

● **Dark patterns : deux études publiées afin d'identifier les interfaces truquées**

Les *dark patterns* (ou, en français, interfaces truquées) sont des interfaces utilisateur qui, délibérément ou dans les faits, trompent ou manipulent les destinataires du service, en altérant ou en compromettant leur autonomie, leur capacité de décision ou leurs choix. Leur but est d'exploiter les biais cognitifs des utilisateurs pour les contraindre, les orienter, voire les tromper afin qu'ils prennent des décisions qu'ils n'auraient sans doute pas prises initialement.

Depuis le 17 février 2024, le règlement Digital Services Act (« **DSA** ») interdit expressément aux fournisseurs de plateformes en ligne de concevoir, d'organiser et d'exploiter « *leurs interfaces en ligne [...] d'une manière qui, délibérément ou dans les faits, trompe ou manipule les destinataires du service, en altérant ou en compromettant leur autonomie, leur capacité de décision ou leurs choix* ». Il convient de préciser que pour les autres acteurs (par exemple éditeur d'un site e-commerce en propre), les *dark patterns* sont interdits, de façon indirecte, par le RGPD et la directive européenne sur les pratiques commerciales déloyales, transposée à l'article L. 121-1 du Code de la consommation. Bien que certains *dark patterns* soient désormais expressément visés par la loi, il n'en existe pas de liste définitive et exhaustive.

Plusieurs études ont récemment été conduites sur les *dark patterns*. L'UFC-Que Choisir (association de consommateurs) a réalisé au printemps 2024 une étude principalement afin de s'assurer que les plateformes en lignes respectent bien les dispositions du règlement DSA. Le Global Privacy Enforcement Network (réseau d'organismes agissant pour la protection de la vie privée au sein des pays membres de l'OCDE comptant plus d'une vingtaine d'autorités de protection des données dont la CNIL) a réalisé une étude pour identifier sur des sites internet les mécanismes de conception trompeuse en matière de protection des données personnelles. Ces deux enquêtes mettent en évidence l'existence de *dark patterns* dans une grande majorité des sites consultés.

L'étude « *Dark patterns dans l'e-commerce : les interfaces trompeuses sur les places de marché en ligne* » conduite par l'UFC-Que Choisir

L'UFC-Que Choisir a étudié les vingt places de marché en ligne les plus fréquentées en France afin de déterminer l'existence ou non de *dark patterns* (notamment Temu, AliExpress, Veepee, Amazon, Cdiscount, Airbnb et Rakuten France). Toutes les places de marchés étudiées ont recours à des *dark patterns*, avec une utilisation plus fréquente et un caractère plus envahissant sur les plateformes chinoises. Si l'étude se focalise sur les places de marché en ligne, l'UFC-Que Choisir a aussi vérifié 5 sites e-commerce qui ne sont pas des places de marché (Courir, H&M, Lidl, Micromania et Sephora). Il apparaît que les *dark patterns* sont moins courants sur ces sites mais souvent présents.

L'UFC-Que Choisir liste les *dark patterns* les plus courants, notamment :

- **Manipulation visuelle** : Le professionnel utilise des éléments de conception visuels pour influencer la prise de décision en mettant en valeur certaines options. Par exemple, un bouton coloré pour accepter une offre supplémentaire juxtaposé à un bouton terne pour la refuser.
- **Compte obligatoire** : Lors d'un achat ou de l'utilisation d'un service, le consommateur est obligé de créer un compte client, même si ce n'est pas nécessaire pour la prestation.
- **Prix barrés trompeurs** : Le professionnel affiche des prix barrés qui ne correspondent pas à de réelles réductions, mais qui sont plutôt des comparaisons avec des prix arbitraires, induisant les consommateurs en erreur.
- **Suppression de compte difficile** : La suppression d'un compte client est rendue excessivement difficile, voire impossible. Par exemple, le compte client ne peut être supprimé qu'en envoyant un message au service client.
- **Interruption d'achat difficile** : L'interruption de l'achat lors de sa finalisation est rendue excessivement difficile. Par exemple, le consommateur ne peut pas simplement revenir à la page d'accueil en un clic.

Les autres *dark patterns* identifiés par l'UFC-Que Choisir sont la publicité masquée, l'incitation répétitive (*nagging*), le message de preuve sociale (messages informant le consommateur de la popularité du produit ou service comme le nombre de réservation), le message de stock limité, la manipulation textuelle, la présélection, le *sludge* (obstacles excessifs ou injustifiés qui empêchent les consommateurs de réaliser leurs choix comme obliger le consommateur à passer par plusieurs étapes pour refuser une option supplémentaire, alors qu'il peut l'accepter en un seul clic), les coûts cachés, les prix cloisonnés (présentation des différentes composantes du prix sans communiquer au consommateur le coût total ou le coût total estimé, rendant ainsi la comparaison des offres plus difficile), le message de temps limité, la ludification (rendre une option plus facile à choisir comme pour les bannières cookies) et la surcharge d'informations.

À l'issue de son enquête, l'UFC-Que Choisir a annoncé avoir saisi la DGCCRF et la Commission européenne pour les alerter sur ces pratiques afin d'initier des enquêtes complémentaires et sanctionner ces comportements prohibés. En outre, l'association dit rester vigilante dans les prochains mois pour initier toute action en justice nécessaire en cas de persistance de ces pratiques.

Résultats de l'audit « Mécanismes de conception trompeuse » réalisé par le GPEN :

L'audit du GPEN démontre aussi que les interfaces des sites en ligne ont encore des progrès à réaliser en matière de protection de la vie privée. L'étude a été réalisée par le GPEN en coopération avec 26 autres autorités de protection des données nationale (y compris la CNIL) sur 1010 sites internet et applications mobiles (pas uniquement des places de marché en ligne).

Les auditeurs du GPEN ont observé un large panel de choix de conception ayant pour objectif de tromper les utilisateurs. Ces choix de conception trompeurs ont ensuite été regroupés sous cinq indicateurs, ce qui a permis d'aboutir aux résultats suivants :

- **Langage complexe et déroutant** : plus de 89 % des politiques de confidentialité étaient trop longues (55% des politiques contenaient plus de 3000 mots) ou rédigées dans un langage complexe (de niveau universitaire).
- **Interférence de l'interface** : consiste à utiliser des éléments de conception et de méthodes de présentation qui modifient la perception et la compréhension des options par les utilisateurs. Plusieurs types d'interférence de l'interface existent comme la présélection, le fait d'établir une hiérarchie entre les choix ou la manipulation émotionnelle en utilisant par exemple ce type de vocabulaire : « Acceptez et profitez des offres » et « Quoi ? Vous ne voulez pas économiser ? ».
- **Harcèlement** : 35 % des sites web et des applications invitaient à répétition les utilisateurs à reconsidérer leur intention de supprimer leur compte.
- **Obstruction** : consiste à insérer des étapes supplémentaires entre les utilisateurs et leurs objectifs, en dissuadant les utilisateurs de faire les choix prévus ou en rendant les utilisateurs moins motivés à le faire. 40 % des sites mettaient en place des obstacles pour faire des choix en matière de protection de la vie privée ou d'accéder à des renseignements, notamment pour trouver les paramètres de confidentialité ou pour supprimer son compte.
- **Action forcée** : plusieurs types d'actions forcées ont été identifiées, comme demander plus de renseignements personnels au moment de la suppression du compte que lors de la création ou proposer uniquement un bouton « Accepter » pour les cookies sans mécanisme de refus.

Le GPEN conclut son audit en renvoyant à l'essence du RGPD : l'objectif est de faire respecter l'interdiction des *dark patterns* afin de permettre de restaurer la confiance entre les individus et les places de marché en ligne dans l'utilisation des données personnelles. Pour le GPEN, l'abandon de ces pratiques trompeuses est un élément clé dans cette recherche de confiance. C'est pourquoi, le GPEN invite ces sites à se conformer à la réglementation en vigueur en adoptant des bonnes pratiques ; par exemple en mettant en évidence les options qui protègent la vie privée, en utilisant un langage et une conception neutre pour présenter de manière transparente les différents choix en matière de protection de la vie privée ou encore en réduisant le nombre de clics requis pour trouver les renseignements sur la protection de la vie privée (dont la politique de confidentialité), se déconnecter et supprimer son compte.

Liens utiles :

- [Dark patterns sur les sites d'e-commerce - l'UFC-Que Choisir appelle les autorités à sanctionner les interfaces trompeuses](#)
- [Rapport complet dark patterns dans l'e-commerce de l'UFC-Que Choisir - 20 juin 2024](#)
- [Design trompeur : les résultats de l'audit du GPEN \(cnil.fr\)](#)
- [Rapport complet du GPEN – 9 juillet 2024](#)

