Les « *Dark patterns* » : Mieux comprendre les interfaces trompeuses

Introduit en 2010 par Harry Brignull, un spécialiste de l'expérience client, à la suite du boom du e-commerce, le terme « *Dark pattern* », également connu sous les noms d'« *interface trompeuse* », de « *deceptive design* » ou encore de « *mécanisme de conception trompeuse* », est une interface internet qui piège l'utilisateur en affichant des messages trompeurs et manipulateurs.

Son but est ainsi d'orienter l'internaute vers des choix qu'il n'aurait probablement pas faits en connaissance de cause, et qui ne sont pas dans son intérêt mais dans celui du site visité.

Sur le plan de la protection des données personnelles, ces pratiques se traduisent par une collecte beaucoup plus importante d'informations et par une difficulté d'exercice de leurs droits par les personnes concernées.

S'il n'existe pas de liste exhaustive de ces « *dark patterns* », 3 grandes catégories de modèles peuvent néanmoins être identifiées :

- Ceux qui manipulent l'attention de l'utilisateur ou ses préférences ;
- Ceux qui limitent sa capacité d'action ;
- Ceux qui manipulent la désirabilité de l'utilisateur et suscitent l'urgence.

Exemples concrets :

- la case assurance est pré-cochée lors de l'achat d'un billet d'avion
- un utilisateur doit accepter tous les cookies pour naviguer sur un site Internet

Interdiction des « *Dark patterns* » dans l'Union européenne

Entré en vigueur le 17 février 2024 sur le territoire de l'Union européenne, le « *Digital Services Act* » (DSA) interdit la pratique des « *Dark patterns* » dans son article 25 : « *Les fournisseurs de plateformes en ligne ne conçoivent pas, n'organisent pas et n'exploitent pas leurs interfaces en ligne […] d'une manière qui, délibérément ou dans les faits, trompe ou manipule les destinataires de service, en altérant ou en compromettant leur autonomie, leur capacité de décision ou leurs choix* ».

Cette interdiction est précisée dans le considérant 67 du règlement :

« *Les interfaces en ligne trompeuses de plateformes en ligne sont des pratiques qui ont pour objectif d'altérer ou d'entraver sensiblement la capacité des destinataires du service de prendre une décision ou de faire un choix, de manière autonome et éclairée. Ces pratiques peuvent être utilisées pour persuader les destinataires du service de se livrer à des comportements non désirés ou de prendre des décisions non souhaitées qui ont des conséquences négatives pour eux. Par conséquent, il devrait être interdit pour les fournisseurs de plateformes en ligne de tromper ou d'encourager dans un sens les destinataires du service et d'altérer ou d'entraver l'autonomie, la prise de décision ou le choix des destinataires du service par la structure, la conception ou les fonctionnalités d'une interface en ligne ou d'une partie de celle-ci. Cela devrait comprendre, sans s'y limiter, les choix de conception abusifs destinés à amener le destinataire à exécuter des actions qui profitent au fournisseur de plateformes en ligne mais qui ne sont pas nécessairement dans l'intérêt du destinataire, en lui présentant des choix de manière biaisée, par exemple en accordant davantage d'importance à certains choix au moyen de composantes visuelles, auditives ou autres, lorsqu'il est demandé au destinataire du service de prendre une décision.*

Cela devrait également inclure le fait de demander à plusieurs reprises à un destinataire du service de faire un choix lorsque ce choix a déjà été fait, de rendre la procédure d'annulation d'un service nettement plus compliquée que celle de s'y inscrire, de rendre certains choix plus difficiles ou plus longs que d'autres, de rendre excessivement difficile l'interruption des achats ou le fait de quitter une plateforme en ligne donnée permettant aux consommateurs de conclure des contrats à distance avec des professionnels, de tromper les destinataires du service en les incitant à prendre des décisions sur des transactions, ou d'appliquer des paramètres par défaut très difficiles, à modifier, et d'influencer ainsi de manière excessive la prise de décision des destinataires du service, d'une manière qui altère et entrave leur autonomie, leur prise de décision, et leur choix […] »

Quels sont les mécanismes de déception trompeurs les plus courants ?

En début d'année 2024, le Global Privacy Enforcement Network (GPEN) en coopération avec 26 autorités de protection de la vie privée, a conduit un « *ratissage* » de 1010 sites Internet et applications mobiles dont l'objectif était de reproduire l'expérience des consommateurs et d'évaluer comment ceux-ci pouvaient faire des choix en matière de protection de la vie privée, obtenir des renseignements sur la protection de la vie privée, et se déconnecter d'un compte et le supprimer.

L'audit a ainsi révélé que 97 % des sites Web et applications évalués sur la base de cinq indicateurs identifiés par l'Organisation de coopération et de développement économiques (OCDE) comme étant caractéristique des modèles de conception trompeuse, utilisaient au moins un des modèles suivants :

Un langage complexe et déroutant (observé dans 89% des cas)

L'audit a montré que la majorité des politiques de confidentialité sont longues (plus de 3000 mots) et rédigées dans un langage complexe.
Cela rend difficile pour les utilisateurs de comprendre comment leurs données sont collectées, utilisées et partagées. Un langage juridique dense et des explications prolixes découragent souvent les utilisateurs de lire ces politiques, les laissant dans l'ignorance quant aux implications de leurs choix.

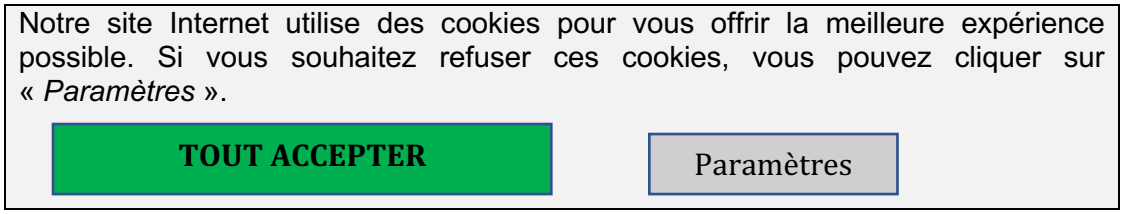
Les interférences d'interface (observées dans 43% des cas)

Ces pratiques ont pour objectif de manipuler l'interface utilisateur pour favoriser certaines actions au détriment d'autres. Cela peut inclure la dissimulation d'informations importantes, la présélection d'options par défaut, ou encore l'utilisation de techniques de manipulation esthétique pour attirer l'attention de l'utilisateur.

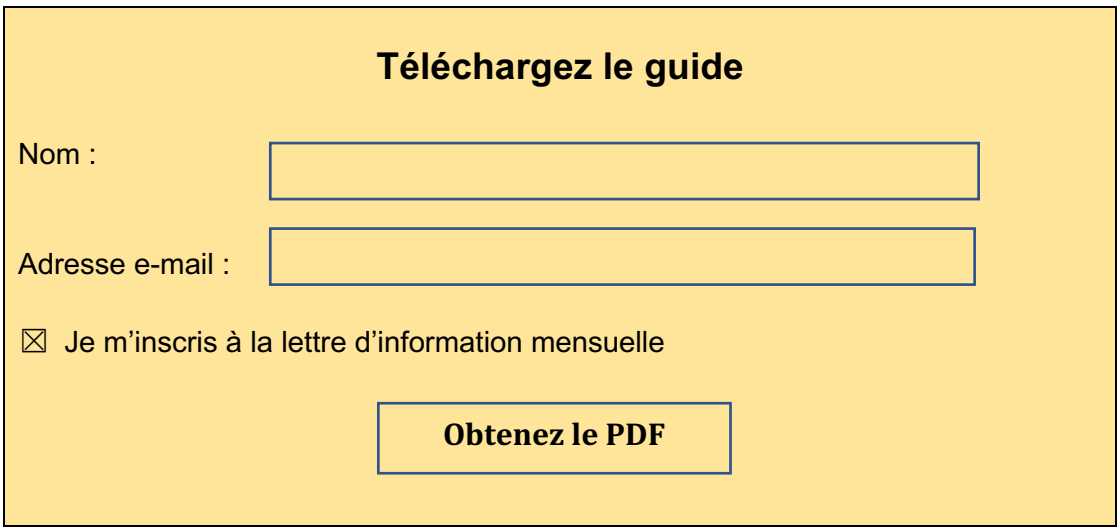
Plusieurs types d'inférences existent :

- la fausse hiérarchie : les paramètres de confidentialité les plus permissifs – et favorisés par l'organisation – sont plus grands, plus colorés et plus en évidence, alors que l'option la plus restrictive est plus petite, plus pâle et plus discrète.

  Exemple :

- la préselection : l'option privilégiée par le Site Internet, et souvent la plus attentatoire à la vie privée, est présélectionnée par défaut

- la manipulation émotionnelle : par le biais d'un langage à connotation émotionnelle le site Internet pousse les utilisateurs à se tourner vers les options de confidentialité les moins intéressants pour eux.

Exemple 1 :

☐ Je souhaite recevoir des offres promotionnelles

☐ Non merci, des prix plus bas ne m'intéressent pas

Exemple 2 :

Confirmation de la suppression de votre compte

Etes-vous certain de vouloir supprimer votre compte ? Ce serait dommage de perdre tous vos privilèges client !

Je confirme la suppression de mon compte

L'obstruction (observée dans 39% des cas)

En insérant des étapes supplémentaires, non nécessaires, entre les internautes et leurs objectifs, les sites Internet souhaitent rendre plus difficile ou fastidieux l'exécution de certaines actions et ainsi dissuader lesdits internautes de faire les choix prévus initialement.

Les actions forcées (observées dans 21% des cas)

Ces pratiques obligent le consommateur à effectuer une action pour accéder à une fonctionnalité spécifique, comme remplir ses informations de paiement pour participer à un essai gratuit ou accepter tous les cookies pour naviguer sur un site Internet.

Exemple :

Le harcèlement (observé dans 14% des cas)

Par le biais d'incitations ou pop-ups persistants, les sites Internet invitent les internautes à effectuer des actions spécifiques pouvant aller à l'encontre de leurs intérêts en matière de protection de la vie privée, comme s'abonner à une newsletter ou ajouter un article à leur panier.

Quelles recommandations pour éviter ces mécanismes de déception trompeurs?

Des politiques de confidentialité rédigées en des termes clairs et simples

Les informations doivent être fournies de la façon **la plus simple possible**, en évitant les phrases et les structures linguistiques complexes.

Elles ne doivent pas être formulées dans des termes vagues, abstraits, ambigus, ou bien encore être sujettes à différentes interprétations.

Les termes trop juridiques, techniques ou spécialisés ne sont pas recommandés.

Une attention particulière doit être portée à l'information destinée aux mineurs. Le responsable du traitement doit ainsi s'assurer que le vocabulaire, le ton et le style de langage sont adaptés au jeune public. Des mots beaucoup plus simples ou des illustrations peuvent par exemple être utilisés.

Une transparence dans les choix

Les interfaces utilisateur doivent présenter des options de consentement de manière équilibrée, sans favoriser les choix moins protecteurs pour la vie privée.

Exemple de choix équilibrés :

☐ Je souhaite recevoir des offres promotionnelles

☐ Je ne souhaite pas recevoir d'offres promotionnelles

Un accès facile aux paramètres de confidentialité

L'internaute qui souhaite accéder aux paramètres de confidentialité, et éventuellement les modifier, ne doit rencontrer aucune entrave inutile.

Une procédure simple pour supprimer un compte

Tout internaute doit pouvoir facilement supprimer son compte sans avoir à divulguer d'informations supplémentaires.