

Dark Patterns



Introduction

Cette fiche thématique a pour but d'aiguiser votre conscience sur l'influence possible des designs numériques porteurs de risque sur votre comportement en tant qu'utilisateur et, plus particulièrement, de montrer ce que sont réellement les dark patterns, où vous pouvez les rencontrer, comment ils agissent sur vous et ce à quoi vous devez prêter attention.

Elle doit vous aider à garder le contrôle sur vos actes et vos données en tant qu'utilisateur, et à vous protéger des abus, des tromperies et de la manipulation.

Table des matières

1. Les dark patterns, un risque
2. Que sont les dark patterns : définition et objectif / mode d'utilisation
3. Alors, les dark patterns sont-ils bénéfiques ou nuisibles pour l'utilisateur ?
4. À quoi ressemblent les dark patterns : exemples les plus courants
5. Ont-ils le droit ? À propos des règles, des zones grises et des nouveaux défis
6. Vous pouvez vous protéger !
7. Liens utiles

1. Les dark patterns, un risque

Les design patterns se trouvent dans les applications, les médias sociaux, les plateformes et réseaux, pour des services de streaming et des boutiques en ligne, mais également dans les jeux en ligne, les moteurs de recherche et les systèmes d'exploitation – bref, partout où les interactions entre l'humain et la machine sont possibles par le biais d'interfaces numériques.

Ce sont **des schémas récurrents dans la structure des applications ou des sites internet**. Ils permettent bien souvent à l'utilisateur de garder plus facilement une vue d'ensemble et d'agir dans le monde en ligne. Ainsi, les design patterns **peuvent influencer le comportement et les décisions d'un utilisateur, ce qui peut présenter un risque ou un avantage pour les utilisateurs, selon le cas**. Il est donc important que l'utilisateur soit bien conscient de cette influence et qu'il accueille toujours attentivement et s'interroge de façon critique sur les objectifs et les pratiques des designs numériques ou des designs des interfaces utilisateurs.

Avez-vous déjà accepté tous les cookies sans lire les conditions précises, regardé une deuxième puis une troisième vidéo en streaming simplement parce qu'elles continuaient automatiquement, cliqué sur un article après l'autre dans votre fil d'actualité ou même acheté un produit sans l'avoir décidé de manière consciente ? Alors, vous avez très probablement déjà rencontré les « dark patterns », ces designs numériques porteurs de risques.

2. Que sont les dark patterns : définition et objectif / mode d'utilisation

Les dark patterns peuvent aussi être qualifiés de *Deceptive Design* ou *Unethical Design* ou « d'interface truquée » en français. Ce terme vaste, évoqué [pour la première fois en 2010 par le designer en expérience utilisateur Harry Brignull](#), décrit un phénomène auquel presque tout le monde a probablement déjà été confronté, aussi bien hors ligne que, plus récemment, en ligne et ce sous différentes formes.



Le [Comité Européen de la Protection des Données](#) définit les dark patterns comme

« Des interfaces et des expériences utilisateur implémentées sur les plateformes de médias sociaux et incitant les utilisateurs à prendre des décisions non intentionnelles, non consenties et potentiellement nuisibles en rapport avec leurs données personnelles.

Les interfaces truquées visent à influencer le comportement des utilisateurs et peuvent gêner leur capacité « à protéger efficacement leurs données personnelles et à prendre des décisions conscientes », en les empêchant, par exemple, de donner « un consentement libre et éclairé ». Cela peut être réalisé dans différents aspects du design, notamment par le choix des couleurs des interfaces et le placement des contenus. »

(voir Guidelines 03/2022, p. 2; traduction libre de l'anglais)

Du fait que les gens passent de plus en plus de temps en ligne et transfèrent les activités par analogie vers l'espace numérique, que ce soit pour faire des achats, jouer, regarder des films ou communiquer avec des amis, une nouvelle course pour capter leur attention s'est développée. La clé pour gagner cette attention se trouve dans ce que l'on appelle User Experience – ou « UX » en abrégé, c'est-à-dire l'expérience utilisateur. Plus une application ou un site internet, par exemple, est facile, intuitif et agréable pour l'utilisateur, plus ce dernier aimera y passer du temps.

C'est pourquoi **les fournisseurs essaient d'optimiser le design de ces produits numériques et de leurs interfaces en fonction des habitudes, du comportement et des besoins des utilisateurs**. S'appuyant sur la psychologie moderne du comportement et sur le nombre d'utilisations, les façons de présenter exactement ce que les utilisateurs cherchent ou ce à quoi ils s'intéressent sont devenues de plus en plus sophistiquées. Et davantage de stratégies visent à entraîner un certain comportement. Le but des fournisseurs / exploitants / développeurs est de gagner des clients, de développer des produits et d'augmenter leurs ventes.

Ainsi, pour atteindre ces objectifs, de plus en plus d'entreprises dans le monde ont réalisé des investissements financiers pour ne citer que ces exemples au cours des dernières années pour concevoir systématiquement les sites internet, les applications ou les produits digitaux de façon à ce que la recherche de données, les moyens de paiement ou les enregistrements, ne prennent que quelques secondes et soient les plus simples possibles.

On pourrait donc supposer que cette évolution soit avantageuse pour les deux parties – fournisseur et utilisateur. C'est vrai dans bien des cas, notamment lorsque les design patterns servent à améliorer l'utilisabilité du web - c'est le cas des « [Good Patterns](#) ».

Cependant, les produits digitaux sont de plus en plus souvent optimisés pour faire accroître le nombre des utilisateurs et de générer de gros chiffres d'affaires, capter des données, maximiser la durée d'utilisation ou simplement pour faire augmenter le trafic sur le web le plus rapidement possible. Cela a également conduit à la diffusion d'interfaces, de designs et de mécanismes qui suivent les objectifs commerciaux des fournisseurs, mais qui sont en contradiction avec les intérêts des utilisateurs, voire présentent des risques, des inconvénients et des dangers.

Cela est dû au fait que les objectifs, les intérêts et les besoins des fournisseurs et des utilisateurs divergent (peuvent diverger) ! Il est donc primordial de se demander

si le design du produit autorise l'utilisateur à prendre les décisions conformes à ses objectifs ou ses besoins, ou s'il l'entraîne plutôt à prendre les décisions qui correspondent aux objectifs commerciaux du fournisseur. En d'autres termes, l'utilisateur est-il client ou produit du fournisseur ?

Si l'utilisateur n'est qu'un produit et qu'un procédé ou **un design oriente le comportement des utilisateurs de telle sorte qu'ils les pousse à des actions qu'ils ne voulaient pas ou n'avaient pas prévues au départ, on parle alors d'un « dark pattern ».**

Les dark patterns se basent sur un nombre gigantesque de mécanismes d'influence différents et ne se limitent pas à un seul domaine ou type de produits. Les dark patterns exploitent les comportements humains tels que **l'inattention, le confort ou les attentes.**

De ce fait il existe ainsi des formes plus douces d'influence qui s'apparentent aux pratiques de marketing et de ventes courantes, avec parfois une dérive vers les dark patterns. L'influence de ces derniers peut finalement entraîner des coûts plus élevés, la vente de données personnelles ou la violation de droits, notamment celui de l'autodétermination informationnelle.

3. Alors, les dark patterns sont-ils bénéfiques ou nuisibles pour l'utilisateur ?

À la question de savoir si un design sera bénéfique ou nuisible, **la réponse se fera au cas par cas. En fin de compte, l'expérience utilisateur est unique.** Pensez par exemple aux recommandations à la fin d'un article sur votre fil d'actualité ou de votre panier. Ces conseils sont personnalisés et se basent probablement sur vos autres activités en ligne. Alors que vous vous réjouissez peut-être parce que cela vous aura épargné d'autres recherches et fait gagner du temps, d'autres ne trouveront probablement pas cela bénéfique, mais plutôt dérangeant. En outre, il est possible que vous restiez plus longtemps que prévu sur le site ou que vous achetiez un produit que vous n'aviez pas l'intention d'acheter.

Selon la définition du Comité européen de la protection des données (voir encadré page 2), pour parler de dark patterns dans les médias sociaux, il faut que ceux-ci poussent les utilisateurs à prendre des décisions ayant des conséquences potentiellement négatives en rapport avec leurs données personnelles. En d'autres termes, **les dark patterns représentent un risque pour les utilisateurs d'Internet.** [La classification élargie de la « EU Kids online classification » du projet CO:RE « The 4 Cs: Classifying online risk to children »](#), établie au niveau international et regroupant en grandes catégories tous les risques principaux pour les enfants lors de l'utilisation en ligne, arrive à la même conclusion. Depuis la révision de cette classification en 2021, les dark patterns sont intégrés comme risque dans la catégorie « Contract Risk » (en français « risque contractuel »). Par conséquent, les dark patterns font partie des principaux risques auxquels sont confrontés les enfants lorsqu'ils utilisent Internet.

Finalement, l'utilisation d'un certain design, en particulier des dark patterns, a-t-elle des effets néfastes ? La réponse à cette question dépend beaucoup des objectifs poursuivis.

C'est pourquoi, en tant qu'utilisateur, vous devez vous demander :

- Est-ce que le design m'aide à agir comme je le souhaite ?
- Est-ce que je poursuis toujours mon propre but ?
- En tant qu'utilisateur, suis-je à cet instant client ou produit du fournisseur ?
- Quel est le résultat de mon action actuelle ?

4. À quoi ressemblent les dark patterns : exemples les plus courants

Il est pratiquement impossible de surfer en ligne sans rencontrer de dark patterns. Voici quelques exemples courants avec leurs mécanismes et modes d'action respectifs :

- **Bannière de cookies** : ce sont les dark patterns les plus courants que les utilisateurs rencontrent. Depuis l'instauration [du nouveau règlement général sur la protection des données](#) en 2018, les utilisateurs sont invités, par le biais de bandeaux ou de pop-ups, à transmettre des données privées pour ainsi dire à chaque visite de site internet. La plupart du temps, on dirait qu'une seule réponse est possible, celle « d'accepter tous les cookies ». Or, les possibilités de choix ou l'option de réponse négative ne sont soit pas proposées, soit seulement de manière cachée. Comme l'attention et l'action de l'utilisateur sont orientées activement sur l'action souhaitée par le fournisseur (« accepter tous les cookies ») – il s'agit d'un dark pattern.
- Le mécanisme selon lequel **le refus d'une action est plus difficile et plus chronophage que son acceptation** est un dark pattern utilisé pour de nombreuses opérations sur le web : en particulier lors de la résiliation de contrats. De même, souvent aussi dans le cadre de **tentatives de résiliation, des index du menu sont cachés, variables ou encore absents**, ce qui rend l'action de l'utilisateur difficile.

- **Préréglage** : La plupart du temps, les sites internet et les applications sont préréglés dans l'intérêt du fournisseur, de façon à apporter le plus grand avantage avec le choix par défaut. Certes, les préréglages peuvent être modifiés, mais c'est souvent compliqué et chronophage. Par conséquent, la majorité des utilisateurs conservent les préréglages même s'ils auraient fait d'autres choix de leur propre chef. Dans les années 1950, des scientifiques spécialistes de la recherche cognitive et de l'économie comportementale avaient déjà découvert que la surinformation entraînait l'incapacité d'action. Les personnes confrontées à un trop grand nombre de choix préfèrent ne pas prendre de décision et acceptent les préréglages.
- L'utilisation d'un **design confus, de formulations équivoques ou d'une organisation déconcertante** : l'apparence et la langue jouent également un rôle prépondérant. Les formulations inversées telles que « Je ne souhaite pas m'abonner à la newsletter », l'utilisation de différentes tailles, polices et couleurs, notamment pour les cases à cocher « Accepter » et « Refuser », compliquent l'action de l'utilisateur. C'est probablement ce qui favorise le clic hâtif et erroné.
- **Confirmshaming** : comme le nom l'indique, il s'agit de faire honte à l'utilisateur lorsqu'il n'agit pas comme voulu. Ainsi, des possibilités d'actions sont certes proposées mais, en même temps, expriment un jugement par une formulation particulière. Il s'agit par exemple de « Je ne soutiens pas une bonne cause » ou « Je ne souhaite pas être informé/e ». Des pop-ups supplémentaires indiquant à nouveau la décision supposée erronée (« Êtes-vous sûr/e, que... ») et exigeant un nouveau clic, relèvent du confirmshaming.



Le Hall of Shame des dark patterns :
www.deceptive.design/hall-of-shame/all

- Dans le domaine de [l'achat en ligne](#) : si le champ de recommandation sous un produit ou l'avertissement « les clients qui ont acheté le produit A ont également acheté le produit B » peuvent aider à comparer des produits, ils peuvent aussi inciter à effectuer d'autres achats. **La pénurie fictive, les prétendues fortes demandes d'un produit ou les décomptes simulés** font partie des astuces techniques des fournisseurs. Ils ne sont pas toujours conformes à la réalité et servent à exercer une pression auprès des acheteurs potentiels afin d'accélérer le processus d'achat. Ainsi, les comptes à rebours pour les achats « limités dans le temps » sont réinitialisés, notamment à chaque fois que la page est téléchargée. Et/ou les références et les indications de fortes demandes ou de stocks bas sont falsifiées. Certains fournisseurs **placent des produits supplémentaires dans le panier**. Il s'agit classiquement de services supplémentaires comme les assurances lors de la réservation d'un voyage ou de variantes premium d'abonnements. Si ces produits supplémentaires sont clairement identifiés, ils peuvent au contraire ne pas être remarqués lors du processus d'achat si on ne s'y attend pas.
- Les **lectures automatiques** sur les services de streaming tels que Netflix ou sur YouTube sont amusantes, font gagner du temps et suscitent la plupart du temps l'intérêt des utilisateurs grâce aux algorithmes, mais peuvent aussi entraîner le binge watching. En outre, le mode de lecture automatique est souvent déjà préconfiguré par défaut, de sorte que les utilisateurs doivent le quitter activement au lieu de le choisir eux-mêmes.
- Dans les **jeux en ligne** : en raison de leur design, les jeux en ligne peuvent [comporter différents risques](#). Les applications gratuites en particulier (comme p. ex. Free2Play), qui, par leur modèle économique, sont attractives pour les enfants et les jeunes, peuvent rapidement devenir des [gouffres de finances et de données](#). Ainsi, en 2020, seuls onze millions d'euros ont été générés par l'achat d'applications en tant que tel, alors que les achats in-apps (c.-à-d. dans les applications) ont rapporté 2 264 millions d'euros. La version de base étant gratuite, ce sont en effet les

extensions et options similaires payantes proposées ultérieurement qui génèrent les gros bénéfices. D'autres [formes pertinentes de dark patterns dans les jeux en ligne](#) sont les time patterns (fidéliser le joueur avec des avantages, des récompenses et des expériences positives), les money patterns (stimuler le joueur à l'aide de microtransactions opaques), les social patterns (exercer une pression sociale sur les joueurs) et les psychological patterns (duper les joueurs).

- Par ailleurs, sur les **réseaux et les médias sociaux**, d'autres mécanismes tels que **les systèmes de récompense ou - au contraire - l'effet « fear of missing out »** sont utilisés pour conserver un engagement élevé des utilisateurs. C'est à cela que servent l'attribution de likes ou le partage de contenus et d'articles, tout comme la production de contenus et de snapstreak sans cesse renouvelés.



Dark patterns : phénomène nouveau ou ancien ?

Les dark patterns ne sont pas vraiment un phénomène nouveau. Depuis toujours, les entreprises ont essayé d'attirer leurs clients (potentiels) et d'exercer une influence sur leur comportement. Que ce soit par le biais d'un discours précis, d'emballages marquants, d'une publicité attirant l'attention du consommateur ou du simple placement de produit dans les supermarchés. Ce qui est nouveau n'est donc pas le phénomène (de tenter) d'influencer mais le transfert par analogie dans l'espace numérique où l'impact est considérable. En effet, les interfaces numériques s'adaptent nettement plus facilement, de manière plus dynamique et individuelle aux souhaits et au comportement des clients que les méthodes conventionnelles de marketing et de vente dans les rayons du magasin ou sur une affiche publicitaire. En outre, il est plus facile de configurer les différents outils et de mesurer leur impact.

5. Ont-ils le droit ? À propos des règles, des zones grises et des nouveaux défis

Les dark patterns, comme phénomène de masse, sont assez récents dans le monde en ligne. Ils s'accompagnent de **nouveaux défis pour la protection des données de**

tous les consommateurs et en particulier des enfants et des jeunes ainsi que pour la régulation des médias et des plateformes. À l'heure actuelle, de plus en plus de personnes de la société civile et politique réclament une réglementation et des interdictions de telles pratiques. Ils exigent que ce qui n'est pas autorisé hors ligne soit également interdit en ligne. La question de savoir si, jusqu'à présent, les lois existantes suffisent à protéger les utilisateurs des manipulations et des abus en rapport avec tous les dark patterns définis, reste à éclaircir. Selon une expertise sur le cadre juridique des dark patterns commandée par la Fédération allemande du commerce en ligne et de la vente par catalogue (BEVH), une interdiction totale des « dark patterns » ne serait pas nécessaire en raison [des conditions cadres du droit fondamental en vigueur \(comme la liberté contractuelle, la liberté entrepreneuriale, et les droits fondamentaux relatifs à la protection des données\) et du modèle de référence du consommateur](#). D'après cette expertise, cela signifierait aussi bien des interventions injustifiées dans la liberté contractuelle et à la liberté d'entreprise ainsi qu'une mise sous tutelle des utilisateurs, ce qui ne serait pas compatible avec l'image d'un consommateur majeur. En 2022, le Comité européen de la protection des données a publié [des directives sur les dark patterns dans les interfaces utilisateurs des médias sociaux](#), dont notamment celles qui expliquent comment les reconnaître en tant qu'utilisateur, et comment les éviter en tant que fournisseur.

Aujourd'hui, les designs à risque ne sont pas encore bien définis juridiquement sous le terme générique « dark patterns ». Il convient donc de décider au cas par cas ce qui peut être défendable en fonction de la législation actuelle et ce qui ne l'est pas. Une nouvelle réglementation européenne, le « Digital Services Act », mettra à l'avenir le fournisseur face à ses responsabilités en ce qui concerne les dark patterns, l'objectif étant de mieux protéger les utilisateurs (voir encadré page 6).

Toutefois, cela vaut la peine d'examiner dès à présent les offres digitales existantes qui prennent en compte

les objectifs des utilisateurs dans le but de les soutenir. Certaines mettent par exemple des outils à disposition des utilisateurs, leur permettant de suivre le temps qu'ils passent sur les différentes applications et sites internet. Pour les utilisateurs intéressés, cela peut être un moyen efficace pour entretenir, avec ce « point de vue extérieur », un rapport plus conscient au temps et à l'attention accordés au monde numérique.



Le Digital Services Act :

- Le [Digital Services Act](#) a été ratifié en juillet 2022 par le Parlement européen et doit prendre effet à l'automne 2022 (situation en juillet 2022).
- Le règlement qui entrera en application dans deux ans dans toutes l'UE a pour objectif de mieux protéger les utilisateurs et les consommateurs d'offres numériques. Il doit garantir davantage de transparence des plateformes et de leurs mécanismes internes (algorithmes), imposer des mesures contre les contenus illégaux et les offres illégales et limiter la publicité ciblée à l'individu.
- Il comporte également un article visant spécialement les dark patterns, qui stipule qu'il est interdit au fournisseur de plateforme en ligne d'utiliser des designs et interfaces susceptibles de mal orienter les utilisateurs, de les manipuler ou de les empêcher par ailleurs de prendre les décisions en connaissance de cause.
- Cependant, la jurisprudence devra encore montrer comment identifier et selon quels critères précis exactement, sanctionner et empêcher les dark patterns.

6. Vous pouvez vous protéger !

Les dark patterns sont un phénomène omniprésent avec des défis pour toute la société. Il est donc important de connaître et de reconnaître leurs mécanismes et leurs modes opératoires. À noter que de nombreuses personnes ont déjà l'habitude de manipuler les dark patterns de manière réfléchie.

Les astuces suivantes peuvent vous y aider :

- **Parlez** avec les enfants, la famille, les amis et les collaborateurs de ce sujet et aidez les personnes de votre entourage pour qui ce sujet est nouveau.



Documentaire Netflix : « Derrière nos écrans de fumée »

Le documentaire américain (« The Social Dilemma » en anglais) aborde de manière critique les conséquences des médias sociaux pour la société. Tout au long du portrait d'une famille fictive américaine, on explique comment les designs web et les données collaborent étroitement pour influencer la prise de décision des utilisateurs. Il s'agit explicitement de l'utilisation excessive des médias sociaux (avertissement de contenu sensible) et d'interviews de différentes personnalités américaines issues des grandes entreprises de médias sociaux. Le design des comptes des médias sociaux comme forme de dark patterns joue ici un rôle important.

- **Soyez toujours critique** : Abordez toujours attentivement le design des interfaces utilisateur et demandez-vous de manière critique quels sont les objectifs recherchés par le fournisseur avec le design.
- **Ne perdez pas de vue votre objectif** : De quoi avez-vous réellement besoin en ce moment ? Est-ce que, finalement le design/le chemin dirigé vous aide à atteindre le but recherché ?
- **Prenez votre temps** : Lisez tranquillement les pop-ups, les options et autres éléments similaires. Ne précipitez aucune transaction, ni contrat ni opération semblable.
- **Faites bien attention à la formulation exacte et à la mise en forme** : De quoi s'agit-il exactement et êtes-vous d'accord avec cela ?
- **Protégez vos données** : Vous ne devez pas révéler plus d'informations sur vous que ce que vous souhaitez ! Il y a ensuite de nombreuses astuces et moyens techniques grâce auxquels vous pouvez naviguer en toute sécurité sur Internet.
- **Questionnez-vous** : En tant qu'utilisateur, suis-je en ce moment un client ou un produit de l'application du fournisseur ?
- Ne vous mettez **aucune pression et n'ayez pas mauvaise conscience** : En cas de doute, interrompez l'action et recommencez à un meilleur moment ou avec le soutien d'une autre personne.

7. Liens utiles

- Deceptive Design www.deceptive.design/reading-list/all
- La forme des choix https://linc.cnil.fr/sites/default/files/atoms/files/cnil_cahiers_ip6.pdf
- Dark Patterns – die dunklen Machenschaften der Unternehmen <https://recht-auf-audio.podigee.io/10-dark-patterns-die-dunklen-machenschaften-der-unternehmen>
- Les dark patterns ou l'art de tromper l'utilisateur www.la-rem.eu/2021/12/les-dark-patterns-ou-lart-de-tromper-lutilisateur/?print=pdf
- Guidelines 3/2022 on "Dark patterns in social media platform interfaces: How to recognise and avoid them" www.edpb.europa.eu/system/files/2022-03/edpb_03-2022_guidelines_on_dark_patterns_in_social_media_platform_interfaces_en.pdf
- Feedback on Guidelines 3/2022 on "Dark patterns in social media platform interfaces: How to recognise and avoid them" www.edpb.europa.eu/system/files/2022-05/comments_to_edpb_guidelines_on_dark_patterns_for_social_media_-_decepticon_unilu_0.pdf
- Dark patterns: sombres jeux d'influence sur le web www.frc.ch/sombres-jeux-dinfluence
- The 4Cs: Classifying Online Risk to Children www.ssoar.info/ssoar/handle/document/71817



Éditeur : Service national de la jeunesse (SNJ)

Service national de la jeunesse L-2926 Luxembourg
www.snj.lu
www.bee-secure.lu



Consulter la licence Creative Commons de cette publication :
www.creativecommons.org/licenses/by-nc-sa/4.0/deed.fr

Initié par :



Opéré par :



Cofinancé par :



Fiche thématique - Dark Patterns - 09.2022
ISBN 978-2-919796-58-8
Ressource électronique