Global Privacy Enforcement Network

Ratissage du GPEN 2024 : « Mécanismes de conception trompeuse »

Rapport

Le 9 juillet 2024

Table des matières

Contexte

Le ratissage de 2024 du Global Privacy Enforcement Network (GPEN) (le « ratissage ») a eu lieu dans la semaine du 29 janvier au 2 février. Il a examiné la fréquence et les types de mécanismes de conception trompeuse (aussi appelées « interfaces truquées ») observés dans les interactions avec les sites Web et les applications mobiles.

De manière générale, les mécanismes de conception trompeuse sont des choix de conception utilisés dans les interfaces de plateforme pour influencer ou manipuler les utilisateurs, ou pour les contraindre à prendre des décisions qui ne sont pas dans leur intérêt primordial[1]. En ce qui concerne la protection de la vie privée, les mécanismes de conception trompeuse peuvent :

1. inciter les utilisateurs à fournir plus de renseignements personnels que nécessaire pour obtenir des produits ou des services;
2. exiger des utilisateurs qu'ils prennent des mesures supplémentaires pour choisir l'option protégeant le mieux la vie privée;
3. entraver les efforts des utilisateurs pour obtenir des renseignements relatifs à la protection de la vie privée.

Les mécanismes de conception trompeuse peuvent être utilisés indépendamment ou en parallèle. Lorsque deux mécanismes de conception trompeuse ou plus sont utilisés ensemble, ils peuvent influencer plus efficacement les décisions des utilisateurs en matière de protection de la vie privée. L'utilisation d'un mécanisme de conception trompeuse peut également faciliter les utilisations en aval des autres mécanismes de conception trompeuse.

Alors que les individus passent un temps considérable à utiliser des sites Web et des applications pour effectuer des activités quotidiennes, les organismes de réglementation se concentrent de plus en plus sur la façon dont ces plateformes sont conçues pour orienter les interactions des personnes de manière à recueillir une plus grande quantité de renseignements personnels. Par exemple, l'Organisation de coopération et de développement économiques (OCDE), l'European Data Protection Board (EDPB), la Federal Trade Commission (FTC) des États-Unis et le Digital Regulation Cooperation Forum (DRCF) du Royaume-Uni ont tous récemment publié des rapports distincts sur les mécanismes de conception trompeuse[2].

---

[1] « Dark Commercial Patterns », Documents de travail de l'OCDE sur l'économie numérique, octobre 2022, nº 336; « Guidelines 3/2022 on Dark patterns in social media platform interfaces: How to recognise and avoid them », version 2.0, adoptée le 14 février 2023.

[2] Ibid.; « Bring Dark Patterns to Light », Federal Trade Commission, Staff Report, septembre 2022; « Harmful Design in Digital Markets: How Online Choice Architecture Practices can Undermine Consumer Choice Choice Choice and Control on Personal Information », document de position conjoint de l'Information Commissioner's Office et de la Competition and Markets Authority, août 2023.

Cette année, 26 autorités d'application des lois sur la protection de la vie privée (les « autorités ») ont participé au ratissage en examinant 1 010 sites Web et applications[3]. En raison de la pertinence des mécanismes de conception trompeuse à la fois du point de vue de la protection de la vie privée que du point de vue de la protection des consommateurs, le GPEN a coordonné pour la première fois son action avec celle de l'International Consumer Protection and Enforcement Network (ICPEN) dans le cadre du ratissage. Les membres de chaque réseau ont examiné les mécanismes de conception trompeuse sous l'angle de leur réglementation respective. Bien que le GPEN et l'ICPEN aient déjà collaboré, notamment à la publication d'un communiqué de presse conjoint concernant le Google Play Store, et à l'organisation d'un atelier conjoint de renforcement des capacités en matière d'application des lois en 2021,[4] le ratissage de cette année représente l'exemple le plus complet à ce jour de coopération réglementaire entre les autorités de protection de la vie privée et les autorités de protection des consommateurs, avec un total de 53 autorités participantes (26 autorités chargées de l'application des lois en matière de protection de la vie privée et 27 autorités de l'ICPEN). Cette coopération croissante entre le GPEN et l'ICPEN tient compte de l'intersection croissante des deux sphères réglementaires dans l'économie numérique.

Méthodologie

L'objectif du ratissage était que les participants (les « ratisseurs ») reproduisent l'expérience des consommateurs en utilisant un site Web ou une application mobile pour évaluer comment ils pouvaient i) faire des choix en matière de protection de la vie privée, ii) obtenir des renseignements sur la protection de la vie privée et iii) se déconnecter d'un compte et le supprimer.

Le Commissariat à la protection de la vie privée du Canada (le « coordonnateur du ratissage » de cette année) a coordonné le ratissage et élaboré, en collaboration avec les autorités participantes, un ensemble d'instructions et de questions connexes pour guider l'action des ratisseurs vis-à-vis de chaque site Web et application mobile. Cette approche visait à aider à repérer les mécanismes de conception trompeuse tout en veillant à ce que les ratisseurs évaluent les sites Web et les applications selon des normes similaires. Les questions portaient sur cinq indicateurs fondés sur la taxonomie des mécanismes de conception trompeuse définie par l'OCDE qui étaient considérés comme étant pertinents tant dans le contexte de la protection de la vie privée que dans celui de la protection des consommateurs. Les indicateurs, qui seront décrits de façon plus exhaustive dans les sections ci-dessous, étaient les suivants :

---

[3] Plus précisément, les autorités participantes ont examiné 899 sites Web et 111 applications. Comme il est possible qu'elles aient examiné indépendamment différentes versions des sites Web ou des applications, le nombre d'applications et de sites Web distincts ratissés pourrait être inférieur à 1 010.

[4] «Google Play Store to require app providers to provide consumers with detailed information regarding data collection and use following growing international pressure», RICPC et GPEN, mai 2021.

1. Langage complexe et déroutant (p. ex. des politiques de protection de la vie privée techniques ou trop longues qui sont difficiles à comprendre);
2. Interférence d'interface (p. ex. des éléments de conception qui peuvent avoir une influence sur la perception et la compréhension des utilisateurs par rapport à leurs options concernant la protection de la vie privée);
3. Harcèlement (p. ex. les utilisateurs sont invités à plusieurs reprises à prendre des mesures précises qui peuvent aller à l'encontre de leurs intérêts en matière de protection de la vie privée);
4. Obstruction (p. ex. l'insertion d'étapes supplémentaires qui ne sont pas nécessaires entre les utilisateurs et leurs objectifs de protection de la vie privée); et
5. Actions forcées (p. ex. forcer les utilisateurs à fournir plus de renseignements personnels qu'il n'est nécessaire pour accéder à un service ou les amener par la ruse à penser qu'il est nécessaire de les fournir).

Les ratisseurs ont été invités à documenter leurs observations et leurs interactions avec les paramètres et les politiques de protection de la vie privée, ainsi que les processus de création, de déconnexion et de suppression de compte de différents sites Web et applications à l'aide du questionnaire fourni [5].

Chaque autorité participante a choisi l'objectif de son ratissage, par exemple l'examen de sites Web ou d'applications dans des industries spécifiques correspondant à ses priorités stratégiques. Par conséquent, les autorités ont rempli les champs du questionnaire qui étaient pertinents aux particularités de leur ratissage.

Voici (Figure 1) une ventilation sectorielle des sites Web et des applications mobiles examinés dans le cadre du ratissage : [6]

[5] Le ratissage étant basé sur les observations et les interactions des ratisseurs relativement aux sites Web et aux applications, il ne tient pas compte des mécanismes de conception trompeuse qui sont intégrées dans l'architecture du système (p. ex. les pratiques algorithmiques qui orientent les utilisateurs, parfois de manière inconsciente, vers des choix indésirables).

[6] Les sites Web et applications faisant partie de la catégorie « Autres » comprennent, entre autres, les sites de fabricants automobiles et les logiciels complémentaires de l'Internet des objets.

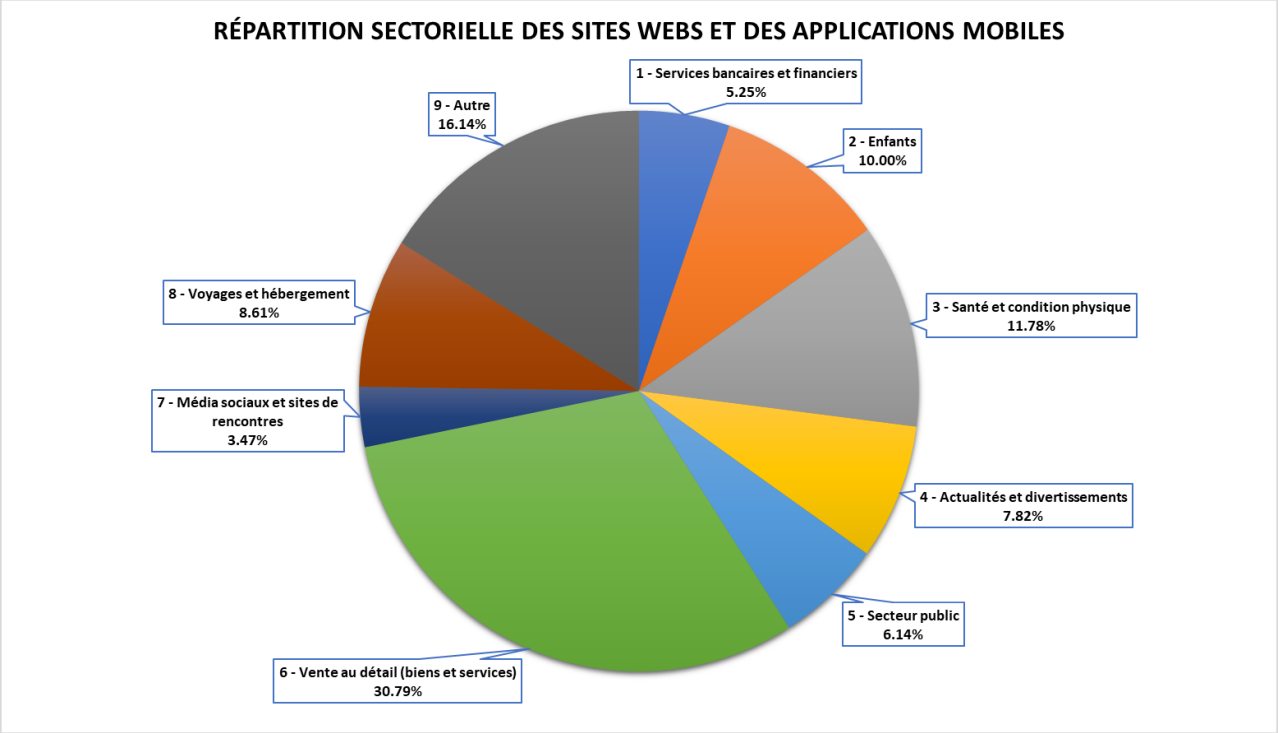

Figure 1

Sommaire des observations

Le ratissage a permis de repérer des mécanismes de conception trompeuse sur la grande majorité des sites Web et des applications examinés. Pour 97 % d'entre eux, et dans des industries multiples, les ratisseurs ont rencontré au moins un mécanisme de conception trompeuse dans leur tentative de prendre des décisions protégeant la vie privée ou d'obtenir des renseignements liés à la protection de la vie privée.

Le mécanisme de conception trompeuse le plus communément observé était l'utilisation d'un langage complexe et déroutant dans les politiques sur la vie privée. Les ratisseurs ont constaté que 89 % des politiques de confidentialité des sites Web et des applications examinés étaient excessivement longues (plus de 3 000 mots) ou contenaient des termes techniques et déroutants, ce qui les rendait difficiles à lire.

Les ratisseurs ont également constaté l'utilisation fréquente des mécanismes de conception trompeuse liés à l'obstruction et à l'interférence d'interface.

En moyenne, les site Web et les applications examinés ont eu recours à une interférence d'interface dans 43 % des interactions[7] (p. ex. des outils linguistiques et visuels) pour inciter les utilisateurs à choisir des options protégeant moins la vie privée. Au total, 41 % des sites Web et des applications ont demandé aux ratisseurs de prendre des décisions en matière de protection de la vie privée lorsqu'ils se sont servis des sites Web ou des applications pour la première fois. Parmi ces cas, 70 % des sites Web et des applications, ce qui représente 31 % de tous ceux qui ont été ratissés, ont fait en sorte que les options protégeant moins la vie privée étaient plus faciles à choisir.

En outre, les ratisseurs ont constaté que les sites Web et les applications avaient recours à l'obstruction dans 39 % des cas afin de créer des obstacles entre les utilisateurs et leurs objectifs, les dissuadant ainsi à faire les choix prévus. Par exemple, dans 16 % des cas, les ratisseurs ne pouvaient pas trouver l'option de déconnexion du compte pour les sites Web et les applications qui offraient l'option de créer un compte. De plus, les ratisseurs ont dû effectuer trois actions ou plus afin de trouver l'option de suppression des comptes dans 27 % des sites Web et des applications examinés et dans 55 % des cas, ils n'ont pas été en mesure de trouver l'option en question. Cela démontre qu'il est souvent plus difficile de supprimer les comptes que de les créer.

En revanche, la plupart des sites Web et des applications ont rendu leurs politiques de protection de la vie privée faciles à trouver (59 % étaient accessibles au moyen d'un seul clic). Toutefois, environ 42 % des politiques consultées étaient plutôt longues et nécessitaient une capacité de lecture au moins du niveau universitaire, et 65 % des politiques de protection de la vie privée ne comportaient pas non plus de menus facilitant la navigation.

Les constatations suggèrent que les plateformes de la plupart des organisations sont conçues pour encourager les utilisateurs à prendre des décisions liées à la protection de la vie privée dans l'intérêt de la plateforme et potentiellement contraires à l'intérêt supérieur des utilisateurs. Les mécanismes de conception trompeuse servent à miner l'autonomie des utilisateurs en matière de protection de la vie privée.

Voici les taux agrégés d'occurrence des mécanismes de conception trompeuse examinés dans le cadre du ratissage :

[7] Dans la suite du présent rapport, le terme « interactions » désigne les tâches précises que les ratisseurs devaient accomplir lors de l'examen des applications et des sites Web (par exemple, prendre une décision concernant les témoins à la demande d'un site Web est une interaction, trouver la politique de confidentialité d'une application en est une autre, etc.).

Indicateur	Probabilité
Indicateur 1 : Langage complexe et déroutant	89 %
Indicateur 2 : Interférence d'interface	43 %
Indicateur 3 : Importunités	14 %
Indicateur 4 : Obstruction	39 %
Indicateur 5 : Action forcée	21 %

Figure 2 – Taux d'occurrence des mécanismes de conception trompeuse

Langage complexe et déroutant (indicateur 1)

Le langage joue un rôle important pour permettre aux utilisateurs de faire des choix éclairés du point de vue de la protection de la vie privée. Si le langage utilisé pour expliquer les pratiques et les paramètres de protection de la vie privée de l'organisation est très technique ou déroutant, les utilisateurs seront moins susceptibles de comprendre comment leurs décisions influent sur la protection de leur vie privée[8]. Dans le même ordre d'idées, si la politique de confidentialité de l'organisation est excessivement longue, les utilisateurs sont moins enclins à la lire et risquent d'accepter des conditions qu'ils ne comprennent pas[9]. Dans chacun de ces cas, les utilisateurs pourraient être amenés à prendre des décisions contraires à leurs préférences réelles en matière de protection de la vie privée.

La formulation complexe et déroutante des politiques de confidentialité des organisations, présente dans 89 % des cas, est le mécanisme de conception trompeuse le plus courant relevé par les ratisseurs dans les sites Web et les applications qu'ils ont examinés.

---

[8] Il est possible que les politiques de protection de la vie privée doivent être rédigées dans un langage précis afin de répondre à certaines exigences légales, ce qui peut contribuer à leur longueur et à leur complexité. Néanmoins, les organisations doivent permettre à leurs utilisateurs d'examiner et de comprendre rapidement les informations clés ayant une incidence sur leurs décisions en matière de protection de la vie privée, par exemple en adoptant une approche par couches permettant aux utilisateurs de contrôler le niveau de détail qu'ils souhaitent obtenir.

[9] European Data Protection Board, «Guidelines 3/2022 on deceptive design patterns in social media platform interfaces: How to recognise and avoid them», alinéa 26.

En outre, les autorités participantes ont indiqué que 55 % des politiques de confidentialité des sites Web et des applications ratissés comptaient plus de 3 000 mots, et que 65 % des d'entre elles ne comprenaient pas de menu ou de table des matières, ce qui rendait plus difficile pour les utilisateurs de trouver des informations précises dans des blocs de texte souvent longs.

Enfin, selon le résultat du test Flesch,[10] 76 % de ces politiques de confidentialité exigeaient une capacité de lecture d'étudiant de premier cycle ou supérieure, et 20 % requéraient une capacité de lecture d'étudiant de cycle supérieur, au minimum.

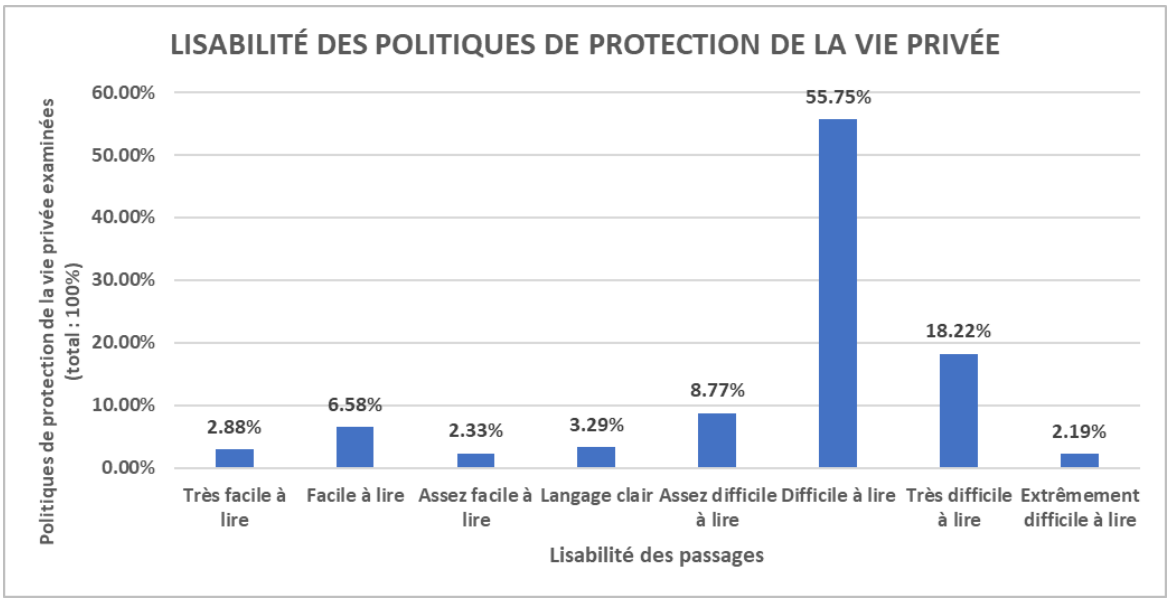

Figure 3

Interférence d'interface (indicateur 2)

La façon dont les utilisateurs réagissent aux options de protection de la vie privée et interagissent avec celles-ci dépend également en grande partie de la façon dont l'information leur est présentée. Les « interférences d'interface » consistent dans l'utilisation d'éléments de conception et de méthodes de présentation qui modifient la perception et la compréhension des options de protection de la vie privée par les utilisateurs. Certains éléments de conception de plateforme subtils peuvent nuire à la capacité de ces derniers de faire des choix qui reflètent leurs préférences réelles en matière de protection de la vie privée.

[10] Le test de lisibilité de Flesch évalue la lisibilité d'un passage en fonction de sa longueur, de la longueur des phrases et du choix des mots. Une note faible correspond à un passage plus difficile nécessitant un niveau d'éducation plus élevé pour être compris. L'outil ne s'applique pas aux langues choisies par toutes les autorités participantes. Sur les 26 autorités participantes, 21 ont utilisé la note du test de lisibilité de Flesch pour évaluer la lisibilité des politiques de protection de la vie privée.

Les mécanismes de conception trompeuse appartenant à la catégorie des interférences d'interface peuvent influencer le processus décisionnel des utilisateurs par divers moyens :

(i) une « fausse hiérarchie » : met l'accent sur certains éléments visuels et en escamote d'autres, dirigeant ainsi les utilisateurs vers des options qui protègent moins la vie privée (voir la « Figure 4 » ci-dessous);

(ii) (ii) une « présélection » : amène à sélectionner par défaut les options les plus intrusives dans la vie privée;

(iii) (iii) une « manipulation émotionnelle » : utilise un langage émotionnel qui amène les utilisateurs à se tourner vers les options privilégiées par les organisations (p. ex. « Acceptez et profitez des offres! » ou « Quoi? Vous ne voulez pas économiser? »; voir aussi la « Figure 5 » ci-dessous).

Le ratissage a révélé qu'en moyenne, les interférences d'interface étaient présentes dans 43 % des interactions.

Fausse hiérarchie

Lorsque les sites Web et les applications offraient des choix en matière de protection de la vie privée aux ratisseurs, 57 % d'entre eux avaient recours à une fausse hiérarchie pour inciter les utilisateurs à sélectionner les choix protégeant moins la vie privée. Consultez la Figure 4 pour un exemple représentatif de cas où le site Web affichait d'abord les choix protégeant le moins la vie privée et les rendant plus visibles que les autres choix en accentuant le contraste des couleurs.

Figure 4 - Exemple de fausse hiérarchie

En encourageant les utilisateurs à créer un compte et, en particulier, à utiliser des comptes de tiers comme des médias sociaux ou des plateformes de courriel pour s'inscrire à ces comptes, les sites Web et les applications sont parfois en mesure d'effectuer un meilleur suivi ou de recueillir plus d'information sur leurs utilisateurs. Une proportion de 54 % des sites Web et des applications consultés faisaient en sorte que l'option du recours aux services de tiers (p. ex. les réseaux sociaux) pour s'inscrire à un compte soit davantage mise en valeur que l'option d'utiliser simplement une adresse courriel.

Présélection

Les ratisseurs ont constaté que 48 % des sites Web et des applications présélectionnaient les options protégeant moins la vie privée lorsqu'ils demandaient aux utilisateurs de faire des choix en matière de protection de la vie privée. Il se peut que la présélection des options les plus intrusives dans la vie privée ne reflète pas les préférences des utilisateurs, car bon nombre d'entre eux ne sont pas au courant qu'ils peuvent modifier les paramètres ou qu'ils ont le temps d'apporter ces changements.

Manipulation émotionnelle

Les ratisseurs ont déterminé que parmi le 34 % des applications qui leur ont demandé de confirmer les paramètres de protection de la vie privée lorsqu'ils les ont utilisées pour la première fois, 42 % d'entre elles (soit 14 % de toutes les applications examinées) ont affiché un langage de manipulation émotionnelle.

Enfin, 29 % des sites Web et des applications tentaient de dissuader les utilisateurs de supprimer pas leur compte au moyen d'un langage manipulateur. L'image ci-dessous en est un exemple :

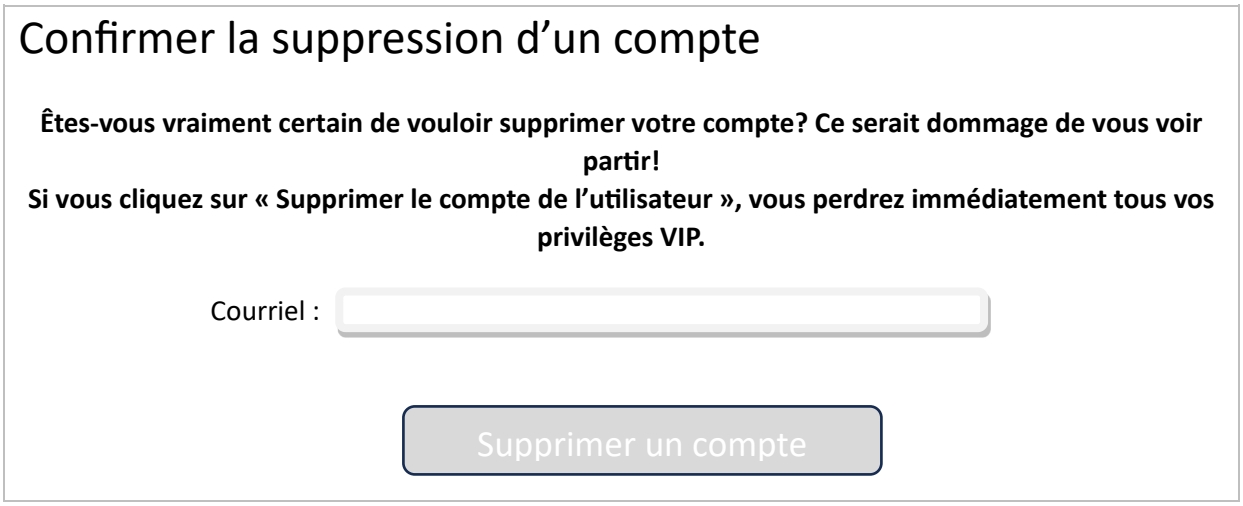

Figure 5 - Exemple d'exploitation du sentiment de culpabilité

Il est raisonnable de demander aux utilisateurs de confirmer qu'ils souhaitent supprimer leur compte, mais l'utilisation d'un langage à connotation émotionnelle pourrait influencer les utilisateurs de manière à ce qu'ils prennent une décision qui n'est pas dans leur meilleur intérêt.

Harcèlement (indicateur 3)

Le harcèlement est une tactique par laquelle les sites Web et les applications invitent, à plusieurs reprises, les utilisateurs à effectuer une action précise (p. ex. modifier leurs paramètres de protection de la vie privée ou se connecter à leur compte) dans le sens des objectifs de l'organisation, ce qui peut aller à l'encontre de l'intérêt supérieur des utilisateurs en matière de protection de la vie privée. Les demandes répétées interrompent l'expérience des utilisateurs et peuvent les encourager à céder aux demandes pour éviter le désagrément d'autres invites.

Le ratissage ayant été conçu pour ne nécessiter qu'une brève interaction avec le site Web ou l'application en question, il n'était pas propice au dépistage du harcèlement possible au fil du temps. Les ratisseurs ont toutefois constaté que 35 % des sites Web et des applications dotés d'une option de création de comptes se livraient à du harcèlement en invitant plus d'une fois les utilisateurs à reconsidérer leur intention de supprimer leur compte.

Obstruction (indicateur 4)

L'obstruction fonctionne en insérant des étapes supplémentaires entre les utilisateurs et leurs objectifs, en dissuadant les utilisateurs de faire les choix prévus ou en rendant les utilisateurs moins motivés à le faire. L'obstruction peut être très efficace parce qu'elle exploite le peu de temps, d'attention et/ou de volonté des utilisateurs pour naviguer sur les sites Web et dans les applications.

Les ratisseurs ont examiné la manière dont les sites Web et applications utilisaient l'obstruction auprès des utilisateurs en créant une « lassitude de clic » en obligeant les utilisateurs à faire de nombreux clics pour se renseigner sur la protection de la vie privée ou faire des choix de protection de la vie privée. Les ratisseurs ont aussi examiné comment les sites Web et applications rendent difficile l'annulation ou la suppression d'un compte par les utilisateurs.

En moyenne, les ratisseurs ont constaté de l'obstruction dans 39 % des interactions avec des sites Web et des applications. Le taux d'occurrence le plus élevé s'est manifesté pendant le processus de suppression de compte, où 55 % des ratisseurs n'ont pas été en mesure de trouver l'option pour supprimer le compte. Même dans le cas des sites Web et applications sur lesquels les ratisseurs pouvaient trouver l'option de suppression de compte (45 %), dans 27 % des cas (ou 10 % des sites Web et applications consultés), les utilisateurs étaient obligés de prendre des mesures peu commodes, par exemple soumettre un long formulaire ou envoyer une demande écrite à l'organisation pour demander la suppression de leur compte.

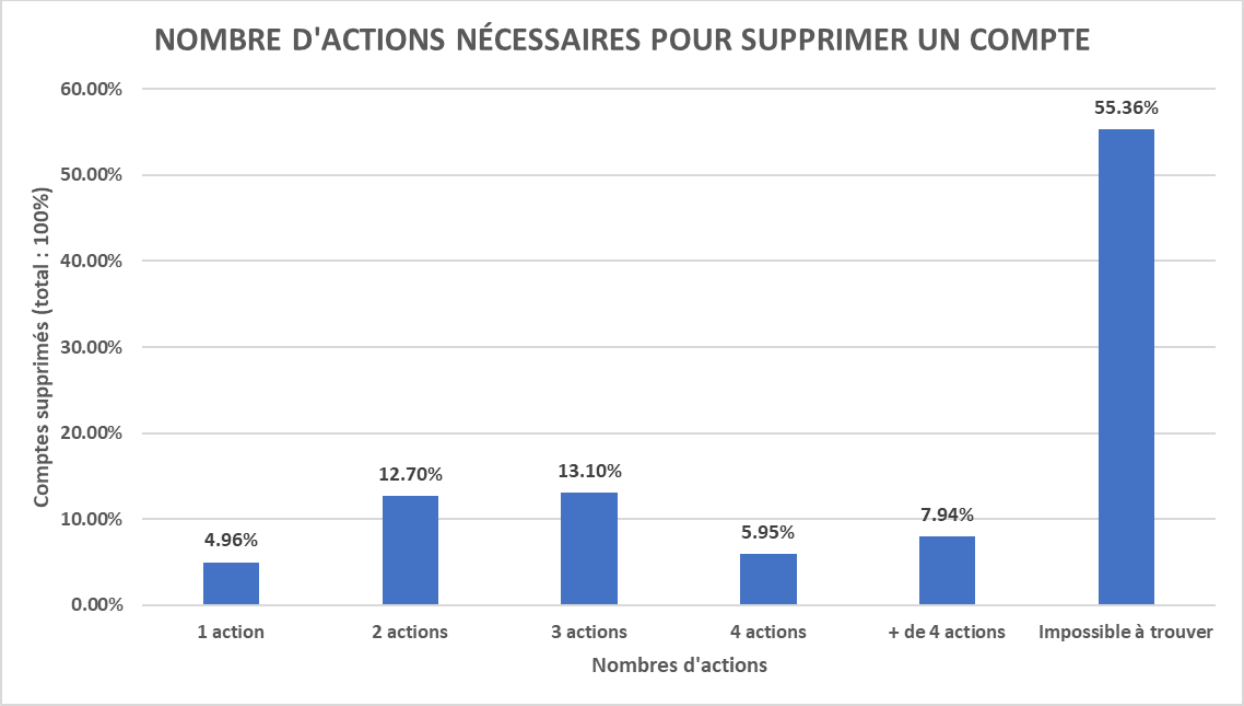

Figure 6

Les ratisseurs ont également fait face à des mesures d'obstruction lorsqu'ils cherchaient à modifier les paramètres de protection de la vie privée. Parmi la minorité de sites Web et d'applications qui permettaient aux utilisateurs d'ajuster leurs paramètres de protection de la vie privée (p. ex. les paramètres des témoins) lorsqu'ils ouvraient l'application ou naviguaient vers la page d'accueil du site Web, 46 % des sites et des applications forçaient les utilisateurs à faire des clics supplémentaires pour refuser l'option protégeant moins la vie privée, qui était celle par défaut.

De plus, il existe un contraste important entre les sites Web et les applications en ce qui concerne le nombre de clics requis pour localiser la ou les pages contenant la politique de protection de la vie privée. Alors que 76 % des ratisseurs ont pu trouver la politique de protection de la vie privée en deux clics ou moins sur les sites Web, 44 % d'entre eux ont pu faire de même dans le cas des applications.

Un total de 77 % des utilisateurs ont pu se déconnecter de leur compte en deux clics ou moins sur l'application ou le site Web, mais 16 % d'entre eux n'ont jamais réussi à trouver comment se déconnecter du compte. Cette situation est préoccupante, car les sites Web et les applications peuvent, dans de nombreux cas, continuer à suivre les utilisateurs tant qu'ils restent connectés.

Actions forcées (indicateur 5)

Les personnes peuvent être invitées à fournir leurs renseignements personnels pour recevoir certains services en ligne. Un principe clé de la protection de la vie privée et des données est que la collecte et l'utilisation des renseignements personnels doivent se limiter à l'information nécessaire.

Les mécanismes de conception trompeuse à action forcée obligent les utilisateurs à fournir leurs renseignements personnels pour accéder aux services ou les amènent par la ruse à penser qu'il est nécessaire de fournir ces renseignements, alors qu'en réalité, ces informations ne sont pas nécessaires à la prestation du service.

Le ratissage a permis d'examiner comment les sites Web et les applications utilisaient des mécanismes de conception trompeuse à action forcée, comme demander aux utilisateurs de divulguer plus de renseignements que nécessaire (c.-à-d. « divulgation forcée »). Ce mécanisme de conception trompeuse était utilisé pour 26 % des sites Web et des applications ratissés qui incitaient les utilisateurs à faire un choix en matière de protection de la vie privée à l'ouverture de la plateforme. La Figure 7 ci-dessous présente un exemple d'un cas où les utilisateurs n'avaient d'autre option que d'accepter les témoins pour pouvoir effectuer une recherche sur le site Web de l'organisation.

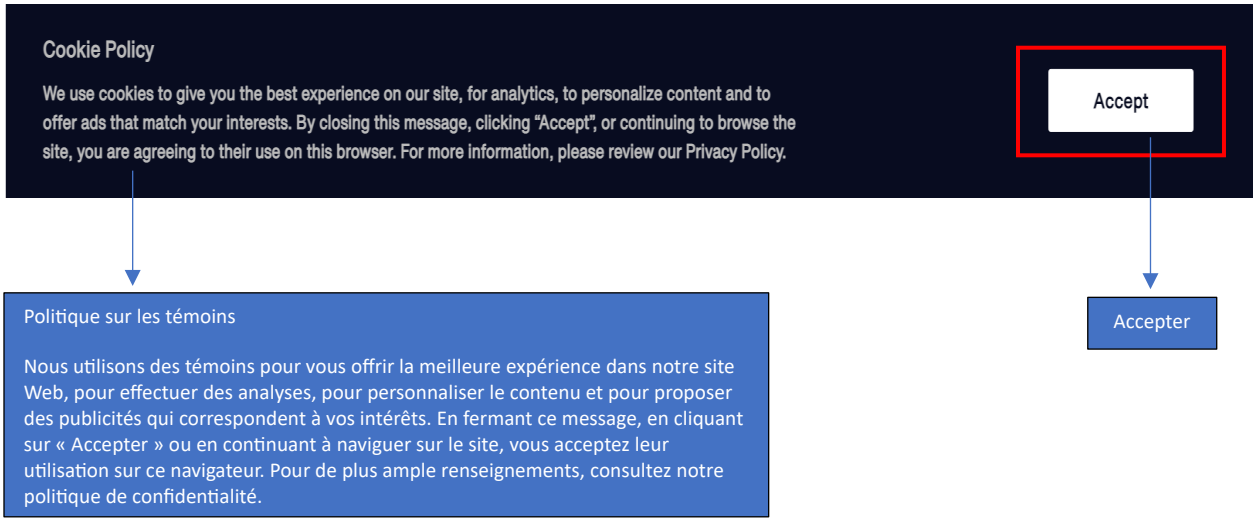

Figure 7 – Exemple de divulgation force

Un total de 9 % des sites Web et des applications ont forcé les utilisateurs à divulguer plus de renseignements personnels qu'ils n'avaient été tenus de le faire pour supprimer le compte. Dans certains cas, les sites Web et les applications rendaient obligatoires des champs de données supplémentaires (p. ex. l'adresse du domicile ou le nom complet) pour supprimer le compte, alors que ces renseignements n'étaient pas requis lors de la création du compte.

Conclusion

Le ratissage du GPEN vise à encourager les organisations à se conformer à la législation sur la protection de la vie privée et des données ainsi qu'à promouvoir la coopération entre les autorités d'application des lois sur la protection de la vie privée dans le monde entier. Bien que le ratissage ne constitue pas en soi une enquête et qu'il n'ait pas pour but d'identifier de manière concluante les problèmes de conformité ou les infractions légales, les préoccupations soulevées par cet exercice peuvent contribuer à soutenir des actions ciblées d'éducation, de sensibilisation des organisations et d'application de la loi à l'avenir.

Les résultats du ratissage de cette année suggèrent une très forte occurrence des mécanismes de conception trompeuse par les sites Web et les applications à l'échelle mondiale : il est donc probable que les utilisateurs soient confrontés, dans la majorité des cas, à au moins un mécanisme de conception trompeuse lors de leurs interactions avec les sites Web et les applications.

Les observations des ratisseurs indiquent que de nombreux sites Web et applications ont été conçus pour encourager les utilisateurs à prendre des décisions en matière de protection de la vie privée qui pourraient ne pas être dans leur intérêt supérieur. Le ratissage montre plusieurs domaines dans lesquels les organisations pourraient améliorer la conception de leurs plateformes pour permettre aux utilisateurs de mieux comprendre et de contrôler l'utilisation et la divulgation de leurs données personnelles.

Les organisations doivent concevoir leurs plateformes, de même que les communications et choix connexes en matière de protection de la vie privée, de manière à permettre aux utilisateurs de prendre des décisions éclairées à cet égard. De bons mécanismes de conception peuvent consister à utiliser par défaut les paramètres protégeant le plus la vie privée, à mettre l'accent sur les options de protection de la vie privée, à utiliser un langage et des conceptions neutres pour présenter les choix de protection de la vie privée, à réduire le volume de clics requis pour naviguer, à ajuster les choix de protection de la vie privée d'un utilisateur et à fournir des options de consentement « juste-à-temps » permettant aux utilisateurs de prendre les décisions en matière de protection de la vie privée au moment où elles sont pertinentes. En mettant en œuvre des mécanismes de conception favorisant la protection de la vie privée, les organisations offriront aux utilisateurs de leurs sites Web et applications des expériences exemptes d'influence, de manipulation et de coercition, et gagneront ainsi leur confiance.

Remerciements

Au nom du GPEN, le coordonnateur du ratissage remercie la Dre Cristiana Teixeira Santos, professeure adjointe en droit et technologie à la Utrecht University, pour ses conseils dans l'élaboration de la méthodologie de ratissage[11].

[10] Consultez la biographique de la Dre Cristiana Teixeira Santos ici.

Annexe A

Au total, 26 autorités de cinq continents ont participé au ratissage.

Les autorités ont présenté leurs résultats :

1. Argentine – Accès à l'information publique (Agence)
2. Australie – Office of the Australian Information Commissioner (OAIC)
3. Baden-Wuerttemberg – Commissaire à la protection des données et à l'accès à l'information
4. Bermudes – Commissariat à la protection de la vie privée
5. Brésil – Autorité nationale de protection des données (Autoridade Nacional de Proteção de Dados)
6. Canada – Commissariat à l'information et à la protection de la vie privée de l'Alberta
7. Canada – Commissariat à l'information et à la protection de la vie privée de la Colombie-Britannique
8. Commissariat à la protection de la vie privée du Canada
9. Canada – Commission d'accès à l'information du Québec
10. Chine – Commissariat à la protection des données personnelles de Hong Kong
11. Macao, Chine – Bureau de la protection des données personnelles
12. Dubaï – Commissaire à la protection des données, Dubai International Financial Centre
13. France – Commission nationale de l'informatique et des libertés
14. Gibraltar – Gibraltar Regulatory Authority (GRA)
15. Guernesey – Office of the Data Protection Authority, Guernsey
16. Italie – Garante per la protezione dei dati personali
17. Japon - Commission de la protection des renseignements personnels
18. Commissariat à l'information de Jersey
19. Malte – Office of the Information and Data Protection Commissioner

20. Mexique – Instituto De Transparencia, Acceso A La Información Pública Y Protección De Datos Personales Del Estado De México Y Municipios

21. Philippines – National Privacy Commission (NPC)

22. République de Colombie – Superintendence of Industry and Commerce

23. Singapour – Personal Data Protection Commission

24. Royaume-Uni – Commissariat à l'information

25. États-Unis – California Privacy Protection Agency

26. États-Unis – Federal Trade Commission