15 août 2020
Big Brother

Comment Facebook et les géants de la Silicon Valley nous manipulent pour que nous leur abandonnions toujours plus de données privées

Les plateformes de réseautages sociaux manipulent nos choix en utilisant des "Dark Patterns" pour nous inciter subrepticement à divulguer davantage de données personnelles.

Avec Franck DeCloquement

Atlantico : La récolte des données personnelles par les grandes plateformes sociales du Web, est au cœur même de leur modèle économique. Mais par quelles astuces secrètes ces réseaux sociaux tentent-ils encore aujourd'hui de nous soutirer toujours plus d'informations personnelles, de manière non éthique, à l'image des fameuses « Dark Patterns » ?

Franck DeCloquement : La récolte, l'exploitation et le traitement des données personnelles sont devenus en l'espace de quelques années une question centrale dans le développement de projets numériques. « L'UX design » consiste par exemple à penser et à concevoir un site web, mais de manière à ce que l'expérience utilisateur soit la meilleure possible. Reste cependant à définir dans le contexte hyperconcurrentiel actuel, ce qu'est une « bonne » expérience utilisateur ! Et si l'enjeu de l'éthique semble clair pour beaucoup, certains relèvent néanmoins la contradiction qui se fait jour entre la volonté de développer un produit « pour un client » (le plus souvent en très forte demande de données), et l'expérience de « l'utilisateur » lui-même.

Un article fort intéressant paru très récemment dans Wired, nous explique au demeurant assez clairement par le menu, les ressorts de ce paradoxe apparent, et ses conséquences parfaitement délétères pour nos données personnelles. Sous la plume aiguisée d'Arielle Pardes, son texte nous rappelle qu'en 2010, l'Electronic Frontier Foundation en avait plus qu'assez de l'interface proposée à ses clients par Facebook. Car cette plateforme avait la réputation ancrée de rendre très peu accessible pour ses utilisateurs, le contrôle de leurs paramètres de confidentialité. Et cela, pour une raison assez simple : les exigences inhérentes du secteur du courtage de données. Car lorsque vous utilisez un service (par exemple une carte de fidélité de magasin), la présence de très petits caractères cachés dans les conditions générales d'utilisation, octroie la permission de vendre vos données personnelles à n'importe qui. Ces courtiers en données achètent donc celles-ci, puis les combinent avec d'autres ressources disponibles en ligne qu'ils peuvent quérir sur vous. Et ceci, afin de réaliser des profils extrêmement précis sur votre compte, qu'ils revendent à leur tour à des tiers acheteurs. De ce fait, votre profil peut donc contenir et recouper des informations substantielles et très fines, sur vos préférences personnelles. Une mine d'Or !

En réponse aux commentaires peu élogieux des consommateurs et aux griefs des groupes de protection de la vie privée de l'époque, Facebook a donc dû rectifier le tir prestement, et innover en créant d'urgence une « zone de paramétrage de confidentialité » dans son interface utilisateur, plus intuitive et plus claire. Et finalement plus simple à opérer par le commun des mortels… En théorie seulement ! Car ne s'avouant pas vaincu, il fallut naturellement compenser très vite, et par la bande, ce manque à gagner pour la firme en matière de d'accès à la captation de données qualifiées. Et inventer dans la foulée de nouvelles formes délétères de coercitions

cognitives, plus fines et moins détectables aux yeux des profanes. Le tout, en y intégrant des ressorts tactiques renouvelés…

Dénommé par Tim Jones en hommage au PDG de Facebook, Mark Zuckerberg, l'expression « Privacy Zuckering » était née ! Comme nous l'avons vu plus haut, le « Privacy Zuckering » s'opère principalement en coulisses, quand vous êtes très progressivement invité par la plateforme de réseautage social à partager publiquement beaucoup plus d'informations sur vous-même, que vous ne le souhaitiez initialement… Le sobriquet « Privacy Zuckering » a d'ailleurs finit par s'imposer aux Etats-Unis pour qualifier un tel procédé qui repose pour l'essentiel sur une « Dark Pattern ». Autrement dit, un « élément de design douteux » qui visent à orienter ou manipuler le choix de l'utilisateur en ligne. Ils s'opposent en cela à « l'UX éthique » (ou design éthique), qui consiste à penser et à concevoir comme nous l'avons évoqué plus haut, un site web de manière à ce que l'expérience utilisateur soit privilégiée, et demeure la meilleure possible.

Le principe de ces Dark Patterns repose sur un précepte assez simple en définitive : inciter l'utilisateur à faire une action qu'il n'aurait pas eu l'intention d'effectuer de lui-même. Et, si possible, sans qu'il s'en rende compte… Le but final recherché étant par exemple de collecter ses données personnelles, de lui faire ajouter des produits dans son panier utilisateur, ou encore de lui faire passer plus de temps sur une interface spécifique afin d'améliorer le trafic du site. Mais la plupart des internautes ne veulent tout simplement pas partager autant d'informations, avec les spécialistes du marketing ou les « partenaires de confiance » des firmes géantes de la Tech. Il n'est donc pas surprenant que certaines d'entre elles se risquent à jouer sur deux tableaux, en tordant quelque peu la réalité des faits sur leurs modalités secrètes d'action, afin d'y parvenir insidieusement tout de même, mais en sourdine : « C'est aussi cela le jeu, ma bonne dame ! » La « dénégation plausible » en cas de flagrant délit, restant très classiquement la meilleure ligne de défense en la circonstance…

A l'image du « Privacy Zuckering » que nous évoquions précédemment, les chercheurs ont répertorié bien d'autres tactiques digitales opérationnelles et parfaitement roublardes, qui demeurent bien en ligne encore actuellement, comme autant d'armes de persuasion massive.

On répertorie en outre, 11 types de « Dark Patterns » selon l'agence Sharing :

- **L'achat surprise, ou « Sneak into basket »** : vous faites vos courses en ligne, et constatez qu'un produit s'est glissé dans le panier contre votre gré. Par exemple, vous achetez un ticket pour un évènement et découvrez finalement que vous avez aussi souscrit une assurance par la même occasion. Comment est-ce possible ? Via un algorithme qui coche automatiquement une case à un moment donné de votre processus d'achat.

- **La perpétuation d'abonnements, ou « Forced continuity** : beaucoup d'interfaces proposent, avant de souscrire un abonnement payant, un essai gratuit de plusieurs jours. La perpétuation d'abonnement est le fait de débiter le compte de l'utilisateur, dès la fin de la période d'essai. Et sans l'avertir…

- **Le piège à cafards, ou « Roach motel »** : vous avez souscrit une offre avec une facilité déconcertante : un numéro de carte de crédit et une simple adresse mail, et le tour est joué. Le jour où vous souhaitez vous désinscrire, en revanche, le processus se révèle être soudain un réel parcours du combattant. Avec le processus de « Roach Motel » (dont le nom est emprunté à une marque américaine de pièges à cafards), l'interface espère en réalité que l'utilisateur n'aille pas au bout de sa démarche de désinscription…

- **La technique Zuckerberg, ou « Privacy zuckering »**, comme nous l'évoquions précédemment : rares sont les internautes qui lisent entièrement la politique de confidentialité d'un site web, ses conditions d'utilisation, etc. En vous inscrivant sur Facebook par exemple, vous n'avez certainement jamais lu sa politique de confidentialité très particulière, et pourtant vous l'avez acceptée ! Sachez que vous avez tout simplement offert vos données personnelles qualifiées au réseau social, et qu'à tout moment elles peuvent être utilisées, voire revendues à des tiers. Le tout, sans votre consentement !

- **L'impossibilité de comparer les prix, ou « Price comparison prevention »** : les détaillants ont bien compris qu'en montrant deux produits quasiment similaires, l'un dont le prix est au kilogramme et l'autre à la pièce, il est plus difficile pour le consommateur de les comparer. Il est donc relativement simple d'orienter le client vers le produit souhaité, en jouant sur l'affichage des prix pour qu'il paraisse – à tort – moins cher qu'un autre…

- **Le détournement d'attention, ou « Misdirection »** : généralement, on le retrouve sur les interfaces de paiement. Avec des jeux de couleurs ou un design particulier, l'utilisateur aura l'œil attiré par l'option de paiement la plus chère, tandis que l'option standard sera plus difficile à trouver. L'inversion des couleurs est souvent utilisée. L'utilisateur est habitué à voir du vert pour le « oui » et du rouge pour le « non ». Il suffit alors d'inverser ces deux couleurs pour inciter l'utilisateur à faire un choix contraire à sa volonté initiale, potentiellement sans qu'il s'en rende compte…

- **Les coûts cachés, ou « Hidden costs** : les hidden costs sont ces coûts imprévus que l'on découvre à la dernière étape du processus de paiement, par exemple des coûts de livraison ou des taxes…

- **Appâter et attraper, ou « Bait and switch »** : en entreprenant une action sur un site avec une attente précise, l'utilisateur peut finalement obtenir un résultat totalement différent. Par exemple, au milieu d'un article, il sera confronté à un message « inscrivez-vous pour continuer à lire cet article ». Contraint d'entrer une adresse mail pour accéder à la fin du contenu, il aura finalement souscrit un abonnement à une newsletter « à l'insu de son plein gré »…

- **Faire culpabiliser l'internaute, ou « Confirmshaming »** : on le retrouve généralement lors de l'annulation d'une souscription, ou lors d'une désinscription. Il s'agit cette fois-ci de jouer avec les mots pour faire culpabiliser l'utilisateur en espérant qu'il se résigne, ou se ravise...

- **Les publicités déguisées, ou « Disguised ads »** : particulièrement présents sur les sites de streaming et de téléchargement, les publicités déguisées sont des faux boutons (par exemple « regarder en HD » ou « télécharger gratuitement »), qui redirigent finalement l'internaute sur une publicité. Si depuis 2016 Google est supposé bloquer ce type de pratiques, étonnamment ce dernier n'est toujours pas efficace…

- **Le spam de contact, ou « Friend spam »** : certains sites demandent des données pour améliorer l'expérience de l'utilisateur. Par

exemple, on peut vous proposer de synchroniser vos contacts avec une interface telle que Facebook ou Linkedin, pour pouvoir les y retrouver plus facilement. On peut aussi vous proposer de créer un compte sur un site en se connectant à l'aide d'un réseau social tel que Facebook. Ces deux actions paraissent plutôt sécurisées, mais donnent finalement accès à une liste de contacts à spamer.

Ces techniques de manipulation sont redoutablement efficaces à court terme. Un internaute recherche avant toute chose, un service simple, intuitif et transparent. S'il est trompé sur un site, il ne renouvellera pas l'expérience. Il est aussi du devoir des développeurs et UX designers de se poser les bonnes questions, et de convertir l'utilisateur par la confiance plutôt que par la force. Quoi qu'il en soit, ces Dark patterns seront très progressivement amenées à disparaître, notamment grâce à l'entrée en vigueur progressive du Règlement Général de la Protection des Données (ou « RGPD »). On l'espère en tout cas, si l'on adopte le point de vue des utilisateurs.

Ces firmes géantes cherchent-elles à piéger sciemment leurs utilisateurs dans leurs filets ? Et à quelle fin ? Ceux-ci sont-ils clairement avertis, et leur consentement éclairé réellement pris en considération ?

En fait, cette manière de procéder est un très vieux truc. Facebook l'a d'ailleurs utilisé en 2010 lorsque le réseau social a permis à ses utilisateurs de se retirer des sites Web « partenaires » de la firme, qui collectaient à l'envi et enregistraient en douce leurs informations Facebook rendues accessibles...

Quiconque refusait alors cette « personnalisation » à des fins commerciales, a immédiatement vu un pop-up s'afficher sur son écran d'ordinateur demandant : « Êtes-vous sûr ? Permettre une personnalisation instantanée vous offrira une expérience plus riche lorsque vous naviguez sur le Web. » Jusqu'à très récemment, Facebook a également mis en garde ses usagers contre la désactivation de ses fonctionnalités de reconnaissance faciale : « Si vous désactivez la reconnaissance faciale, nous ne pourrons pas utiliser cette technologie si un inconnu utilise votre photo pour usurper votre identité. » Le bouton pour activer le réglage est lumineux et bleu ; alors que le bouton pour l'éteindre est d'un gris beaucoup moins accrocheur… Manigance perceptive manifeste, là encore ? Personne ne semble en douter…

En prônant un écosystème de « confiance » et de « responsabilité » apparent, et face aux appétences commerciales grandissantes et toujours plus aiguisées des annonceurs, la fonction première de ces messages est en réalité de rassurer le grand public, et de quérir – ou de produire – une forme de « consentement automatique » des fidèles. Un consentement « réflexe » en quelque sorte… Le paradoxe n'est pas mince ! Nous l'avons vu, les spécialistes du domaine qualifient ces décisions de conception et de formulation : des « modèles sombres », ou « Dark Patterns ». Des procédés fallacieux qui tentent ostensiblement de manipuler sciemment les choix individuels, en mettant à profit les dernières trouvailles en neurosciences. Quand Instagram nous demande par exemple, et à plusieurs reprises, « d'activer les notifications » et ne présente pas d'option annexe pour éventuellement refuser cette proposition, il s'agit d'un « modèle sombre ». Lorsque LinkedIn nous donne à voir une partie seulement d'un message « InMail » à partir de notre propre e-mail, mais nous oblige cependant à visiter la plateforme en ligne pour en savoir plus, il s'agit là encore du même procédé manipulatoire. Un autre « motif sombre » en somme ! Quand Facebook nous « redirige » aimablement dans les méandres de son arborescence digitale, lorsque nous essayons en vain de désactiver ou de supprimer nos comptes utilisateurs pour nous déconnecter définitivement, il s'agit également là aussi d'un « motif sombre ». Ces « Dark patterns » se retrouvent partout sur le Web, incitant les chalands à s'abonner à des newsletters ici, à ajouter des éléments à leur panier client là-bas, ou encore à s'inscrire à des services qui leurs sont parfaitement inutiles…

Malgré la multiplication des scandales ces dernières années, les grandes plateformes opérants les réseaux sociaux tels que Facebook ou Twitter, changent-ils imperceptiblement leur façon d'agir et de fonctionner à ce propos ?

Facebook a de son côté essuyé suffisamment de scandales ces dernières années, pour apprendre à ses dépens que les internautes – et le grand public – se soucient visiblement de plus en plus de ces formes de manigances manipulatoires. Il y a quelques mois, la firme californienne a d'ailleurs réglé une très lourde amende d'un montant de 5 milliards de dollars, pour avoir fait « des déclarations jugées trompeuses sur la capacité de ses utilisateurs à contrôler véritablement la confidentialité de leurs données personnelles »… Les grandes firmes de la Tech changent régulièrement leurs paramètres spécifiques leur permettant de capter à l'envi les données personnelles, en les faisant sensiblement évoluer aux yeux de leurs utilisateurs. Mais toujours en trompe l'œil cependant. Car il en va naturellement de la préservation et la pérennité de leur business model, in fine.

Dans WIRED, la journaliste Arielle Pardes rapporte à cet effet les propos de Colin Gray, un chercheur en « interaction homme-machine » de l'Université Purdue aux Etats-Unis. Ils sont particulièrement éclairants concernant ces fameux « droits utilisateurs » que les plateformes sociales géantes espèrent se voir concéder par leurs usagers. Colin Gray étudie les « Dark patterns » depuis 2015. Lui et son équipe de recherche en ont d'ailleurs identifié cinq types à leur corps défendant : « le harcèlement », « l'obstruction », « la furtivité », « l'interférence d'interface » et « l'action forcée ». Tous ces procédés apparaissent de manière récurrente dans les contrôles de confidentialité. Colin Gray, comme d'autres chercheurs, a naturellement remarqué la dissonance cognitive qui persiste à des fins évidentes d'ingénierie sociale, entre les grandes réformes engagées par les géants de la Silicon Valley en matière de confidentialité d'une part, et les outils concrets qu'ils mettent – de guerre lasse – à disposition des habitués pour moduler leur choix, d'autre part… Des interfaces qui restent percluses pour le commun des mortels, d'éléments de langages technicistes et souvent hermétiques à la compréhension commune. Une sémantique étudiée parfaitement déroutante, et de conceptions passablement ambigües, qui en dit long sur les intentions sous-jacentes… Depuis l'entrée en vigueur du RGPD en 2018, les sites Web sont en effet tenus de demander aux internautes leur « consentement éclairé » pour collecter certains types de données. Mais ces « bannières de consentement » demandent simplement à chacun, dans la plupart des cas, « d'accepter les politiques de confidentialité », sans autre forme de procès. Et sans aucune possibilité de dire « non ». Et certaines recherches engagées suggèrent d'ailleurs que « plus de 70% des bannières de consentement dans l'UE comportent une sorte de « motif sombre » (Dark Patterns) intégré, explique Colin Gray à la journaliste de Wired. « Cela est très problématique lorsque vous cédez des droits substantiels.»

Mettre en place les « Best practices » pour surfer avec des traces moindres s'impose à chacun pour demeurer libre. Les différentes méthodes abordables pour le grand public sont désormais bien connues, et permettent en réalité de mettre en place des protections tout à fait relatives, comme nous l'indiquions d'ailleurs dans un précédent article pour Atlantico… Très récemment, Facebook et Twitter ont par exemple octroyé à leurs utilisateurs respectifs un meilleur contrôle de leur vie privée sur leurs plateformes en ligne. La

vérification de la confidentialité des données privées qu'à récemment déployée Facebook, guide chacun d'entre nous à travers une série de choix agrémentés d'illustrations et de motifs aux couleurs très vives. Mais Colin Gray note cependant que les valeurs incluses « par défaut » sont encore trop souvent définies avec beaucoup moins de précision que les précédentes, et que les très nombreuses cases à cocher qui demeurent peuvent avoir pour effet immédiat de submerger la volonté des internautes en l'amoindrissant de manière intentionnelle, ou de saturer ces mêmes utilisateurs sur le plan de la perception : « Si vous avez une centaine de cases à cocher, qui va réellement le faire ? », s'indigne-t-il dans les colonnes de Wired.

L'année dernière, les sénateurs américains Mark Warner et Deb Fischer ont présenté un projet de loi qui interdirait ce type « d'interfaces utilisateur à vocation manipulatoire ». La Loi sur la réduction des expériences trompeuses pour les utilisateurs en ligne – « DETOUR » en abrégé – rendrait illégal pour des sites Web comme Facebook d'utiliser ces « modèles sombres », ou « Dark Patterns », lorsqu'il s'agit de données personnelles : « des invitations trompeuses à cliquer simplement sur le bouton « OK », peuvent souvent immédiatement transférer vos contacts, vos messages, vos activités de navigation, vos photos ou vos informations de localisation sans même que vous vous en rendiez compte », a écrit le sénateur Fischer lors du dépôt du projet de loi. « Notre législation bipartite vise à freiner l'utilisation de ces interfaces malhonnêtes, et à accroître a contrario la confiance en ligne.»

Reste qu'un problème demeure : il devient de plus en plus difficile de définir une « Dark Pattern ». « Tout design a un niveau de persuasion », indique Victor Yocco, l'auteur de l'excellent ouvrage américain : « Design for the Mind : Seven Psychological Principles of Persuasive Design ». Yocco est chercheur, mais aussi un stratège avisé qui officie à « l'Intuitive Company » : une société de conception et de développement spécialisée sur l'expérience utilisateur, située à Philadelphie, en Pennsylvanie. Par définition, le design d'un produit oriente ou encourage les individus à utiliser celui-ci d'une manière très particulière, ce qui n'est pas intrinsèquement mauvais en soi indique Yocco. Mais il va plus loin encore dans la quatrième de couverture de son livre : « Aujourd'hui, les concepteurs Web sont animés par des questions pertinentes comme celles-ci : comment gagnerai-je la bataille de la courte durée d'attention ? Comment mettre les visiteurs à l'aise et leur fournir les informations pertinentes auxquelles ils s'attendent consciemment (et inconsciemment) ? Comment la conception de mon site encouragera-t-elle les utilisateurs à s'engager, à naviguer ou à acheter ? » Victor Yocco indique qu'il existe un ensemble de principes psychologiques testés qui peuvent transformer les conceptions numériques en anticipant et en tirant meilleur parti de la façon dont les êtres humains réagissent aux stimuli : « cette approche scientifique du processus de prise de décision, les attitudes face au risque et à la récompense, l'influence de groupe, (etc.) représente un trésor prêt à être appliqué au domaine de la conception de sites Web. »

Son opus « Design for the Mind » enseigne en outre aux concepteurs Web et aux développeurs comment créer des sites et des applications qui font appel à nos réponses naturelles innées, et nos motifs cognitifs en tant qu'êtres humains. Le livre présente à ce titre les concepts psychologiques les plus immédiatement pertinents et applicables, et décompose chaque théorie en principe facilitateur, aisément digérable par le praticien. Puis il montre comment ils peuvent être mis à profit et utilisés pour générer des conceptions puissantes en matière d'influence. L'idée n'est pas tant de produire un ensemble de modèles à utiliser par cœur à des fins de persuasion numérique de masse, que d'approfondir la compréhension des raisons pour lesquelles les individus réagissent comme ils le font, afin de concevoir des caractéristiques et des approches plus intelligentes, plus naturelles, plus engageantes et plus persuasives… Vaste programme ! Dans WIRED, Yocco indique cependant avec un langage particulièrement fleuri que si certains espéraient faire usage de ses trouvailles « pour tromper les gens, ce sont des connards »…

En définitive, beaucoup de ces modèles sombres ou « Dark Patterns », sont utilisés pour extraire des mesures qui indiquent le succès, comme la croissance des utilisateurs ou le temps passé sur les plateformes. Colin Gray cite l'exemple de l'application pour smartphone « Trivia Crack », qui incite ses utilisateurs à jouer à un autre jeu, toutes les deux à trois heures environ. Ces types de notifications sous forme de spam sont utilisés par les plateformes de médias sociaux depuis des années pour induire le type de FOMO qui nous tient accro. Le syndrome FOMO (ou la peur de rater quelque chose), est une sorte d'anxiété sociale caractérisée par la crainte constante de manquer une nouvelle importante, ou un quelconque événement, donnant une occasion d'interagir socialement. « Nous savons que si nous donnons aux individus des choses comme le balayage ou des mises à jour de statut, il est plus probable que ces mêmes personnes reviendront, et les verront encore et encore », dit Yocco. « Cela peut conduire à des comportements compulsifs. » Les schémas d'actions les plus sombres de tous surviennent lorsque les gens essaient de quitter ces plates-formes : essayez de désactiver votre compte Instagram et vous constaterez que c'est extrêmement difficile. Tout d'abord, vous ne pouvez même pas le faire depuis l'application elle-même. À partir de la version de bureau du site, le paramètre est enterré à l'intérieur de l'onglet « Modifier le profil », et est livré avec une série d'interstitiels. (Pourquoi désactivez-vous ? Trop distrayant ? Ici, essayez de désactiver les notifications. Juste besoin d'une pause ? Pensez à vous déconnecter, etc.).

« Cela induit des frictions notables qui ralentissent drastiquement la manière d'atteindre votre objectif, afin de vous compliquer la tâche », déclare Nathalie Nahai, l'auteur de « Webs of Influence : The Psychology of Online Persuasion ». Il y a des années, lorsque Nahai a supprimé son compte Facebook, elle a trouvé un ensemble similaire de stratégies de manipulation. « Ils ont utilisé les relations et les connexions que j'avais pour dire : 'Êtes-vous sûr de vouloir arrêter ? Si vous partez, vous ne recevrez pas de mises à jour de cette personne', etc », puis affichez les photos de certains de ses amis proches. « Ils utilisent ce langage qui est, dans mon esprit, de la coercition », dit-elle. « Ils rendent le départ de chacun psychologiquement douloureux. » Pire encore, rapporte Colin Gray : car la recherche montre que la plupart des gens dans ce contexte ne savent même pas qu'ils sont manipulés ! Mais selon une récente étude, dit-il, « lorsque les gens étaient familiarisés à l'avance avec le langage, pour montrer à quoi ressemblait la manipulation, deux fois plus d'utilisateurs pouvaient alors identifier ces motifs sombres. Au moins, il y a un espoir qu'une plus grande prise de conscience puisse restituer aux utilisateurs une partie de leur pouvoir de contrôle.

A ce titre, n'oublions jamais cette phrase prophétique d'Orwell tiré de son chef d'œuvre impérissable « 1984 » : « Pour diriger et continuer à diriger, il faut être capable de modifier le sens de la réalité ». Maintenant nous le savons tous…