Les cookies, PJS3 - Groupe 207

Le monde d'internet a une particularité quasi voir totalement unique : son modèle économique est basé principalement sur la gratuité des services. Cependant, les entreprises d'internet devaient pouvoir payer les serveurs, les employés… Afin de remédier à ce problème, une solution a été trouvée : c'est la publicité. En récoltant certaines données sur les utilisateurs de leurs sites, ils pouvaient garantir à d'autres entreprises l'efficacité et l'utilité de financer des publicités sur ces sites. En connaissant leurs utilisateurs, ils ciblent les publicités qui vont convenir le plus aux intérêts de ces derniers, en conséquence, les pubs sont plus efficaces.

Pour ce faire, on utilise des traceurs, plus communément connues sous le nom Cookies qui contiennent des données relatives à votre activité sur un site. Il s'agit de données téléchargées sur votre machine (ordinateur, téléphone…) qui renseignent sur votre activité, parfois de manière très précise comme notamment le mouvement de votre souris, le temps passé à chaque pixel de votre écran… D'abord créées pour un but utile (garder des données pratiques pour un meilleur maintient du site), elles vont ensuite être utilisées pour collecter ces données puis s'en servir comme argument commercial.

Il se pose ainsi un problème : Quels sont les dangers d'une telle technologie et quelles sont les solutions mises en rigueur afin de protéger les internautes, et notamment leur vie privée ?

Nous aborderons ce sujet en deux grandes parties. On évoquera d'abord la partie éthique et relative aux dangers pour l'utilisateur, sa vie privée... Puis on parlera plus en détail des juridictions prises vis-à-vis des traceurs et de la protection des données internautes au niveau national et international.

Si les cookies ont avant tout été créés pour l'aspect pratique que cela pouvait apporter aux sites quant à la sauvegarde des identifiants des utilisateurs et de leur habitude sur ces derniers, les cookies ont rapidement attiré l'œil d'un autre domaine qui est celui du commerce. L'utilisation originelle des cookies a par conséquent grandement été détournée et représente aujourd'hui une source de revenue considérable pour les gérants de la majorité des sites. Elle permet aux marchands d'exposer leur publicité chez un public d'internautes très ciblés dont les données personnelles et les préférences de navigation ont été données via les cookies qu'ils acceptent sans s'en rendre compte. Leurs données personnelles sont vendues à leur insu. Outre le fait que cela pose un questionnement sur l'aspect éthique et moral de la situation, cela peut surtout engendrer des risques et des dangers réels quant à la vie privée et à la sécurité des internautes.

Le premier danger qui peut survenir et qui paraît être le plus risqué est celui du hacking. Effectivement, cela est relativement aisé pour un hacker confirmé d'obtenir des informations privées et stockées dans des cookies étant donné que ces

derniers naviguent et circulent dans l'internet quasi librement et sont constamment en mouvement. Ainsi, le hacker n'a qu'à intercepter le fichier lors de sa transmission et il sera désormais dans ses mains. Cela engendrera par la suite des cyberattaques de sites en masse grâce aux informations que les cookies donneront ou alors la mise en application de chantages destinés aux utilisateurs des sites internet qui risquent de voir leurs données personnelles fuiter.

Le deuxième réel danger est l'espionnage de la population dirigé par des organisations publiques appartenant pour la plupart à l'État. L'histoire d'espionnage de masse la plus médiatisée et controversée du monde et celle du NSA qui avait exploité entre autres les cookies afin de surveiller la vie des internautes ciblés et de surveiller toutes leurs navigations. Cette technique permet y compris de prendre le contrôle du PC d'une personne ciblée afin d'y extraire toutes les données s'y affilient. Cette histoire fut publiée par le très célèbre Edward Snowden, ancien employé chez le NSA.

En vue des problématiques abordées précédemment, il a rapidement été nécessaire de réglementer l'utilisation des cookies et autres traceurs. Selon la CNIL, les cookies couvrent plusi²eurs choses : Les cookies HTTP, Flash, le résultat du calcul d'une empreinte unique du terminal dans le cas du "fingerprinting", les pixels invisibles ou enfin "*tout autre identifiant généré par un logiciel ou un système d'exploitation (numéro de série, adresse MAC, identifiant unique de terminal (IDFV), ou tout ensemble de données qui servent à calculer une empreinte unique du terminal (par exemple via une méthode de « fingerprinting »)*" (source : CNIL).

Le 6 Janvier 1978, la loi **n°78-17** est entrée en vigueur, elle a permis d' entamer une législation concernant l'informatique en général. Incomplète face à une technologie qui évolue de plus en plus rapidement, elle sera modifiée via la loi **n°88-227** du 11 mars 1988, ou via la loi **n°2004-801** du 6 août 2004 qui imposera à certaines entreprises de se conformer à la loi, notamment en matière de protection des données utilisateurs. Le 5 décembre 2013, la CNIL frappa un grand coup en publiant la délibération **n°2013-378** portant principalement sur les cookies qui va entraîner une modification de la loi de 1978 permettant enfin une législation plus claire et efficace vis-à-vis des cookies.

De plus, en 2016, l'UE a adopté le RGPD (Règlement Général sur la Protection des Données) visant à réglementer l'utilisation des données des utilisateurs au niveau européen. Celui-ci s'applique pour toutes les entreprises européennes ou les entreprises qui traitent les données de citoyens européens. Le RGPD précise qu'on doit donner son consentement pour que l'entreprise puisse manipuler nos données, il précise aussi que "*La personne concernée a le droit de retirer son consentement à tout moment. Le retrait du consentement ne compromet pas la licéité du traitement fondé sur le consentement effectué avant ce retrait. La personne concernée en est informée avant de donner son consentement. Il est aussi simple de retirer que de donner son consentement*".

Enfin, la loi n’est pas toujours en faveur des internautes, en effet, l’ordonnance **n°2018-1125** autorise à l'État de collecter et d’utiliser nos données sans notre consentement.

Les traceurs sont des outils d’une praticité incontestable pour les sites internet et leur création ont réellement permis d’améliorer l’expérience de navigation des internautes. Cependant, son utilité seconde concernant le commerce de données sur le net représente aujourd’hui un sujet très controversé au sein du débat sur la vie privée et de la préservation des données personnelles. Les risques sont nombreux comme le piratage ou l’espionnage. De ce fait, des lois ont évidemment dû être mises en place pour limiter la liberté des organisations numériques à manipuler leur stock de données privées comme bon leur semble et à protéger de façon très sérieuse ces dernières au risque d’être victime de représailles. Malgré cela, les risques liés à cela peuvent devenir irréversibles, étant donné la population massive que cela touche. Nous pouvons dès lors nous demander ce qui se passerait si une multinationale comme Google, YouTube ou bien encore Facebook, sites utilisés par des milliards de personnes par jour, finissaient par se faire pirater leurs cookies, et donc une partie de leur donnée comprenant celles des internautes et de la population mondiale. Enfin, le danger de la surveillance étatique abusive (Big Brother) est de plus en plus évoqué au vu de l'actualité, notamment en Chine ou aux Etats-Unis...

Membres du groupe :

BERTRAND	Baptiste	207
BORGES	Ludovic	207
HASSAINE	Ilyes	207
H’MIDA	Eymen	207
MAHDJOUBI	Bilal	207