Dark Patterns : le CEPD présente ses lignes directrices

David Dias Matos, le 23 avril 2022

Le Comité européen de la protection des données a présenté son projet de lignes directrices sur les *Dark Patterns* dans les interfaces de médias sociaux. La présente contribution en restitue les grandes lignes.

Comité européen de la protection des données (CEPD), Lignes directrices 3/2022 sur les interfaces truquées (« *dark patterns* ») dans les interfaces des plateformes de médias sociaux (disponibles uniquement en anglais à ce jour).

Le 21 mars 2022, le CEPD a publié un projet de lignes directrices 3/2022 sur les interfaces truquées (« *Dark Patterns* ») dans les interfaces des plateformes de médias sociaux (Lignes Directrices). Leur but est d'offrir des recommandations pratiques aux développeurs et utilisateurs de médias sociaux afin d'évaluer et d'éviter les *Dark Patterns* dans les interfaces de plateformes de médias sociaux qui contreviennent aux exigences du RGPD. Le CEPD définit les *Dark Patterns* comme :

> « des interfaces et des expériences utilisateur mises en œuvre sur les plateformes de médias sociaux qui amènent les utilisateurs à prendre des décisions involontaires, non désirées et potentiellement préjudiciables en ce qui concerne le traitement de leurs données à caractère personnel ».

Il les classe en 6 catégories principales :

1. **Surcharge** (« ***Overloading*** ») : l'utilisateur est confronté à une grande quantité de demandes, d'informations, d'options ou de possibilités pour l'inciter à partager plus de données.
2. **Saut** (« ***Skipping*** ») : concevoir l'interface ou l'expérience de l'utilisateur de sorte que celui-ci oublie ou ne considère pas tous ou certains aspects de la protection des données.
3. **Émotions** (« ***Stirring*** ») : faire appel aux émotions des utilisateurs ou utiliser des stimuli.
4. **Entraves/Obstacles** (« ***Hindering*** ») : bloquer ou empêcher l'utilisateur de s'informer

sur l'utilisation de ses données ou d'exercer un contrôle sur celles-ci en rendant certaines actions difficiles ou impossibles à réaliser (p. ex. en créant plus d'étapes pour l'utilisateur, qui souhaiterait limiter la collecte de ses données).

5. **Incohérence** (« ***Fickle*** ») : concevoir l'interface de manière incohérente et peu claire, ce qui rend difficile la navigation dans les différents outils de contrôle de protection des données ou la compréhension des finalités du traitement.
6. **Laissé dans le noir** (« ***Left in the dark*** ») : concevoir les interfaces de manière à masquer l'information, les paramètres, ou à laisser les utilisateurs dans l'incertitude quant à la manière dont leurs données sont traitées et au contrôle qu'ils peuvent exercer sur celles-ci.

Pour le CEPD, ces 6 catégories peuvent être regroupées en *patterns* basés sur le contenu ou sur l'interface. Les premières portent sur le contenu de l'information comprenant la formulation, le contexte et les composantes informationnelles. Les deuxièmes se réfèrent à la manière dont le contenu est visuellement présenté et comment l'utilisateur peut interagir avec.

Les Lignes Directrices sont construites autour des cinq étapes de la vie d'un compte d'utilisateur de médias sociaux, à savoir : (1) ouvrir un compte ; (2) rester informé sur le média social ; (3) rester protégé sur le média social ; (4) exercer ses droits personnels liés aux données ; et (5) quitter un média social.

(1) Ouvrir un compte

Le CEPD prend pour point de départ l'exigence du consentement au moment de l'ouverture d'un compte sur un média social. Il rappelle que le consentement doit être clairement distinct. Partant, il ne peut pas être inclus dans les conditions d'utilisation et/ou la politique de confidentialité qui devraient impérativement être acceptées pour accéder à la plateforme.

La position du CEPD sur le retrait du consentement est intéressante. Le Comité adopte une position stricte, expliquant que celui-ci ne peut être considéré comme un motif de licéité du traitement acceptable si sa révocation nécessite plus d'étapes que celles nécessaires pour le donner. Concrètement, si un « clic » suffit pour consentir, un « clic » devrait aussi suffire pour refuser ou retirer son consentement.

En transposant cette règle à une situation connue, comme celle des *cookies*, cela semble particulièrement difficile à mettre en place. En effet, le consentement des utilisateurs se fait généralement en un clic sur un *pop-up*. Or le simple fait d'accéder aux réglages pour déco-

cher la case serait déjà considéré « de trop ». Cet écart entre la règle et la réalité devrait sans doute encore être éclairci.

Il est intéressant de relever que le *Landgericht* de Rostock en 2020 déjà, avait examiné la question de la présentation des *cookies banners* et des *Dark Patterns*. Le Tribunal allemand dans son arrêt (LG Rostock, du 15.09.2020, 3 O 762/19) a décidé qu'un bouton « refuser » doit apparaître aux côtés de celui qui permet d'accepter et que ces deux boutons ne peuvent différer que par leur texte. Du reste, ils doivent être identiques en taille, police et couleur.

(2) Rester informé sur les médias sociaux

Le CEPD explique que, malgré les prescriptions de transparence et d'information du RGPD (art. 12–14), « plus d'information ne signifie pas nécessairement une meilleure information. Trop d'informations non pertinentes ou confuses peuvent masquer les points importants du contenu ou réduire les chances de les trouver ».

Le CEPD illustre cette situation par l'utilisation de *Dark Patterns* qui fournirait des informations contradictoires, avec une formulation ambiguë, présentée sans hiérarchie ni logique, se répétant plusieurs fois et/ou très difficile à trouver.

Pour cette raison, le CEPD recommande de mettre en place une politique de confidentialité étagée permettant à la fois de rendre accessible et compréhensible l'information. Une telle politique de confidentialité peut par exemple contenir une table des matières déroulante affichée en permanence sur l'écran et un bouton permettant de remonter rapidement au haut de la page.

(3) Rester protéger sur les médias sociaux et (4) exercer ses droits sur le média social

Le consentement doit pouvoir être retiré de manière aisée et à tout moment (art. 7 par. 3 RGPD). Il doit donc être possible de le retirer complètement ou partiellement pour certaines finalités (par exemple, uniquement pour le ciblage publicitaire).

Dans le cas de figure où, à l'ouverture d'un compte, l'utilisateur aurait déjà refusé certaines finalités, le responsable du traitement ne peut pas réitérer sa demande à chaque fois que l'utilisateur se connecte. L'utilisateur n'aurait alors d'autres choix que de consentir pour éviter cet obstacle et sa liberté s'en verrait indûment restreinte. Ce consentement serait donc considéré comme invalide.

Le CEPD préconise que les utilisateurs puissent adapter les paramètres de confidentialité durant toute la vie de leur compte. Le CEPD ne prévoit pas un nombre d'étapes (ou de clics) limite, mais insiste sur le fait que leur nombre doit être réduit au minimum. Une stratégie visant à proposer trop d'options, de (sous-) menus ou trop de pages différentes empêcherait un choix clair et surchargerait l'utilisateur. Le CEPD recommande aussi de centraliser les différents paramètres relatifs à la protection des données sur une seule page accessible à tout moment.

(5) Quitter un compte de média social

Au moment de quitter le compte, si l'exercice du droit à l'effacement de l'art. 17 RGPD est rendu difficile sans motifs le justifiant, cela constitue une violation du RGPD. De plus, l'exercice de ce droit doit être compris comme un retrait implicite du consentement, si le traitement se fondait sur le consentement, au sens de l'art. 7 par. 3 RGPD.

Pour cette dernière situation, le CEPD met en garde contre plusieurs *Dark Patterns* qui pourraient surgir. En utilisant des tournures telles que « vous allez tout perdre » ou encore « vos amis vont vous oublier » par exemple, la plateforme pourrait tenter de toucher l'affect de l'utilisateur pour le faire douter de sa décision de la quitter. Finalement, si l'information n'est pas assez claire et trop ambiguë, l'utilisateur ne serait pas en mesure de déterminer si son compte est bien effacé ou seulement suspendu temporairement.

Conclusion

Bien qu'encore au stade de projet, ces Lignes Directrices contribuent à un (nouveau) regard détaillé sur la manière de mieux protéger l'utilisateur de médias sociaux et influenceront les tribunaux et autorités dans leurs futures décisions relatives à ces thématiques.

Ces différents *Dark Patterns* peuvent aisément se retrouver sur d'autres interfaces que les médias sociaux. Elles serviront alors certainement de source d'inspiration pour mieux évaluer et juger les pratiques concernées ou pour aiguiller les développeurs de plateforme ou d'applications.

De surcroît, comme le relève à juste titre le CEPD, ces *Dark Patterns* peuvent aussi provoquer l'application des lois de protection des consommateurs ou de concurrence déloyale, ce qui nécessite donc une attention d'autant plus accrue du responsable du traitement.

Pour terminer, il y a lieu de mentionner que, le 22 avril 2022, le Conseil et le Parlement euro-

péen ont trouvé un accord provisoire sur la proposition de la Commission européenne de règlement européen sur les services numériques (*Digital Services Act*). Ce règlement ambitionne de s'appliquer à l'ensemble des intermédiaires en ligne fournissant des services dans l'Union européenne. Il imposerait des obligations proportionnées aux services concernés en fonction du nombre d'utilisateurs et viserait, entre autres, à interdire les *Dark Patterns*.

Proposition de citation : David Dias Matos, Dark Patterns : le CEPD présente ses lignes directrices, 23 avril 2022 *in* www.swissprivacy.law/138

Les articles de swissprivacy.law sont publiés sous licence creative commons CC BY 4.0.