

Pourquoi les amateurs de porno en ligne feraient bien de se préoccuper sérieusement du risque d'étalage de leurs habitudes en place publique



Les systèmes de tracking mis en place par les sites porno et les navigateurs ne permettent plus aux usagers de protéger leur anonymat, même lorsque ces derniers visionnent des vidéos en navigation privée.

Avec Franck DeCloquement
Avec Frédéric Mouffle

Atlantico : Un ingénieur américain, Brett Thomas a estimé sur son blog que "si vous regardez du porno en 2015, même en navigation privée, vous devez vous attendre, à un moment donné, à ce que l'historique de vos vidéos soit rendu public et rattaché à votre nom". Quel est le raisonnement à l'origine de cette affirmation ?

Franck DeCloquement : Les prédictions d'Orwell restent plus que jamais d'actualité. Nous le vérifions chaque jour un peu plus. **Après l'œil inquisiteur de son emblématique « Big Brother », voici venir les affres du « Your Porn Is Watching You » pourrait-on dire !** Et ceci, bien entendu, en raison d'une multitude d'informations personnelles qui sont collectées à tout moment à partir d'un cycle de navigation sur la toile, par les sites incriminés, puis renvoyées dans la foulée à de très grandes entreprises consommatrices de « BIG DATA » à haute valeur ajoutée. A l'image de Tumblr, AddThis ou Google.

Ainsi, dans son article en ligne publié sur MotherBoard, l'un des sites de Vice Magazine, Brett Thomas – développeur de logiciel de son état – nous explique que **les sites pornographiques parmi les plus visités de la planète (à l'image de XHamster, Pornhub, YouPorn, Redtube, Xvideos, XXNX, etc.), utilisent tous des outils de « tracking », afin de transmettre les données collectées à un nombre significatif de sociétés destinataires.** Selon les estimations du même Brett Thomas, 88% des 500 sites pornographiques les plus visités auraient des éléments de suivi installés permettant en outre de révéler les détails obscènes de chaque vidéo visionnée... Aimable perspective !

Frédéric Mouffle : Nous n'apprenons rien de nouveau quand à la commercialisation des données de navigation. En revanche, ce qui est intéressant dans les affirmations de Brett Thomas c'est qu'elles semblent un peu fantaisistes, dans la mesure où aucun nom d'utilisateur n'a jamais été associé à des données de navigation.

Si les sites pornographiques, comme d'autres, utilisent des outils de suivi et envoient certaines données collectées à des organismes tiers, identifier l'utilisateur nommément peut-il se faire aussi aisément que le sous-entend Brett Thomas ?

Frédéric Mouffle : Les sites internet dit "commerciaux" fonctionnent à peu près tous sur le même modèle. Les données collectées sur

les sites pornographiques sont revendues à des régies publicitaires en vue de générer de la "publicité ciblée". A aucun moment Brett Thomas nous explique comment l'identité d'une personne peut être dévoilée à partir de ses données de navigation ! C'est légalement impossible, les deux informations ne sont tout simplement pas liées. Il faudrait pour cela utiliser des méthodes de "hacking" pour déterminer l'identité des utilisateurs.

Franck DeCloquement : Nul ne pourrait dire qu'il n'était prévenu. **Comme chacun le sait, la majorité de nos gestes en ligne sont épiés, captés, classés puis stockés dans l'attente d'être revendus à des organismes tiers, en effet.** Et vos historiques d'affichages ou de visites à caractère pornographique, sont attachés à votre nom dès lors que vous vous y adonnez. Certaines études neuroscientifiques nous révèlent même, que consommer très régulièrement de la pornographie en ligne augmenterait substantiellement nos appétits sexuels. **Mais l'aficionado avide de spectacles pornographiques filmés craint par-dessus toute chose, l'humiliation publique qui consisterait à voir fuiter la nature de ses inclinaisons intimes, à l'extérieur de sa sphère privée.** Car certaines pratiques sexuelles sont aussi passibles de très graves sanctions – et parfois même de sévices insoutenables – pouvant aller jusqu'à la peine de mort sous d'autres latitudes. Et ceci, compte tenu des mœurs parfois rétrogrades en vigueur dans de très nombreux pays du globe, où le respect des droits humains fondamentaux ne pèse pas lourd. En conséquence, les données personnelles qui pourraient être exposées sur la place publique dans un tel contexte, pourraient également mettre en danger la vie d'autrui. Et cela très concrètement...

Le fait d'être en navigation privée peut-il protéger les utilisateurs de ce tracking ?

Frédéric Mouffe : La navigation privée protège correctement l'utilisateur même si certaines données sont collectées, dans un but de fonctionnalité (dialogue "machine-machine"). Votre adresse "IP" permet une localisation de l'utilisateur afin d'optimiser les requêtes vers le site internet visité.

Néanmoins, dès lors que vous naviguez sur un site "X", un certain nombre de fenêtres publicitaires s'ouvrent automatiquement, et parfois en mode "non privé". Ce qui peut avoir pour conséquence l'accès à plus d'information qu'en navigation en "mode privé". L'utilisation d'un bloqueur de Pop-up tel que "Adblock" limite drastiquement l'ouverture des Pop-up indésirables. Quand le dispositif est de surcroît couplé à une connexion VPM, votre niveau de sécurité sera d'autant plus important.

Franck DeCloquement : Comme chacun le sait, les moteurs de recherches sont ainsi capables de guider individuellement chaque utilisateur dans ses recherches – et corrélativement de le pister en retour – afin de le mener tout droit vers ses préférences personnelles, en fonction de ses inclinaisons sexuelles propres. Les habitudes de navigation des amateurs de pornographie en ligne ne sont donc pas aussi secrètes qu'ils peuvent le penser. Et de très nombreux experts en sécurité informatique s'accordent à le dire, même si par ailleurs leurs conclusions ne sont pas toutes en accord avec les propos tenus par Thomas dans son billet. **Dés lors, Et même si l'amateur éclairé à eu la présence d'esprit de se mettre préalablement en mode « navigation privée »... Peine perdue. Il sera tout de même tracé.** Sans compter qu'en cliquant le plus simplement du monde sur une vidéo X lambda, un internaute envoie des données qui peuvent être utilisées pour identifier très classiquement son ordinateur, comme son adresse IP. Même si certains sites assurent publiquement qu'ils n'enregistrent pas leurs utilisateurs « non-inscrits » pour des raisons évidentes de marketing commercial, ils partagent tout de même leurs données – ainsi que les URL des vidéos que leurs visiteurs ont visionnées – à d'autres entreprises tierces, pourvoyeuses de subsides.

Les sites pornographiques n'ont-ils pas intérêt à bien/mieux protéger les données de leurs utilisateurs ?

Franck DeCloquement : Si l'on en croit les statistiques que l'IFOP publia en 2014, 26% des Français admettaient avoir visionné un film pornographique au cours des trois derniers mois qui précédaient cette étude. **Aux Etats-Unis, 30 millions d'américains regarderaient régulièrement des films pornographiques en ligne, selon une autre enquête citée par le célèbre Wall Street Journal.** Mais seulement 12% d'entre eux admettaient le faire en 2013. Pudeur oblige... Eu égard à cette formidable manne financière virtuelle, il semble évident que les sites pornographiques ont tout intérêt à garantir la confiance, à singer la confidentialité et à bichonner leurs visiteurs épisodiques. Très souvent, les plus soupçonneux. L'objectif manifeste étant de ne pas trop effrayer le chaland et le détourner de ses habitudes de consommation compulsive. C'est aussi le prix à payer pour sécuriser les âmes en peine, et profiter allègrement des subsides qu'offrent – à qui sait s'en emparer discrètement pour les faire fructifier – leurs vices privés.

Frédéric Mouffe : Le marché de la pornographie – et notamment aux Etats-Unis – représente 12 milliards de dollars de chiffre d'affaires en 2006. Les sites internet n'ont aucun intérêt à mettre dans l'embaras leurs utilisateurs au risque de perdre des parts de marché, en effet.

Qui pourrait vouloir diffuser ce genre de données et à quelles fins ?

Franck DeCloquement : On peut aisément imaginer que des hackers à leur propre solde, ou employés par des puissances étrangères, ou des groupes criminels organisés, pourraient aisément mettre à profits certaines collectes de données confidentielles à caractère pornographique, ou certains trackings individuels, pour profiter de la situation. Mais aussi pour retourner des individus ciblés, ou en déconsidérer d'autres afin de les rendre plus vulnérables, plus malléables. Et ceci, quel que soit l'effet final recherché en définitive (chantage, compromission, discrédit, défection, retournement, etc.). Dans ce registre, l'imagination criminelle est sans limites comme chacun le sait.

Frédéric Mouffe : Si les données existent bien, il y a beaucoup de personnes, de groupes politiques ou religieux activistes qui seraient très intéressés par la diffusion sauvage de ces informations ciblées. Et ceci dans le but évident de conforter leurs idéologies en faisant pression. Il faut aussi se rappeler qu'aux Etats-Unis où le puritanisme est toujours très prégnant, plusieurs organismes très actifs luttent frontalement – et avec des moyens très offensifs – contre l'industrie de la pornographie. Pour mémoire, l'homme d'affaires Larry Flint en avait fait les frais ; dès 1978 ; en se faisant tirer dessus à bout portant par un extrémiste... Le risque de manœuvre politique est donc bien réel et relativement élevé, et reste une valeur sûre pour discréditer un éventuel candidat, éligible à un poste important.

Le scénario de Brett Thomas est-il alarmiste ? Comment se prémunir afin de ne pas voir de telles données révélées sur la place publique ?

Frédéric Mouffe : Ces données n'existent pas dans la forme évoquée, c'est-à-dire un "historique lié" à l'identité d'une personne en propre. Le scénario est évidemment alarmiste mais aucune preuve ni démonstration n'a été faite à ce jour. Ces spéculations n'engagent donc que leur auteur. Mais le "buzz" généré par cette affaire a d'ores et déjà réussi.

Franck DeCloquement : Très schématiquement, il faut bien considérer que les propos tenus par Brett Thomas le sont dans un contexte américain. **Les normes comportementales, mais surtout les conditions du respect de la vie privée ne sont pas les mêmes en Amérique qu'en Europe.** Le modèle Google en a d'ailleurs fait les frais, compte tenu de son obligation à procéder à l'effacement de certaines données personnelles qui seraient jugées peu gratifiantes par un utilisateur lambda, mais ressortissant de l'Union européenne. Ceci fut strictement stipulé au géant américain dans le récent arrêt de la Cour de justice de l'Union européenne (CJUE) depuis la publication de sa décision en date du 13 mai 2014. Occasionnant dans la foulée de profondes répercussions pour les moteurs de recherche en Europe. Nous savons tous par ailleurs que les accords TAFTA (Trans-Atlantic Free Trade Agreement) de libre échange « euro-atlantique » en cours de négociation, ambitionnent sur le fond d'harmoniser par d'autres moyens (que d'aucuns qualifieraient de détournés), certains modèles de comportement en matière de consommation, sur celui de nos voisins anglo-saxons. Pour autant, les européens ne semblent pas disposés à se laisser faire à l'heure où ces lignes sont écrites. Et plus spécifiquement encore, sur le respect de la vie privée. Rien ne semble joué, donc.

Dés lors, qui vivra verra !

Propos recueillis par Carole Dieterich