

TYPOLOGIE DES DESIGN TROMPEURS liés à la protection des données au sein des réseaux sociaux

FAIRE OUBLIER (2)

❓ L'interface ou le parcours utilisateur sont conçus de sorte à ce que la **personne oublie**, voire de tout ou d'une partie des aspects liés à la protection de ses données personnelles.



Réglage intrusif par défaut

Par défaut, les fonctions et options **les moins respectueuses** de la vie privée et des données personnelles sont activées.



Détourner l'attention

Une action ou une information concernant les données personnelles est **mise en concurrence avec un autre élément**, en lien ou non avec les données. Lorsque les personnes se laissent distraire par cet élément, elles sont susceptibles d'oublier l'information ou l'option qu'elles cherchaient initialement.

INFLUENCER (2)

❓ Le choix des personnes est influencé en faisant appel à leurs **émotions** ou en utilisant des incitations visuelles.



Chantage émotionnel

Les personnes sont confrontées à des formulations ou des éléments visuels (ex. style, couleurs, images ou autres) qui donnent soit : une **impression très positive**, les personnes se sentant en confiance, en sécurité ou récompensées, une **impression très négative**, les faisant se sentir effrayées, coupables ou punies.



En toute discrétion

Utiliser un **style** ou une technique visuelle pour la présentation des informations ou des paramètres associés à la protection des données qui **incite les personnes à choisir des options moins restrictives** et donc moins protectrice de leur vie privée et de leurs données personnelles.

RESTER DANS LE FLOU (2)

❓ L'interface est conçue d'une manière qui **cache les informations** ou les paramètres liés à la protection des données.



Informations contradictoires

Les informations données aux personnes **se contredisent**. Les personnes ne peuvent pas savoir avec certitude comment réaliser les actions qu'elles souhaitent, ni si ces actions auront les effets recherchés. Elles sont donc **susceptibles d'abandonner** ce qu'elles voulaient paramétrer et de conserver les réglages par défaut.



Formulation ambiguë

Les informations comportent des **termes ambigus et vagues**. Les utilisateurs ne savent donc pas comment leurs données sont traitées ni comment paramétrer leurs préférences.

FAIRE OBSTACLE (3)

❓ Les personnes sont **gênées ou bloquées** dans leur recherche d'informations ou dans leur gestion de leurs données personnelles car ces actions sont rendues **difficiles voire impossibles** à réaliser.



Impasse

Alors que les personnes **cherchent** une information ou un paramètre, elles ne les trouvent pas car un lien de redirection **ne fonctionne pas ou n'existe pas du tout**. Les personnes se retrouvent dans l'impossibilité d'accomplir leur action.



Conséquences inattendues

Le **décalage** entre les informations fournies et les options à disposition des personnes les amène à effectuer une action qui ne correspond pas à ce qu'elles voulaient faire. La différence entre le résultat de l'action et ce que les personnes souhaitaient faire est susceptible de les **décourager d'aller plus loin**.

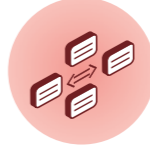


Rallonger le parcours

Lorsque les personnes essaient d'activer des réglages protecteurs de leurs données personnelles, elles doivent **passer par plus d'étapes** que pour configurer les autres réglages. Cet allongement du parcours est susceptible de leur faire abandonner le paramétrage de leurs préférences à la protection de leurs données.

RENDRE INCOHÉRENT (4)

❓ La conception de l'interface est **instable et incohérente**, ce qui rend difficile pour les personnes de comprendre et choisir la manière dont leurs données personnelles sont traitées.



Manque de hiérarchie

L'information concernant la protection des données manque de hiérarchie : les renseignements apparaissent plusieurs fois et sont **présentés de manière différente**.



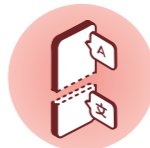
Hors contexte

Une information ou un paramètre en lien avec la protection des données personnelles est **fourni sans contexte** sur une page dont le sujet est différent.



Interface instable

Une interface n'a **pas de cohérence** dans différents contextes ou ne correspond pas aux attentes et aux habitudes des personnes qui l'utilisent.



Rupture linguistique

Les informations au sujet de la protection des données **ne sont pas dans la ou les langues officielles** du pays où vivent les personnes, alors que le reste du service l'est.

SURCHARGER (3)

❓ Les personnes sont **submergées** par une **masse de sollicitations**, d'informations, d'options ou de possibilités qui les dissuade d'aller plus loin et les oblige à conserver ou à accepter certaines pratiques en matière de données.



Sollicitation répétée

Les personnes sont poussées à fournir plus de données personnelles que nécessaire ou à accepter un nouvel usage de leurs données au travers de **demandes répétées** de fourniture de données ou de consentement à une nouvelle finalité.



Parcours labyrinthique

Lorsque les personnes souhaitent obtenir certaines informations, paramétrer des réglages ou exercer leurs droits, il leur est particulièrement difficile de les trouver car ils doivent **naviguer dans un trop grand nombre de pages**, sans en avoir un aperçu clair et complet.



Options en excès

Les personnes ont face à elles un (trop) grand nombre d'options parmi lesquelles choisir. Cette **quantité d'options** les empêche de faire un choix ou ne leur permet pas de voir certains paramètres, surtout si des renseignements ne sont pas mis à disposition.

Cette typologie a été établie dans les lignes directrices européennes :

Relatives aux interfaces trompeuses dans les interfaces des plateformes de médias sociaux : comment les reconnaître et les éviter ?
Adoptées le 14 février 2023 par le Comité européen de la protection des données (CEPD).

Elles ont pour but d'identifier des bonnes pratiques liées à l'interprétation du RGPD (règlement général sur la protection des données).

Principes du RGPD concernés

Chacun des designs trompeurs décrits dans cette typologie contrevient à un ou plusieurs des principes du RGPD liés :

- à la limitation des finalités
- au consentement
- la protection des données par défaut et dès la conception
- à la transparence et à l'information
- à l'exercice des droits

Tous vont à l'encontre du principe de loyauté.

