_swissprivacy.law

Dark patterns : wait & see

Nathanaël Pascal, le 13 septembre 2024

Le Conseil fédéral a présenté son rapport « Dark patterns. Documenter la nébuleuse ». La présente contribution a vocation à en restituer les grandes lignes sous l'angle de la LPD et offre un survol de la pratique relative aux *dark patterns* dans le cadre des bannières cookies au sein de l'Union européenne, ainsi qu'un aperçu de la situation outre-Atlantique.

Rapport du Conseil fédéral, Dark patterns. Documenter la nébuleuse

Le 14 juin 2024, le Conseil fédéral a adopté le rapport « Dark patterns. Documenter la nébuleuse » qui a pour finalité de documenter le recours aux *dark patterns* sur internet (sites internet, plateformes en ligne et applications) et d'identifier si une adaptation de la législation en vigueur est nécessaire.

I. Définition

Selon une étude de la Commission européenne datant de 2022, 97% des sites e-commerce et applications les plus populaires au sein de l'Union contiennent des *dark patterns*. Toutefois, la Suisse n'est pas en reste comme en témoigne l'enquête conjointe de la Fédération romande des consommateurs et de Public Eye qui examine quinze grands sites de commerce en ligne spécialisés dans la mode à la recherche de vingt pratiques pouvant être identifiées comme des *dark patterns*. Le résultat est sans appel : la totalité des sites consultés ont recours aux *dark patterns*. Mais qu'est-ce qu'un « *dark pattern* » ? À l'heure actuelle, le droit suisse ne propose pas de définition juridique de cette notion contrairement au droit de l'Union européenne au sein de plusieurs actes normatifs :

« Les interfaces en ligne trompeuses de plateformes en ligne sont des pratiques qui ont pour objectif ou pour effet 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. » (considérant 67 DSA)

« Les interfaces trompeuses sont des techniques de conception qui poussent les consommateurs à prendre des décisions ayant des conséquences négatives pour eux ou qui les induisent en erreur à cette fin. » (considérant 38 Data Act)

« [des] interfaces et des expériences utilisateur mises en œuvre sur les plateformes de médias sociaux qui incitent les utilisateurs à prendre des décisions involontaires, non désirées et potentiellement préjudiciables en ce qui concerne le traitement de leurs données personnel » (CEPD, lignes directrices 03/2022 sur les designs trompeurs dans les interfaces de réseaux sociaux : comment les reconnaître et les éviter du 14 février 2023 ; traduction libre).

Nonobstant l'absence de définition unique au sein même du droit communautaire, l'ensemble des définitions prennent en compte le fait qu'il existe une interaction avec des utilisateurs qui les conduit à prendre une décision ne reflétant pas leur véritable intention et pouvant avoir des conséquences négatives pour eux.

Dans son rapport, le Conseil fédéral retient ainsi que les caractéristiques communes inhérentes aux *dark patterns* sont (i.) une conception numérique, (ii.) qui exploite des connaissances issues de la psychologie comportementale, (iii.) à destination de personnes physiques, indépendamment des motifs de leurs actions, et ce (iv.) au bénéfice du fournisseur, lequel exploite ainsi son pouvoir de conception à son propre avantage (v.) intentionnellement ou non. À la vue de ces éléments, le Conseil fédéral suggère de recourir aux termes de « *design* trompeur » et « *design* manipulateur ».

II. Classification des *dark patterns*

Compte tenu de la nature protéiforme des *dark patterns* qui peuvent se recouper ou combiner, le Conseil fédéral dresse une liste exemplative de *dark patterns* les plus fréquents, dont :

1) Paramètres par défaut : il s'agit d'une présélection d'offres ou de réglages par défaut prédéfinis pouvant ne pas être dans l'intérêt de l'utilisateur (p. ex. des cases pré-cochées).

2) Cadrage : recours à des techniques qui ont pour but d'encourager l'utilisateur à réagir ou à prendre la décision souhaitée par le fournisseur en utilisant des mots, des graphiques ou des éléments visuels spécifiques.

3) Formulations ambiguës : utilisation de formulations ambiguës susceptibles de prêter à confusion telle que le recours à la double négation dans des circonstances impromptues ou encore la dénomination trompeuse de boutons.

4) Piège à cafards : conception d'interfaces visant à piéger l'utilisateur, lequel ne pourra que,

par exemple, plus difficilement résilier un abonnement comparé à sa conclusion, ou encore faciliter le recueil du consentement de l'utilisateur et en complexifier sa révocation.

5) Harcèlement : il s'agit d'émettre des demandes répétées, voire agressives d'effectuer une action déterminée (p. ex. une fenêtre *pop-up* invitant à renseigner une adresse électronique).

6) Abonnement ou prolongation d'abonnement involontaire, inscription obligatoire : conception d'interfaces incitant l'utilisateur à conclure ou prolonger un contrat de façon indésirée, surprenante ou contre son gré.

7) Culpabilisation : l'utilisateur se voit exercer une pression, morale ou émotionnelle, notamment en recourant à la peur ou à la culpabilité afin de l'orienter vers une option plutôt qu'une autre. En pratique, cela peut prendre la forme d'un message informant l'utilisateur qu'il ne pourra pleinement accéder au contenu du site internet consulté en raison de son refus en matière de traçage.

Le Conseil fédéral scinde les *dark patterns* en deux catégories : ceux conçus de sorte à induire l'utilisateur en erreur ou à tromper ce dernier afin de l'influencer ; et ceux conçus en vue d'exercer une pression ou une contrainte sur l'utilisateur.

III. Appréhension des *dark patterns* par la LPD

La neutralité technologique de la LPD permet de saisir les *dark patterns* existants. En outre, cette neutralité a pour corolaire la capacité de s'adapter aux évolutions technologiques ce qui permettra à la LPD de saisir, tant les mutations futures que l'apparition de nouveaux *designs* trompeurs.

L'utilisation de *dark patterns* peut se révéler contraire aux principes du traitement des données à divers égards. Elle peut notamment générer plus de données personnelles que nécessaire pour fournir un service, conduire des personnes physiques à la communication de données non-nécessaires au traitement, à procéder à une telle communication en absence de connaissance de la finalité du traitement, pouvant violer de la sorte les principes de la proportionnalité (art. 6 al. 2 LPD) et plus particulièrement dans son acceptation de principe de minimisation des données, mais également les principes de transparence et de la bonne foi (art. 6 al. 2 et 3 LPD), de finalité (art. 6 al. 3 LPD) et faillir à son devoir d'information (art. 19 LPD).

Toutefois, l'utilisation de *dark patterns* peut être justifiée par des intérêts privés prépondérants du fournisseur (art. 31 LPD). Afin de déterminer si l'atteinte à la personnalité est justifiée, il convient de procéder à une pesée des intérêts entre ceux du responsable du traitement (fournisseur) et celui de la personne concernée à ce que sa liberté de disposer de ses données personnelles soit préservée. Figure parmi les cas d'intérêt privé prépondérant de l'art. 31 al. 2 LPD le motif relatif au traitement de données en relation directe avec la conclusion ou l'exécution d'un contrat (art. 31 al. 2 let. a LPD), lequel peut sembler pertinent *prima facie*.

Afin que le fournisseur puisse se prévaloir de ce motif justificatif, le traitement concerné doit être limité aux données personnelles nécessaires à la conclusion et à l'exécution du contrat. Néanmoins, il appert en pratique que les fournisseurs tentent régulièrement de traiter, notamment lors de la collecte, davantage de données personnelles que nécessaire à la conclusion ou l'exécution du contrat. De ce fait, les fournisseurs sont contraints de recueillir le consentement de l'utilisateur qui constitue un motif justificatif n'intervenant qu'en dernier lieu en raison de ses spécificités, notamment le droit pour l'utilisateur de refuser de fournir son consentement ou encore de retirer celui-ci en tout temps. Au surplus, le consentement n'est valable que si l'utilisateur exprime librement sa volonté concernant le traitement déterminé et après avoir été dûment informé (art. 6 al. 6 LPD).

Or la libre expression de la volonté et l'information sont deux aspects capitaux en ce qui concerne les *dark patterns*. En effet, le recours aux *dark patterns* susmentionnés de paramètres par défaut et de formulations ambiguës sont problématiques à l'égard de l'information. Pour ce qui est de la composante relative à la libre expression de la volonté, nous pouvons nous interroger quant au degré d'influence permettant de considérer que le consentement a été donné librement lorsque l'utilisateur est confronté au cadrage, au piège à cafards, au harcèlement ou encore à la culpabilisation.

Dans ce cadre, le Conseil fédéral relève que le fait, pour un fournisseur de médias sociaux, de faire dépendre l'utilisation de ses services au recueil du consentement à de nombreux traitements de données peut s'avérer illicite, notamment en cas d'enregistrement obligatoire. Cette position du Conseil fédéral se recoupe avec celle du Préposé fédéral à la protection des données et à la transparence (PFPDT) qui estime que l'obligation d'ouvrir un compte client pour procéder à un achat viole le principe de proportionnalité (cf. swissprivacy.law/299). En outre, il convient de soulever que le principe européen selon lequel il doit être aussi simple de retirer que de donner son consentement pourrait trouver application également en Suisse selon le Conseil fédéral.

Les *dark patterns* peuvent également influer sur l'exercice des droits des utilisateurs par le biais de conceptions visant à rendre ce dernier plus difficile. Il s'agit notamment du piège à cafards et de certaines formes de cadrage. Dans le premier cas, l'utilisateur se trouve empêché de supprimer tout ou partie de ses données personnelles. Dans le second cas, le cadrage ne permet pas à l'utilisateur de trouver aisément les informations nécessaires à l'exercice de ses droits.

Le Conseil fédéral constate que les dispositions de la LPD pourraient être violées lorsque des *dark patterns* sont employées, afin d'inciter les utilisateurs à divulguer plus de données qu'elles ne l'auraient fait consciemment ou à consentir à des traitements non voulus. En cas de violation de la LPD, l'utilisateur pourra notamment procéder à une dénonciation au PFPDT (art. 49 al. 1 LPD), lequel devra, s'il existe des indices suffisants laissant penser qu'un traitement de données pourrait être contraire à des dispositions de protection des données et que dite violation revêt une certaine importance, ouvrir une enquête et rendre des décisions (art. 49 ss LPD).

Nonobstant les pouvoirs conférés au PFPDT, les moyens dont disposent les utilisateurs sur le fondement du droit de la protection des données ne leur permettent pas de conclure à l'annulation d'un contrat lorsque le fournisseur a recouru à des *dark patterns* en vue de les inciter à conclure ou à prolonger un contrat sans qu'ils ne le souhaitent.

Estimant que la récente révision de la LPD contribue à ce que le droit en vigueur couvre les *dark patterns*, le Conseil fédéral conclut qu'il n'y a aucune nécessité de légiférer en la matière sous l'angle de la protection des données et qu'il convient d'observer l'évolution dans l'Union européenne (référence faite au DSA, DMA, Data Act et AI Act) ainsi que son impact sur la Suisse.

IV. Le cas des bannières cookies dans l'Union européenne

L'un des aspects les plus visibles et controversés de notre expérience en ligne, en tant qu'utilisateurs, est la bannière cookies. Ces bannières, censées recueillir notre consentement pour le suivi de notre activité en ligne, constituent un parfait exemple d'utilisation des *dark patterns*. En effet, il n'est pas rare de voir une combinaison de plusieurs *dark patterns* au sein d'une seule et même bannière, maximisant ainsi l'effet trompeur en vue de recueillir un consentement supposément libre.

Subséquemment à la publication du rapport du Conseil fédéral, l'association de protection de la vie privée et des données *noyb* a publié un rapport intitulé « *Consent Banner Report*

Overview of EU and national guidelines on dark patterns » (uniquement disponible en anglais) offrant une vue d'ensemble des lignes directrices européenne et nationales relatives aux *dark patterns.* Ladite association a effectué une comparaison des conclusions contenues dans le rapport « *Report of the work undertaken by the Cookie Banner Taskforce* » émis par la task-force du CEPD pour chaque violation des bannières cookies avec les positions adoptées par les autorités nationales de protection des données dans leur documentation ainsi que dans les décisions rendues.

Dans ce rapport, huit pratiques spécifiques sont identifiées desquelles découle des consentements viciés :

1) L'absence de bouton de rejet au premier niveau d'information : tant la taskforce du CEPD que diverses autorités de protection des données nationales européennes (ci-après : APD) considèrent que l'absence de cette option enfreint les conditions posées en matière de recueil du consentement. Au surplus, le fait que refuser de consentir à un traitement de données requiert plus d'étapes que de l'accepter ne permet pas de recueillir un consentement valide en raison de la pression exercée sur l'utilisateur afin que ce dernier accepte les cookies, et ce, notamment en contradiction avec le principe de transparence du RGPD.

2) Les cases pré-cochées : les bannières contenant des cases pré-cochées qui contraignent l'utilisateur à procéder à leur décochage pour refuser de consentir au traitement imposent un effort supplémentaire par rapport à un consentement fourni en un seul clic et ne constitue pas un consentement valable. En effet, un consentement recueilli par ce biais ne reflète pas une manifestation de volonté active ni une décision éclairée de la part de l'utilisateur.

3) La conception trompeuse de liens : lorsque l'utilisateur est confronté à un bouton « tout accepter » et à l'option « refuser » qui n'apparaît que sous la forme d'un lien, lequel est fréquemment dissimulé dans un paragraphe de texte, l'utilisateur est poussé à croire qu'il n'y a pas d'autre option que de « tout accepter ». La conséquence du recours à un tel *dark pattern* est de tromper et induire en erreur l'utilisateur moyen, de sorte que le consentement recueilli est vicié.

4) Les couleurs trompeuses des boutons : des fournisseurs emploient des couleurs différentes pour les options disponibles de sorte à mettre en avant le bouton « tout accepter » (souvent de couleur verte par opposition à des couleurs grisées voire rouges). Ceci contrevient au principe de loyauté et de transparence (art. 5 para. 1 let. a RGPD) et le consentement fourni par l'utilisateur est entaché d'ambiguïté.

5) Le contraste trompeur des boutons : ce cas de figure s'apparente au précédent car il s'agit de l'utilisation de différents ratios de contraste pour les options présentées afin de mettre en avant l'option « tout accepter ». Alors que la taskforce du CEPD retient qu'une analyse au cas par cas est requise pour évaluer la loyauté et transparence de la bannière, certaines APD adoptent une position plus tranchée. Cela est notamment le cas de la *Datenschutzkonferenz* (DSK) qui a retenu que l'option de refuser de consentir au traitement doit être clairement présentée comme une alternative équivalente à l'option de donner le consentement, ce qui est présumé lorsqu'il y a, à côté du bouton « tout accepter », un bouton « continuer sans accepter » particulièrement similaire en termes de taille, de couleur, de contraste et de police de caractère.

6) La revendication d'un intérêt légitime à tort : bien que l'intérêt légitime du fournisseur ou d'un tiers (art. 6 para. 1 let. f RGPD) soit invoqué pour des traitements figurant dans la bannière cookies, tant le stockage que l'accès aux informations stockées dans l'équipement terminal (à l'exception des cookies essentiels) ne peuvent être fondés que sur le consentement de la personne concernée conformément à l'art. 5 para. 3 ePrivacy. La taskforce du CEPD a estimé que le non-respect de cette disposition a pour corollaire que tout traitement ultérieur ne peut être conforme au RGPD.

7) La mauvaise classification des cookies :il se peut que des cookies soit classés comme « essentiels » ou « strictement nécessaires » de manière erronée. Un tel classement conduit à l'impossibilité pour l'utilisateur de refuser ces traitements, permettant ainsi au fournisseur de stocker et d'accéder à des informations sur l'équipement de l'utilisateur avant toute interaction de ce dernier avec la bannière cookies. La taskforce du CEPD a observé qu'il existe des outils permettant de générer un rapport listant l'ensemble des cookies placés sur le terminal de l'utilisateur, mais que ces outils ne permettent d'aucune manière que ce soit de vérifier la nature desdits cookies et ce notamment en raison du fait que les caractéristiques des cookies changent régulièrement ce qui ne permet pas d'établir une liste stable et fiable des cookies essentiels. Afin de juger du caractère essentiel du cookie concerné, les APD se fondent notamment sur l'avis du Groupe de travail « article 29 » relatif à l'exemption de l'obligation de consentement pour certains cookies datant de 2012. La *Datenschutzbehörde* (DSB) précise que le caractère essentiel du cookie ne doit pas être interprété du point de vue du fournisseur mais de l'utilisateur.

8) La difficulté accrue pour retirer le consentement en comparaison de son recueil : en vertu de l'art. 7 para. 3 *in fine* RGPD, il doit être aussi simple de retirer que de donner son consentement. De la sorte, si une option de consentement est visible de manière proéminente, il doit

en être de même de l'option de retrait. En pratique, cette exigence peut notamment être assurée par le biais d'icônes flottantes et visibles de manière permanente renvoyant aux paramètres de gestion du consentement. La DSB a précisé que les options de retrait doivent être clairement décrites dans la bannière cookie, laquelle doit indiquer comment et où le consentement peut être retiré.

Par conséquent, il appert que les pratiques couramment observées dans les bannières cookies ne respectent pas la législation européenne en vigueur. Les techniques identifiées, telles que l'absence de bouton de rejet accessible au premier niveau d'information, l'utilisation de cases pré-cochées et les manipulations visuelles (couleurs et contrastes), ne permettent pas le recueil d'un consentement valable, de sorte que les fournisseurs doivent veiller à prévoir un mécanisme de recueil de consentement en adéquation avec la position du CEPD et porter une attention particulière à la position adoptée par les DPA afin de se conformer aux potentielles spécificités nationales.

V. Les *dark patterns* outre-Atlantique

Les États-Unis ont saisi la problématique des *dark patterns* au niveau fédéral et étatique. Sur le plan fédéral, nous pouvons observer l'obligation faite aux fournisseurs d'indiquer de manière transparente les conditions importantes avant que le client ne leurs communique leurs informations de facturation (*Restore Online Shoppers' Confidence Act*).

À l'échelle des États, la Californie (« *California Privacy Rights Act of 2020* » (CPRA)), le Colorado (« *Colorado Privacy Act* » (CPA)) et le Connecticut (« *Virginia Consumer Data Protection Act* » (VCDPA)) ont adopté des textes avec des incidences sur l'utilisation de *dark patterns*.

Au cours des dernières années, la *Federal Trade Commission* (FTC) s'est saisie de la problématique. En 2022, elle a publié un rapport intitulé « *Bringing Dark Patterns to Light* » qui examine les façons dont les interfaces masquent ou entravent l'autonomie des consommateurs dans la prise de décision. Ce rapport met en lumière quatre finalités particulières des *dark patterns* :

1) Tromper les consommateurs et dissimuler la publicité : il s'agit des interfaces qui créent de fausses croyances, comme les comptes à rebours qui laissent faussement entendre qu'il s'agit d'offres à durée limitée, mais également les publicités présentées de manière trompeuse pour ressembler à un contenu éditorial indépendant, ainsi que des sites de comparaison d'achats prétendument neutres qui opère en réalité un classement des entreprises en

fonction de leur rémunération.

2) Rendre la résiliation difficile : une autre pratique consiste à complexifier notamment la résiliation des abonnements et des offres d'essai gratuit en obligeant le consommateur à suivre un processus d'annulation complexe, difficilement accessible, long et confus qui peuvent, en outre, contenir des liens redirigeant le consommateur hors du processus d'annulation.

3) Dissimuler des termes clés et des coûts : en recourant à la dissimulation ou l'obscurcissement d'informations essentielles au consommateur (p. ex. limitations du produit consulté, frais cachés) dans des conditions générales d'utilisation complexes, les fournisseurs attirent le consommateur en affichant une fraction du prix final et ne révèlent les frais supplémentaires qu'à la fin du processus d'achat.

4) Tromper les consommateurs pour qu'ils fournissent davantage de données personnelles : en offrant un prétendu choix au consommateur concernant les paramètres de confidentialité ou le partage des données, le fournisseur a conçu l'interface de sorte à inciter le consommateur a divulgué le plus de données personnelles.

En dépit des efforts réglementaires, les cas d'application continuent de souligner la nature omniprésente des *dark patterns* comme peut en témoigner l'accord conclu en 2023 entre la FTC et un éditeur de jeux vidéo pour un montant de plus d'un demi-milliard de dollars (voir en ce sens le communiqué de la FTC). Selon la FTC, la disposition de l'interface de l'un des célèbres jeu vidéo de l'éditeur était caractérisée par des placements de boutons contre-intuitifs, incohérents et prêtant à confusion, qui facilitait les frais involontaires avec une seule pression sur un bouton. Par ailleurs, la FTC avait invoqué le fait que l'éditeur avait déplacé et minimisé le bouton permettant d'annuler l'achat et avait également conçu un long processus à destination du consommateur qui chercherait à obtenir des remboursements. Au surplus, la FTC avait formulé un grief selon lequel l'éditeur aurait facilité le processus d'achat pour les joueurs mineurs en contournant la nécessité d'obtenir une approbation parentale.

Les cas d'application, tels que l'accord susmentionné, illustrent la volonté de la FTC de sanctionner les entreprises recourant aux *dark patterns* afin de tromper leur clientèle. Cela dénote une tendance vers une surveillance accrue et d'importantes sanctions financières pour dissuader les fournisseurs de recourir à de telles pratiques et protéger les consommateurs, en particulier les plus vulnérables, comme les mineurs.

VI. Conclusion

L'adoption du rapport « Dark patterns. Documenter la nébuleuse » du Conseil fédéral marque une étape significative dans la reconnaissance par les autorités des défis posés par les *dark patterns*. La mise en œuvre des principes de *privacy by design* et *by default* sous la LPD révisée constitue un progrès notable vers une protection accrue des données personnelles. Néanmoins, il convient de souligner que, malgré cette avancée helvétique, l'application de la législation pourrait se révéler limitée en raison de l'opacité inhérente aux *dark patterns* et de la difficulté pour l'utilisateur de se constituer des moyens de preuve.

La démocratisation de l'intelligence artificielle générative soulève des préoccupations nouvelles quant à la capacité de ces technologies à créer des *designs* trompeurs hautement personnalisés susceptibles d'altérer la rationalité des utilisateurs de manière plus subtile et sophistiquée. Une observation attentive de l'efficacité des dispositifs réglementaires européens et de leurs éventuelles répercussions sur la situation des justiciables suisses doit être réalisée afin de permettre au législateur de revoir, en temps opportun, sa position quant à la nécessité de légiférer en la matière.

Dans l'attente d'une éventuelle adaptation législative et en vue d'assurer la sécurité juridique, il est crucial, tant pour les utilisateurs que pour les fournisseurs, que des critères objectifs délimitant la persuasion acceptable de la tromperie soient établis.

Proposition de citation : Nathanaël Pascal, Dark patterns : wait & see, 13 septembre 2024 *in* www.swissprivacy.law/316