en est suivie la création d'une pétition exigeant que la firme à la Pomme corrige le tir. À ce jour plus de 40 000 personnes ont signé le texte. En fait, du côté des OS, seul *Linux*, le système d'exploitation gratuit et participatif, semble respecter la vie privée de ses utilisateurs.

Les jolies applis

Qu'elles soient gratuites ou payantes, les applis que l'on aime installer sur nos smartphones et autres tablettes n'hésitent pas non plus à nous observer par le trou de la serrure. Une situation sur laquelle la Cnil s'est d'ailleurs penchée à plusieurs reprises. Avec l'aide de l'Inria (Institut national de recherche en informatique), la Commission dite « Informatique et Liberté » a créé une appli destinée à espionner les applis qui nous espionnent. Baptisée *Mobilitics*, ce petit programme a été installé pendant plusieurs mois, fin 2014, sur les smartphones d'un groupe de volontaires. Au final, la Cnil constate que plus de la moitié des applis étudiées transmettent à leurs éditeurs des identifiants du téléphone. Des identifiants qui permettront, notamment, l'envoi de publicités ciblées. Dans son rapport, la Commission met également en évidence que les données de localisation intéressent près d'un tiers des appli. Jusque-là rien d'anormal, hormis, précise la Cnil, « l'intensité et la fréquence d'accès à cette information par certaines applications ». À titre d'exemple, le rapport cite le cas d'une appli qui bien que non spécialisée dans le calcul d'itinéraire a en trois mois seulement accédé pas moins d'un million de fois aux données de localisation de son utilisateur. Plus embêtant, la Cnil précise que certaines applications associées à l'OS et donc impossibles à désinstaller, comme *Play*, le magasin d'applis d'*Android*, font partie des pires espions. À méditer.

Quoi faire ?

Si l'on peut toujours ressortir son vieux *Nokia 3310* et refuser de passer à *Windows 10*, chacun sait que ce choix n'est pas tenable bien longtemps. Certes, opter pour *Linux* peut être tentant, mais malheureusement tous les logiciels métiers sont loin d'être compatibles avec l'OS collaboratif. Alors en attendant, il est conseillé, du moins à ceux qui trouvent désagréables d'être espionnés, de désactiver certaines fonctionnalités de leurs OS et de leurs navigateurs. Par exemple pour *Windows 10*, il faut se rendre dans les paramètres de confidentialité du menu « Démarrer » pour désactiver la géolocalisation ou encore cliquer sur le bouton « arrêter de me connaître » dans les paramètres de l'assistant Cortana. Les fonctionnalités d'envoi de données peuvent également être neutralisées via le menu de paramétrage du navigateur *Edge*. Il en va de même pour le navigateur *Chrome* de *Google* (menu « paramètres / Confidentialité »). À noter que d'un point de vue vie privée, le navigateur Firefox est, de l'avis général, bien plus respectueux que ses concurrents. Enfin, concernant les applis, il est conseillé de bien vérifier quelles autorisations de transfert de données doivent être données pour permettre leur installation. En outre, même si la mémoire des smartphones et des tablettes ne cesse de croître, il convient de désinstaller toute application qui n'est pas régulièrement utilisée.