Les dark patterns ou l'art de tromper l'utilisateur

written by Jacques-André Fines Schlumberger | 23 décembre 2021

Une *dark pattern*, en français « interface truquée », est minutieusement conçue pour tromper ou manipuler l'utilisateur d'un site ou d'une application web. Mise sous pression, obligation, obstacle, cachotterie ou entourloupe sont des tactiques perverses qui participent de la chasse au clic sur le Net.

Le terme *dark pattern* a été forgé en août 2010 par Harry Brignull, spécialiste du design d'interfaces numériques. Le site darkpatterns.org, qu'il a créé il y a plus de dix ans pour dénoncer ces pratiques, en recense un grand nombre parmi lesquelles *Sneak into Basket* (« se faufiler dans le panier »), qui consiste à ajouter, à son insu, un article supplémentaire dans le panier d'un client effectuant des achats sur le web ; *Roach Motel* (« motel des cafards »), qui entraîne facilement l'utilisateur à souscrire à un abonnement premium, dont il aura ensuite bien du mal à se défaire ; *Privacy Zuckering* (« Zuckering de la vie privée »), du nom du président de Facebook, Mark Zuckerberg, qui pousse l'utilisateur d'un service web à partager publiquement bien plus d'informations qu'il ne l'imagine ; ou encore le *Misdirection*, dont le design appelle volontairement l'internaute à se concentrer sur une chose afin de lui en faire discrètement accepter une autre.

L'association allemande Dark Pattern Detection Project recense vingt types de *dark patterns* différents, regroupés en cinq catégories : les mises sous pression, les obligations, les obstacles, les cachotteries et les entourloupes. Comme l'explique Claude Castelluccia, directeur de l'équipe Privatics de l'Inria (Institut national de recherche en informatique et en automatique) dans une interview pour *La rem* n°49, ces manipulations, *« très étudiées en marketing comportemental (neuromarketing), sont les conséquences même du modèle économique de l'internet et de ses services* "gratuits" *»* où les données personnelles de l'utilisateur sont systématiquement enregistrées à son insu pour être revendues à des tiers.

L'objet d'une « interface truquée » est d'orienter l'utilisateur vers des choix qu'il n'aurait probablement pas faits en connaissance de cause, et qui sont dans l'intérêt de la plateforme. La *dark pattern* la plus répandue actuellement concerne le bandeau des cookies que l'utilisateur doit accepter pour naviguer sur un site web. Depuis l'entrée en vigueur du règlement général sur la protection des données personnelles (voir *La rem* n°42-43, p.21), les sites web ont l'obligation de recueillir le consentement de l'utilisateur lorsque des cookies sont

déposés dans son navigateur. Or, la plupart du temps, le bouton d'acceptation de ces cookies est particulièrement visible tandis que celui qui permet de les refuser est un lien trop discret, voire difficilement accessible. La plupart du temps, ces manipulations complexes ou chronophages découragent les utilisateurs qui, de guerre lasse, acceptent le dépôt de cookies afin d'accéder rapidement au contenu recherché.

Une *dark pattern* peut être plus subtile, comme celle installée en novembre 2020 sur le média social Instagram, propriété de Facebook. Les onglets « Notifications » et « Nouvelle publication » ont été déplacés sciemment, en haut de l'écran, afin de laisser la meilleure place aux nouveaux boutons « Shopping » et « Reels », format vidéo qui imite celui de l'application concurrente TikTok. Immanquablement, les habitués d'Instagram croyant cliquer par habitude sur le bouton « Notifications », se sont vu diriger vers la boutique ou bien proposer l'option d'un nouveau format vidéo alors qu'ils souhaitaient simplement partager une photo.

Le web fourmille de *dark pattern*s et certaines entreprises en usent plus que d'autres. Amazon fournit de bons exemples : il est quasiment aussi impossible de se désinscrire de son service Prime qu'il est facile d'y souscrire par une simple case à cocher lors d'un achat en ligne. L'équivalent norvégien de l'association de consommateurs UFC Que Choisir a publié un rapport en 2021, dénonçant la façon dont le géant du commerce électronique piège les internautes contraints de *« faire face à un grand nombre d'obstacles : des menus de navigation compliqués, des formulations biaisées et des choix confus »*, soit plus d'une quinzaine d'étapes avant de parvenir à se désabonner d'Amazon Prime.

En France, la Commission nationale de l'informatique et des libertés (Cnil) s'est emparée du problème, notamment en publiant les *« lignes directrices modificatives et sa recommandation sur les cookies et autres traceurs »* en octobre 2020 et en accordant un délai de six mois aux éditeurs de sites web pour se conformer à cette nouvelle réglementation. Mais force est de constater que l'autorité administrative indépendante peine toujours à faire respecter *« l'obligation d'utiliser des boutons et une police d'écriture de même taille, offrant la même facilité de lecture, et mis en évidence de manière identique »*. D'autant que la Commission s'est elle-même contredite par l'adoption d'une recommandation (délibération n°2020-092 du 17 septembre 2020) qui propose des modalités pratiques de mise en conformité en cas de recours aux *« cookies et autres traceurs »* à l'aide d'un exemple visuel de bannière des cookies où les boutons « Accepter » et « Refuser » ne sont ni sur la même ligne ni de la même couleur. Cette recommandation étonnamment proposée par la Cnil, alors même qu'elle reproduit une *dark pattern*, est ainsi devenue le modèle appliqué par de très nombreux sites web français, parmi lesquels lemonde.fr, lesechos.fr ou

encore latribune.fr. Quant à Facebook ou Google, ni l'un ni l'autre n'a consenti à afficher sur son site web ou sur son application un bouton permettant de refuser les cookies.

C'est finalement aux États-Unis que la réglementation évolue dans le bon sens. La Californie a adopté en 2021 une nouvelle réglementation qui vient renforcer la loi historique sur la protection de la vie privée, la California Consumer Privacy Act (CCPA) (voir *La rem* n°56, p.53), et interdit désormais aux entreprises d'utiliser toute forme de *dark pattern* qui aurait pour but *« de compromettre ou d'entraver le choix d'un consommateur de se retirer des systèmes dans lesquels ses données personnelles sont vendues »*. Le texte interdit précisément *« l'utilisation d'un langage déroutant comme les doubles négations ; obliger les utilisateurs à cliquer ou écouter les raisons pour lesquelles ils ne devraient pas soumettre une demande de désinscription avant de confirmer leur demande ; obliger les utilisateurs à rechercher ou faire défiler le texte d'une politique de confidentialité ou d'un document ou d'une page web similaire afin de localiser le mécanisme permettant de soumettre une demande de retrait »*.

Rappelons que ces techniques de manipulation par le design restent… de la manipulation. Lorsqu'elles orientent la prise de décision d'un individu dans son intérêt, elles s'appellent *nudge* (voir *La rem* n°49, p.83) et lorsqu'elles le trompent, elles sont qualifiées de *dark pattern*. Dans les deux cas, et à leur insu, il s'agit de priver les utilisateurs de leur capacité à choisir.

Sources :

- « Délibération n° 2020-092 du 17 septembre 2020 portant adoption d'une recommandation proposant des modalités pratiques de mise en conformité en cas de recours aux "cookies et autres traceurs" », Cnil, cnil.fr.
- « Comment Amazon & Co. nous manipulent grâce aux "dark patterns" », Anouch Seydtaghia, letemps.ch, 14 janvier 2021.
- « Cliquez ici, c'est pour votre bien », Philippe Boyer, latribune.fr, 26 janvier 2021.
- « Les dark patterns ou comment ruiner la navigation Internet », Lorraine Redaud, charliehebdo.fr, 8 février 2021.
- « Attorney General Becerra Announces Approval of Additional Regulations That Empower Data Privacy Under the California Consumer Privacy Act », oag.ca.gov, March 15, 2021.
- « La Californie interdit aux entreprises d'utiliser les "dark patterns" », Bill Fassinou, web.developpez.com, 17 mars 2021.
- « Comment les éditeurs se moquent de la Cnil », pixeldetracking.com, 9 juin 2021.
- « Dark patterns : comment les sites web abusent de petites astuces pour tenter de vous piéger », Gilbert Kallenborn, 01net.com, 21 août

2021.