



# **Index de responsabilité des entreprises 2019**

## **Indicateurs de recherche**

Guide des indicateurs et glossaire inclus

**Septembre 2018**

Ce document est protégé par une licence Creative Commons Attribution 4.0 International.  
Pour consulter la licence : <https://creativecommons.org/licenses/by/4.0/>.



## Remerciements

Les membres suivants de l'équipe de Ranking Digital Rights ont travaillé à la préparation et à l'élaboration de la méthodologie de l'Index de responsabilité des entreprises.

- Rebecca MacKinnon, directrice de projet.
- Amy Brouillette, directrice principale de recherche et de la rédaction
- Laura Reed, analyste principale de recherche et coordonnatrice
- Andrea Hackl, analyste de recherche
- Nathalie Maréchal, chargée de recherche principale
- Lisa Gutermuth, responsable du programme

Vous pouvez consulter la liste complète des membres de l'équipe à l'adresse :  
<https://rankingdigitalrights.org/who/>

Nous tenons à remercier toutes les parties prenantes pour leurs retours indispensables sur les révisions proposées pour la méthodologie de l'Index 2019.

## À propos de Ranking Digital Rights

Ranking Digital Rights (RDR) est un projet de recherche à but non lucratif hébergé par l'Open Technology Institute de New America qui travaille avec un réseau international de partenaires à la mise en place de normes internationales pour les entreprises du secteur des technologies de l'information et de la communication.

Pour en savoir plus sur RDR et son Index de responsabilité des entreprises, consultez le site  
[www.rankingdigitalrights.org](http://www.rankingdigitalrights.org).

Pour découvrir New America, vous pouvez consulter <https://www.newamerica.org/>.

Pour plus d'informations sur l'Open Technology Institute, référez-vous au site  
<https://www.newamerica.org/oti/>.

Pour consulter la liste complète des financeurs et des partenaires du projet, référez-vous au site :  
<https://rankingdigitalrights.org/who/partners/>.

# Table des matières

<b>Remerciements</b>	2
<b>À propos de Ranking Digital Rights</b>	2
<b>À propos de l'Index de responsabilité des entreprises</b>	5
Méthodologie de l'Index	5
Révisions de l'Index 2019	6
Les entreprises	6
Processus de recherche	9
Évaluations et résultats	10
<b>Méthodologie de l'Index 2019</b>	11
<b>Gouvernance</b>	12
G1. Engagement politique	12
G2. Gouvernance et surveillance de la direction	12
G3. Mise en œuvre interne	13
G4. Analyse d'impact	14
G5. Implication des parties prenantes	16
G6. Voies de recours	17
<b>Liberté d'expression</b>	19
F1. Accès aux conditions d'utilisation	19
F2. Modifications des conditions d'utilisation	20
F3. Processus d'application des conditions générales	20
F4. Données sur l'application des conditions d'utilisation	22
F5. Réponse aux demandes de tiers de restreindre l'accès à des contenus ou des comptes	22
F6. Données sur les demandes gouvernementales de restriction d'accès à des contenus ou des comptes	24
F7. Données sur les demandes privées de restriction d'accès à des contenus ou des comptes	25
F8. Information aux utilisateurs sur la restriction d'accès à des contenus et des comptes	26
F9. Gestion du réseau (entreprises de télécommunications)	27
F10. Coupure de réseau (entreprises de télécommunications)	28
F11. Politique relative à l'identité	29
<b>Vie privée</b>	30
P1. Accès aux politiques de confidentialité	30
P2. Modifications apportées à la politique de confidentialité	31

P3. Collecte des données utilisateurs.....	32
P4. Partage des données utilisateurs .....	34
P5. Objectif de la collecte et du partage des données utilisateurs .....	35
P6. Conservation des données utilisateurs .....	35
P7. Contrôle des utilisateurs sur leurs propres informations .....	36
P8. Accès des utilisateurs à leurs propres données.....	38
P9. Collecte de données utilisateurs par des tiers.....	39
P10. Procédure de réponse à des demandes d'information sur les utilisateurs émanant de tiers	39
P11. Données relatives aux demandes de données utilisateurs émanant de tiers .....	41
P12. Notification des utilisateurs à propos des demandes de données provenant de tiers .....	42
P13. Contrôle de la sécurité .....	43
P14. Mesures relatives aux failles de sécurité.....	43
P15. Atteintes à la protection des données .....	44
P16. Chiffrement des communications des utilisateur et du contenu privé .....	45
P17. Sécurité des comptes.....	46
P18. Information et formation des utilisateurs sur les risques potentiels.....	47
<b>Glossaire .....</b>	<b>48</b>

## À propos de l'Index de responsabilité des entreprises

L'Index de responsabilité des entreprises de Ranking Digital Rights (RDR) classe les entreprises du secteur des technologies de l'information et de la communication (internet, mobile et télécommunications) les plus puissantes au monde en fonction de leurs politiques et de leurs pratiques connues qui affectent la liberté d'expression et la vie privée. L'index constitue un outil normatif qui vise à encourager les entreprises à respecter les principes et les normes internationales établies pour protéger la liberté d'expression et la vie privée.

Les critères utilisés par l'Index pour évaluer les entreprises s'appuient sur le travail réalisé sur plus d'une décennie par des groupes de défense des droits de l'homme, de la protection de la vie privée et de la sécurité. Ils incluent les [Principes directeurs relatifs aux entreprises et aux droits de l'homme](#) des Nations Unies, qui affirment qu'à l'instar des gouvernements qui doivent protéger les droits de l'homme, les entreprises ont aussi la responsabilité de les respecter. L'Index s'appuie également sur les principes de la [Global Network Initiative](#) et sur les [directives de mise en œuvre](#) formulées par cet organisme qui traitent des responsabilités spécifiques des entreprises du secteur des TIC en matière de liberté d'expression et de protection de la vie privée face aux demandes des gouvernements de restreindre l'accès à des contenus ou d'obtenir les informations des utilisateurs. Il s'appuie en outre sur un ensemble de règles et de normes mondiales émergentes en matière de protection des données, de sécurité et d'accès à l'information. Les données et les analyses produites par l'Index éclairent le travail des défenseurs des droits humains, des décideurs et des investisseurs responsables. Elles sont utilisées par les entreprises pour améliorer leurs politiques et leurs pratiques.

### Méthodologie de l'Index

L'Index de responsabilité des entreprises publié par RDR a été élaboré au terme de trois années d'études, de mise à l'essai, de consultations et de révisions. Depuis sa création, le projet collabore étroitement avec des chercheurs du monde entier. Pour l'élaboration de la méthodologie, l'étude pilote et l'Index inaugural, nous avons également travaillé avec Sustainalytics, l'un des fournisseurs de pointe en matière de recherche dans le domaine de la performance ESG (pratiques environnementales, sociales ou de gouvernance) pour les investisseurs.

En 2015, RDR lançait son premier Index qui portait sur le [classement](#) de 16 entreprises de l'Internet et des télécommunications.

Pour l'Index 2017, RDR a étendu l'étude à 22 entreprises : l'ensemble de celles évaluées en 2015 et six supplémentaires. En plus des entreprises de l'Internet et des télécommunications, l'Index s'étoffe avec de nouveaux types de services et inclut des entreprises qui développent des logiciels et des appareils que nous appelons « [écosystèmes mobiles](#) ». Par conséquent,

l'équipe du RDR a [revu la méthodologie 2017](#) sur la base d'un examen détaillé des données brutes de l'Index 2015 ainsi que de consultations avec des acteurs de la société civile, des milieux universitaires, des investisseurs et les entreprises elles-mêmes.

L'Index 2018 applique la même méthodologie pour évaluer les 22 mêmes entreprises que l'Index 2017. Cela nous a permis de produire des analyses comparatives de la performance de chaque entreprise et de découvrir les tendances générales.

## Révisions de l'Index 2019

L'Index de responsabilité des entreprises 2018 publié par Ranking Digital Rights a été conçu comme un classement annuel et, à ce titre, le RDR continue de développer la méthodologie de l'index en réponse à l'évolution rapide que connaît le secteur technologique.

La méthodologie de l'Index 2019 a ainsi été élargie pour tenir compte des informations, révélées par les entreprises relatives à leur utilisation d'outils décisionnels automatisés et à leurs politiques et pratiques en matière de publicité ciblée. La méthodologie a également été mise à jour afin d'améliorer l'évaluation des procédures de résolution des réclamations et des recours établies par les entreprises.

Les révisions se limitent à deux indicateurs (G4, G6) afin de préserver la comparabilité d'une année à l'autre. Plus précisément, deux éléments (5 et 6) ont été ajoutés à l'indicateur G4, qui évalue si les entreprises effectuent des études d'impact sur les droits de l'homme (EIDH) pour leurs produits et services. Ces nouveaux éléments permettent d'évaluer si les entreprises effectuent des études sur les risques associés à leur utilisation d'outils automatisés de prise de décision (tels que des algorithmes ou une intelligence artificielle) et à leurs politiques et pratiques en matière de publicité ciblée.

Les révisions apportées à l'indicateur G6 visent à renforcer et clarifier l'évaluation des mécanismes et des procédures de traitement des réclamations et des recours ainsi qu'à mieux aligner les critères du G6 sur ceux énoncés dans les [Principes directeurs relatifs aux entreprises et aux droits de l'homme des Nations Unies](#).

En juillet 2018, RDR a amorcé une période de [consultation publique](#) pour solliciter l'avis des parties prenantes sur ces révisions. Les derniers changements apportés au G4 et au G6, présentés dans le présent document, résultent ainsi de ces avis et des recherches internes menées par RDR.

Nous encourageons les parties prenantes à se renseigner sur l'élaboration de notre méthodologie :

<https://rankingdigitalrights.org/methodology-development/>

## Les entreprises

L'Index de responsabilité des entreprises 2019 évalue 24 entreprises citées ci-dessous. Pour ce projet, les chercheurs examineront les politiques et pratiques générales de la société mère ainsi que celles communiquées par certains services ou sociétés d'exploitation locales (selon la structure de la société).

**Entreprises de télécommunications** : L'index 2019 classe 12 entreprises de télécommunications, dont deux **nouvelles** qui entrent dans le classement cette année (**surlignées en bleu**). Pour chacune de ces sociétés, nous évaluons les politiques globales au niveau du groupe pour les indicateurs pertinents, les services mobiles prépayés et postpayés de la filiale d'exploitation du pays d'origine ainsi que le service de ligne fixe haut débit là où il est proposé :

- América Móvil (Mexique) : services mobiles prépayés et postpayés (Telcel)
- AT&T (États-Unis) : services mobiles prépayés et postpayés, ligne fixe haut débit
- Axiata (Malaisie) : services mobiles prépayés et postpayés (Celcom)
- Bharti Airtel (Inde) : services mobiles prépayés et postpayés, ligne fixe haut débit
- **Deutsche Telekom (Allemagne) : services mobiles prépayés et postpayés, ligne fixe haut débit**
- Etisalat (Émirats arabes unis) : services mobiles prépayés et postpayés, ligne fixe haut débit
- MTN (Afrique du Sud) : services mobiles prépayés et postpayés
- Ooredoo (Qatar) : services mobiles prépayés et postpayés, ligne fixe haut débit
- Orange (France) : services mobiles prépayés et postpayés, ligne fixe haut débit
- Telefónica (Espagne) : services mobiles prépayés et postpayés, (Movistar), ligne fixe haut débit
- **Telenor (Norvège) : services mobiles prépayés et postpayés, ligne fixe haut débit**
- Vodafone (Royaume-Uni) : services mobiles prépayés et postpayés, ligne fixe haut débit

**Entreprises de l'écosystème internet et mobile** : L'index 2019 classe 12 entreprises de l'écosystème des télécommunications et de l'Internet. Pour l'Index 2019, nous avons étendu notre évaluation des services cloud à cinq entreprises : Google, Mail.Ru, Microsoft, Samsung et Tencent (**surlignées en bleu**). De plus, Flickr disparaît de l'index 2019 puisque ce service n'appartient plus à Oath.<sup>1</sup>

Pour chaque entreprise, nous examinons jusqu'à cinq services, comme suit :

---

1

□ L'entreprise SmugMug a acquis Flickr en avril 2018.

- Apple (États-Unis) : écosystème mobile iOS, iMessage, iCloud
- Baidu (Chine) : Baidu Search, Baidu Cloud, Baidu PostBar
- Facebook (États-Unis) : Facebook, Instagram, WhatsApp, Messenger
- Google (États-Unis) : Search, Gmail, Youtube, écosystème mobile Android, [Google Drive](#)
- Kakao (Corée du Sud) : Kakao Search, Kakao Mail, KakaoTalk
- Mail.Ru (Russie) : V Kontakte, messagerie Mail.ru, Mail.ru Agent messaging, [Mail.Ru Cloud](#)
- Microsoft (États-Unis) : Bing, Outlook.com, Skype, [OneDrive](#)
- Oath (États-Unis) : Yahoo Mail, Tumblr
- Samsung (Corée du Sud) : implémentation d'Android par Samsung, [Samsung Cloud](#)
- Tencent (Chine) : QZone, QQ, WeChat, [Tencent Cloud](#)
- Twitter (États-Unis) : Twitter, Periscope
- Yandex (Russie) : Yandex Mail, Yandex Search, Yandex Disk (stockage sur le cloud)



## Processus de recherche

Le processus de recherche et d'évaluation de l'Index de responsabilité des entreprises 2019 sera mené par un réseau mondial de chercheurs ainsi que par l'équipe de recherche de RDR. Il comprend les étapes suivantes :

- **Étape 1 : Collecte des données.** L'équipe de recherche primaire recueille des données pour chaque entreprise et fournit une évaluation préliminaire de sa performance pour tous les indicateurs.
- **Étape 2 : Examen secondaire.** Une deuxième équipe de chercheurs effectue une vérification des évaluations fournies par les chercheurs lors de l'étape 1.
- **Étape 3 : Examen et réconciliation.** L'équipe de RDR examine les résultats des étapes 1 et 2. Elle résout toute divergence.
- **Étape 4 : Premier examen horizontal.** L'équipe de RDR recoupe les indicateurs pour s'assurer qu'ils ont été évalués de façon homogène pour chaque entreprise.
- **Étape 5 : Retours de l'entreprise.** Les résultats préliminaires sont envoyés aux entreprises qui peuvent les commenter.
- **Étape 6 : Examen horizontal secondaire.** L'équipe de RDR conduit une deuxième analyse horizontale à partir des retours des entreprises recueillis à l'étape 5 et procède à une contre-vérification de ces indicateurs pour assurer cohérence et contrôle qualité.
- **Étape 7 : Score final.** L'équipe de RDR calcule les scores finaux.

Les entreprises reçoivent un score cumulatif de leur performance pour chaque catégorie de l'Index. Les résultats montrent également la performance des entreprises dans chaque catégorie et pour chaque indicateur. En outre, les conclusions présentent une comparaison des tendances d'une année à l'autre.

L'index 2019 sera publié en mai 2019 sur un site Internet interactif et sous la forme d'un rapport PDF téléchargeable. Les scores des entreprises seront accompagnés d'une analyse des conclusions principales et des tendances.

De plus, une fiche sera établie pour chaque entreprise. Elle présentera les performances de la société et des renseignements importants qui apportent du contexte et nuancent les résultats. Ces informations peuvent inclure des exemples spécifiques de pratiques de l'entreprise, de

contexte juridique et réglementaire, ou toutes autres observations faites par les chercheurs sur des questions qui ne relèvent pas des paramètres de recherche étudiés par les indicateurs.

**Remarque sur les contextes nationaux** qui affectent la performance des entreprises : Dans la plupart des pays, certaines lois, réglementations ou certains facteurs politiques améliorent ou limitent la capacité d'une entreprise à obtenir de bons résultats pour certains indicateurs. Notre méthodologie ne tient pas compte de ces facteurs. En d'autres termes, l'Index évalue les entreprises selon leurs politiques et pratiques, quelle qu'en soit la raison. Toutefois, les textes consacrés à chaque entreprise comprennent une analyse de l'environnement juridique, réglementaire et politique lié à la juridiction compétente qui pourraient avoir une incidence sur son score. En effet, dans certains cas, le score fort ou faible d'une entreprise pour un indicateur donné s'explique par l'environnement juridique, réglementaire ou politique du pays d'origine de celle-ci. Lorsque les lois et réglementations causent une mauvaise performance des entreprises, nous encourageons ces dernières à plaider en faveur des modifications législatives nécessaires au respect de la liberté d'expression et de la vie privée des utilisateurs par des engagements, des politiques et des pratiques fermes.

## Évaluations et résultats

L'index 2019 évalue les politiques de l'entreprise en vigueur entre le 14 janvier 2018 et le 25 janvier 2019. Les entreprises reçoivent un score cumulé de leur performance pour l'ensemble des catégories de l'index. Les résultats présentent la performance des entreprises pour chaque catégorie et indicateur. Chaque indicateur comporte une liste d'éléments et les entreprises se voient attribuer une appréciation (totale, partielle ou nulle) pour chaque critère rempli. L'évaluation comprend une estimation de l'information disponible pour chaque élément des différents indicateurs, s'appuyant sur l'une des réponses possibles suivantes :

- « Oui » / transparence totale : Les informations communiquées par l'entreprise répondent aux exigences de l'élément.
- « Partielle » : Les informations communiquées par l'entreprise répondent à certains aspects de l'élément seulement ou ne sont pas suffisamment complètes pour répondre à la totalité des exigences de l'élément.
- « Pas d'information trouvée » : Les chercheurs n'ont pas été en mesure de trouver sur le site web de l'entreprise d'informations pour répondre à la question posée par l'élément.
- « Non » : Les informations existent, mais ne répondent pas spécifiquement à la question posée par l'élément. Cette option est distincte de l'option « pas d'information trouvée », mais les deux n'offrent aucun point.
- « s.o. ». Sans objet. Cet élément ne s'applique pas à l'entreprise ou au service. Les éléments marqués « s.o. » ne sont pas comptés pour ou contre une entreprise dans le processus de notation.

## Points

- Oui/transparence totale = 100
- Partielle = 50
- Non = 0
- Aucune information trouvée = 0
- s.o est exclu des scores et des moyennes

## Méthodologie de l'Index 2019

L'Index 2018 classait 24 entreprises selon 35 indicateurs répartis en trois catégories qui mesurent la disponibilité des informations relatives aux politiques et pratiques affectant la liberté d'expression et la vie privée des utilisateurs.

Chaque catégorie contient des **indicateurs** qui mesurent la performance de l'entreprise pour cette catégorie. Chaque indicateur est lui-même composé d'**éléments** mesurant la performance de l'entreprise pour cet indicateur.

*Catégories de l'Index :*

- **Gouvernance (G)**

Cette catégorie comprend six indicateurs qui étudient la publication par les entreprises de leurs engagements à l'égard de la liberté d'expression et des principes de protection de la vie privée, ainsi que les mesures prises pour mettre en œuvre ces engagements dans l'ensemble de leurs activités à l'échelle mondiale.

- **Liberté d'expression (F)**

Cette catégorie comprend 11 indicateurs qui mesurent la publication par les entreprises de leurs politiques et pratiques affectant la liberté d'expression des utilisateurs.

- **Vie privée (P)**

Cette catégorie comprend 18 indicateurs qui mesurent la publication par les entreprises de leurs politiques et pratiques affectant la vie privée des utilisateurs.

Chaque catégorie et indicateur est présenté ci-dessous. Pour les indicateurs, une brève section « **Détails de l'indicateur** » décrit ce qu'ils évaluent.

L'annexe comprend un **glossaire** où figurent les termes affichés en **caractères gras** dans les descriptions des indicateurs.



## Gouvernance

Les indicateurs de cette catégorie visent à étudier si les entreprises ont mis en place des processus de gouvernance qui garantissent le respect du droit à la liberté d'expression et à la vie privée des utilisateurs. Reconnus par la [Déclaration universelle des droits de l'homme](#) et consacrés dans le [Pacte international relatif aux droits civils et politiques](#), ces droits s'appliquent aussi bien en ligne que hors ligne. Pour qu'une entreprise obtienne de bons résultats dans cette catégorie, les informations qu'elle communique doivent au moins respecter et, idéalement, dépasser les [Principes directeurs relatifs aux entreprises et aux droits de l'homme des Nations Unies](#) et d'autres normes en matière de droits de l'homme propres au secteur et axées sur la liberté d'expression et la protection de la vie privée, telles que celles établies par la [Global Network Initiative](#).

### G1. Engagement politique

L'entreprise doit s'engager publiquement à respecter les droits des utilisateurs en matière de liberté d'expression et de vie privée.

1. L'entreprise prend-elle un **engagement politique explicite** et clairement articulé à l'égard des droits de l'homme, y compris de la liberté d'expression et de la protection de la vie privée ?

**Détails de l'indicateur :** Cet indicateur cherche à déterminer si l'entreprise a pris des engagements politiques explicites en faveur de la liberté d'expression et du respect de la vie privée. Ces critères sont décrits dans le principe opérationnel 16 des [Principes directeurs relatifs aux entreprises et aux droits de l'homme des Nations Unies](#) qui stipule que les entreprises doivent adopter des politiques officielles dans lesquelles elles affirment publiquement leur engagement à respecter les normes et principes internationaux relatifs aux droits de l'homme. L'entreprise doit formuler clairement ces engagements par le biais de documents officiels ou d'autres communications qui traduisent la politique officielle de l'entreprise. Il est à noter que cet indicateur évalue l'engagement politique officiel d'une entreprise à l'égard de la liberté d'expression et de la vie privée. Ces engagements doivent être rendus publics. Les entreprises qui font état de leur engagement que pour l'un ou l'autre (liberté d'expression ou protection de la vie privée) recevront une partie des points.

**Sources possibles :**

- Politique de l'entreprise en matière de droits de l'homme
- Déclarations, rapports ou autres communications de l'entreprise reflétant la politique officielle de l'entreprise.
- Rapport annuel de l'entreprise ou rapport de durabilité faisant référence à des engagements politiques officiels

### G2. Gouvernance et surveillance de la direction

La direction de l'entreprise doit **surveiller** l'incidence de ses politiques et de ses pratiques sur la liberté d'expression et la vie privée.

*Éléments :*

1. L'entreprise **indique-t-elle clairement** que son **conseil d'administration** exerce un contrôle formel de l'incidence des pratiques de l'entreprise sur la liberté d'expression et la vie privée ?
2. L'entreprise **indique-t-elle clairement** qu'un **comité, une équipe, un programme ou un agent de l'équipe de direction** contrôle l'incidence des pratiques de l'entreprise sur la liberté d'expression et la vie privée
3. L'entreprise **indique-t-elle clairement** qu'un **comité, une équipe, un programme ou un agent de l'équipe de gestion** contrôle l'incidence des pratiques de l'entreprise sur la liberté d'expression et la vie privée ?

**Détails de l'indicateur :** Cet indicateur étudie si les structures de gouvernance et de gestion interne de l'entreprise tiennent compte de la liberté d'expression et de la protection de la vie privée. Les décisions prises par les dirigeants et les gestionnaires d'entreprises du secteur des technologies de l'information et de la communication affectent considérablement la capacité des personnes à jouir de la liberté d'expression et de la protection de la vie privée. Nous attendons de ces processus décisionnels et de la chaîne de responsabilités au sein des entreprises qu'ils tiennent explicitement compte de ces droits humains.

Pour obtenir le total des points, les entreprises doivent indiquer clairement que chaque niveau de gouvernance (conseil d'administration, direction, responsables de niveau d'équipe de gestion), la liberté d'expression et la protection de la vie privée font l'objet d'une surveillance claire. Au niveau du conseil d'administration, cette surveillance peut comprendre une déclaration du conseil d'administration ou toute autre déclaration publique expliquant la façon dont ce conseil exerce une surveillance des engagements de la société en matière de liberté d'expression et de protection de la vie privée. Aux échelons inférieurs, il peut s'agir d'une unité ou d'une personne de l'entreprise qui relève de la direction ou de l'équipe de direction. La liberté d'expression et la protection de la vie privée doivent figurer explicitement dans la description des responsabilités du comité, du programme, de l'équipe, de l'agent ou tout autre groupe ou personne en charge de la question.

**Sources possibles :**

- Liste des membres du conseil d'administration
- Documents relatifs à la gouvernance de l'entreprise
- Rapport de développement durable de l'entreprise
- Organigramme de l'entreprise
- Politique de l'entreprise en matière de droits de l'homme
- Documents de la Global Network Initiative (si l'entreprise en est membre)

### G3. Mise en œuvre interne

L'entreprise doit disposer de mécanismes pour mettre en œuvre ses engagements en matière de liberté d'expression et de respect de la vie privée au sein de l'entreprise.

*Éléments :*

1. L'entreprise **indique-t-elle clairement** qu'elle offre aux employés une formation sur les questions de liberté d'expression et de protection de la vie privée ?
2. L'entreprise **indique-t-elle clairement** qu'elle possède un **programme de lancement d'alerte** pour les employés qui leur permet de signaler toute préoccupation quant à la façon dont l'entreprise traite la liberté d'expression et le droit à la vie privée de ses utilisateurs ?

**Détails de l'indicateur :** L'indicateur G2 évalue si la direction d'une entreprise s'engage à surveiller les questions liées à la liberté d'expression et à la protection de la vie privée. L'indicateur G3, lui, évalue si l'entreprise communique des informations au sujet de l'existence de mesures institutionnalisées qui traduisent ces engagements et de leur fonctionnement.

Plus précisément, cet indicateur vise à déterminer si l'entreprise aide ses employés à comprendre l'importance de la liberté d'expression et de la protection de la vie privée et, le cas échéant, de quelle manière. Lorsque les employés rédigent le code informatique d'un nouveau produit, examinent les demandes d'obtention de données des utilisateurs ou répondent aux questions des clients sur l'utilisation d'un service, ils agissent d'une manière qui peut directement affecter la liberté d'expression et la vie privée des utilisateurs. Nous attendons des entreprises qu'elles soient transparentes sur le fait qu'elles offrent une formation pour informer les employés de leur rôle dans le respect des droits de l'homme et donner aux employés la possibilité d'exprimer leurs préoccupations à ce sujet.

Pour obtenir la meilleure note, l'entreprise doit communiquer des informations claires sur une formation des employés en matière de liberté d'expression et de protection de la vie privée ainsi que sur l'existence d'un programme de lancement d'alerte à ce sujet. L'entreprise doit aussi préciser que la formation des employés et le programme d'alerte couvrent la liberté d'expression et la protection de la vie privée. Les entreprises peuvent recevoir un crédit partiel pour cet indicateur si le programme de dénonciation d'une entreprise ne mentionne pas expressément les plaintes relatives à la liberté d'expression et à la protection de la vie privée, à condition qu'elles se soient par ailleurs engagées à respecter ces principes et d'une manière qui indique clairement que l'entreprise entendra ces plaintes par le biais de son programme de lancement d'alerte.

**Sources possibles :**

- Code de conduite de l'entreprise
- Manuel de l'employé
- Organigramme de l'entreprise

- Rapport RSE/de durabilité de l'entreprise
- Articles de blog de l'entreprise

## G4. Analyse d'impact

L'entreprise doit mener des audits réguliers, complets et fiables, comme des **études d'impact sur les droits de l'homme (EIDH)**, afin de déterminer comment tous les aspects de ses activités affectent la liberté d'expression et la vie privée et d'atténuer tout risque posé par ces impacts.

*Éléments :*

1. Dans le cadre de son processus décisionnel, l'entreprise tient-elle compte de l'incidence des lois sur la liberté d'expression et la protection de la vie privée dans les territoires où elle exerce ses activités ?
2. L'entreprise évalue-t-elle régulièrement les risques liés à la liberté d'expression et à la protection de la vie privée associés à ses produits et ses services ?
3. L'entreprise évalue-t-elle les risques pour la liberté d'expression et la vie privée associés à une nouvelle activité, y compris le lancement et/ou l'acquisition de nouveaux produits, services ou sociétés ou l'entrée sur de nouveaux marchés ?
4. L'entreprise évalue-t-elle les risques liés à la liberté d'expression et à la protection de la vie privée associés aux processus et aux mécanismes utilisés pour faire respecter ses **conditions générales** ?
5. L'entreprise indique-t-elle qu'elle évalue les risques liés à la liberté d'expression et à la protection de la vie privée associés à son recours à la **prise de décision automatisée**, par exemple au moyen **d'algorithmes** ou d'une **intelligence artificielle** ?
6. L'entreprise évalue-t-elle les risques liés à la liberté d'expression et à la protection de la vie privée associés à ses politiques et pratiques en matière de **publicité ciblée** ?
7. L'entreprise procède-t-elle à une évaluation supplémentaire chaque fois que les études de risques de l'entreprise soulèvent des préoccupations ?
8. Les **cadres supérieurs** et/ou les membres du conseil d'administration de la société examinent-ils et prennent-ils en considération les résultats des études et des audits dans leur prise de décision ?
9. L'entreprise procède-t-elle à des études à intervalles réguliers ?
10. Les études d'impact de l'entreprise sont-elles assurées par une **tierce** partie ?
11. La tierce partie chargée de l'étude d'impact est-elle reconnue pour ses principes pertinents et renommée en matière de droits de l'homme par une organisation fiable ?



**Détails de l'indicateur :** Pour les individus, l'utilisation d'outils numériques comporte des risques en matière de droits de l'homme. Les études d'impact sur les droits de l'homme (EIDH) constituent pour les entreprises un moyen de se renseigner sur ces risques et d'y répondre, ou tout du moins d'essayer de les atténuer, en particulier lorsqu'elles lancent de nouveaux produits et services, lorsqu'elles entrent sur de nouveaux marchés ou intègrent une automatisation du processus décisionnel.

Cet indicateur examine si les entreprises communiquent des informations relatives à l'existence de processus d'études des risques en matière de droits de l'homme, si les entreprises intègrent les études au sujet de la liberté d'expression et de la vie privée dans leur processus décisionnel et, le cas échéant, comment procèdent-elles. Ces études constituent un examen interne systématique visant à s'assurer que les décisions et les pratiques d'une entreprise sont conformes à son engagement (et à sa responsabilité) de respecter la liberté d'expression et la vie privée. Nous attendons des entreprises qu'elles indiquent avoir évalué les risques liés à la liberté d'expression et à la protection de la vie privée associés à leurs nouvelles activités, lorsqu'elles lancent de nouveaux produits ou entrent sur de nouveaux marchés. Nous attendons également d'elles qu'elles évaluent les risques associés à l'application de leurs conditions générales, au déploiement de technologies décisionnelles automatisées (telles que les algorithmes ou les intelligences artificielles) ainsi qu'à leurs politiques et pratiques relatives à la publicité ciblée.

Bien que cet indicateur utilise le terme « études d'impact sur les droits de l'homme », il est possible que les entreprises utilisent des noms différents pour ce processus d'examen. L'appellation revêt moins d'importance que la portée et les résultats de tels processus. Cet indicateur doit inclure un réexamen des études des facteurs relatifs à la vie privée (EFVP) et d'autres processus d'évaluation qui contiennent des caractéristiques ou des éléments énumérés dans cet indicateur, mais pas nécessairement appelés « études d'impact sur les droits de l'homme ».

Il est à noter que cet indicateur n'attend pas des entreprises qu'elles publient les résultats détaillés de leurs études d'impact sur les droits humains, puisqu'une évaluation approfondie comprend des informations sensibles. Il attend plutôt que les entreprises indiquent mener des EIDH et fournissent des renseignements sur ce que le processus comprend. Si une entreprise effectue une EIDH, mais ne l'indique pas publiquement, elle ne reçoit pas de point.

**Sources possibles :**

- Rapports RSE ou de durabilité de l'entreprise
- Politique de l'entreprise en matière de droits de l'homme
- Documents réglementaires (par exemple de la U.S. Federal Trade Commission, la commission fédérale du commerce des États-Unis)
- Rapports d'évaluateurs ou d'organismes d'accréditation tiers
- Rapports de la Global Network Initiative

## **G5. Implication des parties prenantes**

L'entreprise doit **impliquer** un éventail de **parties prenantes** sur les questions de liberté d'expression et de protection de la vie privée.

*Éléments :*

1. L'entreprise est-elle membre d'une **initiative multipartite** dont la mission comprend notamment un engagement en faveur de la liberté d'expression et de la protection de la vie privée selon les principes internationaux des droits de l'homme ?
2. Si l'entreprise n'est pas membre d'une **initiative multipartite**, est-elle membre d'une organisation qui collabore systématiquement et régulièrement avec des acteurs non gouvernementaux et externes au secteur sur les questions de liberté d'expression et de protection de la vie privée ?
3. Si l'entreprise n'est pas membre d'une telle initiative ou organisation, indique-t-elle qu'elle organise ou participe à des réunions avec des **parties prenantes** qui représentent, défendent ou sont des individus dont la liberté d'expression et la vie privée sont directement affectées par les activités de l'entreprise ?

**Détails de l'indicateur :** Cet indicateur vise à déterminer si l'entreprise collabore avec des parties prenantes, et en particulier celles exposées à des risques en matière de droits de l'homme dans le cadre de leurs activités en ligne. Nous attendons que l'engagement des parties prenantes constitue une composante centrale du processus d'élaboration des politiques et d'études d'impact d'une entreprise. L'implication des parties prenantes doit porter sur l'ensemble des questions liées à la liberté d'expression et à la protection de la vie privée des utilisateurs, y compris le processus d'élaboration des conditions générales, des politiques relative à l'identité et à la vie privée d'une entreprise ainsi que l'application de ces politiques.

La collaboration avec des parties prenantes, en particulier celles qui opèrent dans des environnements à haut risque, peut s'avérer délicate. Il se peut qu'une entreprise ne se sente pas à l'aise de communiquer publiquement des renseignements précis sur les parties prenantes qu'elle consulte, le lieu et le moment où elles se rencontrent ou le sujet de leurs discussions. Bien que nous encourageons les entreprises à fournir les détails non-sensibles sur ces collaborations, nous cherchons au moins une déclaration publique indiquant que l'entreprise s'engage auprès de parties prenantes constituées d'utilisateurs dont les droits à la liberté d'expression et à la vie privée sont en danger ou de personnes qui les représentent. L'une des façons pour le public de savoir qu'une entreprise prend ce type d'engagements est l'implication de celle-ci dans une initiative multipartite, dans le cadre de laquelle elle rencontre des représentants de divers groupes d'acteurs concernés, y compris des organismes de défense des droits de l'homme et des droits des groupes à risque.

Si une société reçoit tous les points pour l'élément 1, elle recevra automatiquement tous les points pour les éléments 2 et 3.

**Sources possibles :**

- Rapport RSE ou de durabilité de l'entreprise
- Rapport annuel de l'entreprise

- Blog de l'entreprise
- Liste des adhérents à la Global Network Initiative et à Industry Dialog
- FAQ ou centre d'aide de l'entreprise

## G6. Voies de recours

L'entreprise doit disposer de mécanismes de **réclamations** et de **recours** pour répondre aux préoccupations des utilisateurs en matière de liberté d'expression et de protection de la vie privée.

*Éléments :*

1. L'entreprise **communiquet-elle clairement** qu'elle dispose d'un ou de plusieurs **mécanismes de réclamations** pour que les utilisateurs puissent déposer des plaintes s'ils estiment que les politiques ou pratiques de l'entreprise ont porté atteinte à leur liberté d'expression ou à leur vie privée ?
2. L'entreprise **présente-t-elle clairement** ses procédures de **recours** pour les réclamations relatives à la liberté d'expression ou à la protection de la vie privée ?
3. L'entreprise **communiquet-elle clairement** les délais de traitement des **réclamations** et des **recours** ?
4. L'entreprise **communiquet-elle clairement** le nombre de plaintes reçues relatives à la liberté d'expression et à la protection de la vie privée ?
5. L'entreprise **communiquet-elle clairement** la preuve qu'elle offre un recours pour les réclamations relatives à la liberté d'expression et à la protection de la vie privée ?

**Détails de l'indicateur:** La protection et le respect des droits de l'homme requièrent que les individus disposent de voies de recours lorsqu'ils estiment que leurs droits ont été violés. Cet indicateur examine si les entreprises offrent de tels mécanismes de recours et si elles communiquent publiquement des informations au sujet des procédures implémentées pour répondre aux réclamations des utilisateurs qui estiment que l'entreprise a violé ou directement facilité la violation de leur liberté d'expression ou de leur vie privée.

Nous attendons des entreprises qu'elles présentent clairement un mécanisme de plainte pour que les utilisateurs puissent adresser leurs réclamations s'ils estiment que les politiques ou pratiques de l'entreprise ont porté atteinte à leur liberté d'expression et à leur vie privée. Pour recevoir le nombre de points maximum pour l'élément 1, il n'est pas nécessaire que le mécanisme de traitement des réclamations d'une entreprise indique explicitement qu'il s'applique aux plaintes relatives à la liberté d'expression et à la vie privée. Toutefois, il doit apparaître clairement que le mécanisme peut être utilisé pour déposer tout type de plaintes liées aux droits de l'homme. Nous attendons également des entreprises que les mécanismes de réclamations soit facilement accessibles aux utilisateurs. De plus, l'entreprise doit également expliquer le processus mis en place pour fournir réparation pour ces types de plaintes et

prouver qu'elle agit dans ce sens. Les entreprises doivent présenter des échéanciers clairs pour chaque étape de la procédure de règlement des réclamations et des recours. Ces normes sont décrites dans le Principe 31 des Principes directeurs relatifs aux entreprises et aux droits de l'homme des Nations Unies qui stipule que les entreprises doivent publier des procédures de recours claires, accessibles et prévisibles.

**Sources possibles :**

- Conditions générales de l'entreprise ou contrats d'utilisation équivalents
- Politiques de l'entreprise en matière de contenu
- Politiques de confidentialité de l'entreprise, recommandations ou sites ressources en matière de protection de la vie privée
- Rapport RSE ou de durabilité de l'entreprise
- Centre d'aide de l'entreprise ou guide de l'utilisateur
- Rapport sur la transparence de l'entreprise (pour le nombre de plaintes reçues)

## Liberté d'expression

Les indicateurs de cette catégorie visent à déterminer si l'entreprise respecte le droit à la liberté d'expression, tels qu'énoncé dans la [Déclaration universelle des droits de l'homme](#), le [Pacte international relatif aux droits civils et politiques](#) et d'autres instruments internationaux relatifs aux droits de l'homme. Les politiques et pratiques rendues publiques par l'entreprise montrent comment elle opère pour éviter de contribuer à des actions qui pourraient porter atteinte à la liberté d'expression, sauf lorsque de telles actions sont légales, proportionnées et justifiées. Les entreprises qui obtiennent de bons résultats pour cet indicateur font preuve d'un engagement public ferme envers la transparence, non seulement dans leur réponse aux demandes gouvernementales ou d'autres acteurs, mais aussi dans leur façon de déterminer, de communiquer et d'appliquer les règles privées et les pratiques commerciales qui touchent à la liberté d'expression des utilisateurs.

### F1. Accès aux conditions d'utilisation

Les **conditions d'utilisation** de l'entreprise doivent être **facilement accessibles** et **facilement compréhensibles**.

*Éléments :*

1. Les **conditions d'utilisation** de l'entreprise sont-elles **facilement accessibles** ?
2. Les **conditions d'utilisation** sont-elles disponibles dans la ou les langues les plus couramment parlées par les utilisateurs de l'entreprise ?
3. Les **conditions d'utilisation** sont-elles présentées de manière **facilement compréhensible** ?

**Détails de l'indicateur:** Les conditions d'utilisation d'une entreprise décrivent la relation entre l'utilisateur et l'entreprise. Elles contiennent des règles au sujet des activités et contenus interdits et autorisent les entreprises à prendre des mesures contre les utilisateurs qui les enfreindraient. C'est pourquoi nous attendons des entreprises qu'elles s'assurent que leurs conditions d'utilisation sont facilement accessibles et compréhensibles.

Cet indicateur permet d'évaluer si les conditions d'utilisation de l'entreprise sont faciles à localiser par les utilisateurs. Pour répondre à cette exigence, un document doit se trouver sur la page d'accueil de l'entreprise ou du service, à un ou deux clics de celle-ci ou dans un endroit logique pour les utilisateurs. Les conditions d'utilisation doivent également être disponibles dans la ou les langues principales du marché d'exploitation principal de l'entreprise. De plus, nous attendons d'une entreprise qu'elle prenne des mesures pour aider les utilisateurs à comprendre l'information présentée dans ses documents. Cela comprend, sans toutefois s'y limiter, la présence de résumés, de conseils ou d'explications sur la signification des termes, l'utilisation d'en-têtes de section, d'une taille de police lisible ou de toute autre caractéristique graphique

qui favorise la compréhension, et l'utilisation d'une syntaxe lisible.

**Sources possibles :**

- Conditions générales de l'entreprise, conditions d'utilisation, etc.
- Politique d'utilisation acceptable de l'entreprise, lignes directrices communautaires, règles, etc.

## **F2. Modifications des conditions d'utilisation**

L'entreprise doit **indiquer clairement** que les utilisateurs reçoivent un **avis** et la **documentation** nécessaire lorsqu'elle modifie ses **conditions d'utilisation**.

*Éléments :*

1. L'entreprise **indique-t-elle clairement** qu'elle informe les utilisateurs des changements apportés à ses **conditions d'utilisation** ?
2. L'entreprise **indique-t-elle clairement** comment elle procède pour informer directement les **utilisateurs** de ces changements ?
3. L'entreprise **indique-t-elle clairement** le délai dans lequel elle informe les utilisateurs avant l'entrée en vigueur des changements ?
4. L'entreprise possède-t-elle des **archives publiques** ou un **journal des modifications** ?

**Détails de l'indicateur :** Il est courant pour les entreprises de modifier leurs conditions d'utilisation au fur et à mesure que leurs activités évoluent. Toutefois, ces changements, qui peuvent porter sur les activités et les contenus interdits, peuvent avoir une incidence significative sur le droit à la liberté d'expression des utilisateurs. Nous attendons donc des entreprises qu'elles s'engagent à informer les utilisateurs lorsqu'elles modifient leurs conditions d'utilisation et à leur fournir des informations qui les aident à comprendre la signification de ces changements.

Cet indicateur vise à ce que les entreprises annoncent clairement comment et dans quel délai elle informe les utilisateurs des changements apportés aux conditions d'utilisation. Nous attendons des entreprises qu'elles s'engagent à informer directement les utilisateurs avant l'entrée en vigueur de ces changements. La méthode de notification directe peut varier selon le type de service. Pour les services qui impliquent des comptes utilisateurs, la notification directe peut impliquer l'envoi d'un courrier électronique ou d'un SMS. Pour les services qui ne requièrent pas de compte d'utilisateur, la notification directe peut se traduire par l'affichage d'un avis bien en vue sur la page principale d'accès au service. Cet indicateur cherche aussi des preuves qu'une entreprise fournit publiquement des documents qui contiennent les conditions d'utilisation antérieures afin que le public puisse comprendre l'évolution de ces conditions.

**Sources possibles :**

- Conditions d'utilisation de l'entreprise

### F3. Processus d'application des conditions générales

L'entreprise doit **indiquer clairement** les circonstances dans lesquelles elle peut restreindre l'accès à des **contenus** ou des **comptes utilisateurs**.

*Éléments :*

1. L'entreprise **indique-t-elle clairement** les types de **contenus** ou d'activités qu'elle interdit ?
2. L'entreprise **indique-t-elle clairement** pourquoi elle peut restreindre l'accès au **compte d'un utilisateur** ?
3. L'entreprise **explique-t-elle clairement** les processus qu'elle utilise pour identifier les **contenus** ou les **comptes** qui enfreignent son règlement ?
4. L'entreprise **indique-t-elle clairement** si les autorités gouvernementales reçoivent une attention prioritaire lorsqu'elles réclament la restriction de l'accès à un contenu pour violation du règlement du service ?
5. L'entreprise **indique-t-elle clairement** si des entités privées bénéficient d'un traitement prioritaire lorsqu'elles réclament la restriction de l'accès à un contenu pour violation du règlement du service ?
6. L'entreprise **communiquet-elle clairement** sa manière d'appliquer le règlement ?
7. L'entreprise fournit-elle des exemples clairs pour aider les utilisateurs à comprendre le règlement et son application ?

**Détails de l'indicateur:** Les entreprises peuvent établir des règles qui définissent les contenus que les utilisateurs ont le droit de publier ainsi que les activités autorisées sur le service. Elles ont également la possibilité de restreindre l'accès à un compte utilisateur, à savoir retirer l'accès au service d'un utilisateur si celui-ci a enfreint les règles. Dans le cadre des écosystèmes mobiles, cela inclut la possibilité de restreindre l'accès au compte d'un utilisateur final ou d'un développeur.

Nous attendons donc des entreprises qu'elles présentent clairement leur règlement et son application. Cela inclut les informations sur la façon dont elles apprennent l'existence de contenus ou d'activités contraires à leurs conditions d'utilisation. Par exemple, les entreprises peuvent employer du personnel pour examiner le contenu et/ou l'activité des utilisateurs ou s'appuyer sur des mécanismes de signalement proposés à la communauté qui offrent aux utilisateurs la possibilité de signaler les contenus et/ou l'activité d'autres utilisateurs pour que l'entreprise les examine. Nous attendons également des entreprises qu'elles indiquent clairement si leur politique consiste à étudier en priorité ou plus rapidement les contenus ou les utilisateurs signalés pour infraction au règlement de l'entreprise par des autorités gouvernementales et/ou des membres d'organisations privées ou d'autres entités, identifiées en

tant que tels. Pour les écosystèmes mobiles, nous attendons des entreprises qu'elles indiquent les types d'applications auxquels elles restreignent l'accès. Dans cette communication, l'entreprise doit également fournir des exemples pour aider les utilisateurs à comprendre la portée de ses règles.

**Sources possibles :**

- Conditions d'utilisation de l'entreprise, contrat avec l'utilisateur
- Politique d'utilisation acceptable par l'entreprise, normes communautaires, lignes directrices sur le contenu, politique sur les comportements abusifs ou document similaire expliquant les règles que les utilisateurs doivent suivre
- Support de l'entreprise, centre d'aide ou FAQ (exemples : questions sur la raison pour laquelle un contenu est supprimé, un compte suspendu, etc.)

#### **F4. Données sur l'application des conditions d'utilisation**

L'entreprise doit **communiquer clairement** et régulièrement des données sur le volume et la nature des mesures prises pour restreindre l'accès à des contenus ou des comptes qui enfreignent son règlement.

*Éléments :*

1. L'entreprise **communiquer-t-elle clairement** des données sur le volume et la nature des contenus et des comptes dont l'accès est restreint pour violation de son règlement ?
2. L'entreprise publie-t-elle ces données au moins une fois par an ?
3. Les données publiées par l'entreprise peuvent-elles être exportées sous la forme d'un fichier de **données structurées** ?

**Détails de l'indicateur:** Les entreprises appliquent leurs conditions d'utilisation pour diverses raisons. Nous attendons d'elles qu'elles communiquent publiquement le nombre de cas dans lesquels elles restreignent l'accès à des comptes ou à leurs services. Ces renseignements offrent au public une vision plus transparente et plus précise des processus de suppression de contenu et du rôle des entreprises dans ces suppressions.

Cet indicateur évalue la mise à disposition par l'entreprise de données relatives au nombre de suppressions de contenus ou de restrictions d'accès utilisateurs pour violations des conditions d'utilisation de l'entreprise. La diffusion de ces données offre au public une vision plus précise de l'écosystème de la suppression de contenus ainsi que du rôle des entreprises dans ces suppressions. Les entreprises peuvent obtenir la meilleure note pour cet indicateur que si elles fournissent la preuve qu'elles communiquent clairement et publient régulièrement des données sur leurs décisions de supprimer du contenu. Ces informations doivent être publiées au moins une fois par an et sous la forme d'un fichier de données structurées.



**Source possible :**

- Rapport sur la transparence de l'entreprise

## **F5. Réponse aux demandes de tiers de restreindre l'accès à des contenus ou des comptes**

L'entreprise doit **présenter clairement** ses procédures de réponse aux **demandes gouvernementales** (y compris les ordonnances judiciaires) et aux **demandes privées** de restriction d'accès, de filtrage ou de blocage de **contenus** ou de **comptes**.

*Éléments :*

1. L'entreprise **communique-t-elle clairement** ses procédures de réponse aux **demandes gouvernementales non judiciaires** ?
2. L'entreprise **communique-t-elle clairement** ses procédures de réponse aux **ordonnances judiciaires** ?
3. L'entreprise **communique-t-elle clairement** ses procédures de réponse aux **demandes de gouvernements étrangers** ?
4. L'entreprise **communique-t-elle clairement** ses procédures de réponse aux **demandes privées** ?
5. Les explications de l'entreprise **indiquent-elles clairement** la base juridique sur laquelle elle accède aux **demandes gouvernementales** ?
6. Les explications de l'entreprise **indiquent-elles clairement** sur quelle base elle accède aux **demandes privées** ?
7. L'entreprise **indique-t-elle clairement qu'elle fait preuve de la diligence appropriée** au sujet des **demandes gouvernementales** avant de prendre position ?
8. L'entreprise **indique-t-elle clairement** qu'elle fait preuve de la diligence appropriée à propos des **demandes privées** avant de prendre position ?
9. L'entreprise s'engage-t-elle à refuser les demandes inappropriées ou exagérées **formulées par les gouvernements** ?
10. L'entreprise s'engage-t-elle à refuser les **demandes privées** inappropriées ou exagérées ?
11. L'entreprise fournit-elle des indications claires ou des exemples pour expliquer

l'application de sa procédure de réponse aux **demandes gouvernementales**

12. L'entreprise fournit-elle des explications claires ou des exemples pour expliquer l'application de sa procédure de réponse aux **demandes privées** ?

**Détails de l'indicateur:** Les entreprises reçoivent souvent des demandes de suppression, de filtrage ou de restriction d'accès pour des contenus ou des comptes. Ces demandes émanent d'organismes publics ou de tribunaux (nationaux ou étrangers) ainsi que d'entités privées (non gouvernementales et non judiciaires). Nous attendons des entreprises qu'elles communiquent publiquement leurs procédures de réponse aux demandes des gouvernements et des tribunaux, ainsi qu'aux demandes privées qui découlent d'une procédure fixée ou organisée. Les demandes privées peuvent provenir d'une procédure établie par la loi (par exemple les demandes formulées en vertu du Digital Millennium Copyright Act aux États-Unis, du droit à l'oubli européen, etc.) ou d'un système d'auto-réglementation (par exemple : engagements des entreprises à bloquer certains types d'images).

Cet indicateur évalue si l'entreprise communique clairement la façon dont elle répond aux demandes gouvernementales ou privées de suppression, de filtrage et de restriction d'accès à des contenus ou des comptes. L'entreprise doit notamment exposer les motifs juridiques qui l'obligerait à supprimer des contenus. Dans certains cas, la législation peut empêcher une entreprise de communiquer les informations mentionnées dans les éléments de cet indicateur. RDR documentera de telles situations, mais l'entreprise perdra cependant des points si elle ne remplit pas l'ensemble des éléments. Dans ces cas de figure, la législation va à l'encontre de la compétitivité des entreprises. Nous encourageons celles-ci à plaider en faveur de lois qui leur permettent de respecter pleinement les droits des utilisateurs à la liberté d'expression et à la vie privée.

**Sources possibles :**

- Rapport sur la transparence de l'entreprise
- Directives de l'entreprise relatives à l'application de la législation
- Conditions générales de l'entreprise
- Centre d'aide ou de support de l'entreprise
- Articles de blog de l'entreprise
- Politique de l'entreprise en matière de droit d'auteur ou de propriété intellectuelle

## **F6. Données sur les demandes gouvernementales de restriction d'accès à des contenus ou des comptes**

L'entreprise doit publier régulièrement des données sur les **demandes gouvernementales** (y compris les ordonnances judiciaires) qui visent à supprimer, filtrer ou restreindre l'accès à des **contenus** ou des **comptes**.

*Éléments :*

1. L'entreprise ventile-t-elle le nombre de demandes qu'elle reçoit par pays ?

2. L'entreprise indique-t-elle le nombre de **comptes** concernés ?
3. L'entreprise indique-t-elle le nombre de **contenus** ou d'URL concernés ?
4. L'entreprise dresse-t-elle la liste des types de sujets associés aux demandes qu'elle reçoit ?
5. L'entreprise fournit-elle le nombre de demandes provenant de différentes autorités judiciaires ?
6. L'entreprise fournit-elle le nombre de demandes qu'elle reçoit sciemment de représentants du gouvernement pour restreindre l'accès à des **contenus** ou des **comptes** par des voies non officielles ?
7. L'entreprise indique-t-elle le nombre de demandes auxquelles elle s'est conformée ?
8. L'entreprise publie-t-elle les demandes originales ou communique-t-elle des copies à un **service d'archives publiques tiers** ?
9. L'entreprise communique-t-elle ces données au moins une fois par an ?
10. Les données peuvent-elles être exportées sous la forme d'un fichier de **données structurées** ?

**Détails de l'indicateur:** Les entreprises reçoivent fréquemment des demandes émanant de gouvernements pour supprimer, filtrer ou restreindre l'accès à des contenus ou des comptes. Nous attendons d'une entreprise qu'elle publie régulièrement des données sur le nombre et le type de demandes gouvernementales reçues et sur le nombre de demandes auxquelles elle accède. Les entreprises peuvent recevoir ces demandes par le biais de procédures officielles, comme une ordonnance d'un tribunal, ou par des canaux informels, comme un système mis en place par l'entreprise pour que les individus signalent les contenus qui enfreignent les conditions d'utilisation du service. Les entreprises doivent faire preuve de transparence quant à la nature de ces demandes. Si une entreprise sait qu'une demande émane d'une entité gouvernementale ou d'un tribunal, elle doit l'indiquer en tant que telle. Ces données offrent au public la possibilité de comprendre les relations entre entreprises et gouvernements en matière de contrôle du contenu en ligne. En outre, elles aident le public à tenir les entreprises et les gouvernements responsables de leurs obligations en matière de respect et de protection de la liberté d'expression.

Dans certains cas, la loi peut empêcher une entreprise de divulguer les informations mentionnées dans les éléments de cet indicateur. Par exemple, nous attendons des entreprises qu'elles publient des chiffres exacts plutôt que des fourchettes. Toutefois, nous reconnaissons que les lois ne l'autorisent pas toujours. Les chercheurs documenteront donc les situations le cas échéant, mais une entreprise perdra néanmoins des points si elle ne respecte pas l'ensemble des critères spécifiés dans les éléments ci-dessus. De telles situations empêchent les entreprises de se conformer aux bonnes pratiques. Nous encourageons donc les entreprises à plaider en faveur de lois qui leur permettent de respecter pleinement les droits des

utilisateurs à la liberté d'expression et à la vie privée.

**Sources possibles :**

- Rapport sur la transparence de l'entreprise

## **F7. Données sur les demandes privées de restriction d'accès à des contenus ou des comptes**

L'entreprise doit publier régulièrement des données sur les **demandes privées** de suppression, de filtrage ou de restriction d'accès à des **contenus** ou des **comptes**.

*Éléments :*

1. L'entreprise ventile-t-elle le nombre de demandes qu'elle reçoit par pays ?
2. L'entreprise indique-t-elle le nombre de **comptes** concernés?
3. L'entreprise indique-t-elle le nombre de **contenus** ou d'UR' concernés ?
4. L'entreprise énumère-t-elle les motifs de suppression associés aux demandes qu'elle reçoit ?
5. L'entreprise décrit-elle les types d'acteurs dont elle reçoit les demandes ?
6. L'entreprise indique-t-elle le nombre de demandes auxquelles elle a accédé ?
7. L'entreprise publie-t-elle les demandes originales ou communique-t-elle des copies à un **service d'archives publiques tiers** ?
8. L'entreprise communique-t-elle ces données au moins une fois par an ?
9. Les données peuvent-elles être exportées sous la forme d'un fichier de **données structurées** ?
10. L'entreprise **indique-t-elle clairement** que ses rapports couvrent tous les types de **demandes privées** qu'elle reçoit ?

**Détails de l'indicateur:** Les entreprises reçoivent fréquemment des demandes de tiers par le biais de procédures privées (non gouvernementales ou non judiciaires) pour supprimer, filtrer ou restreindre l'accès à des contenus ou des comptes. Nous attendons des entreprises qu'elles publient régulièrement des données sur le nombre et le type de demandes reçues dans le cadre de procédures privées et sur le nombre de demandes auxquelles elles accèdent. Cet indicateur se concentre sur les demandes qui passent par un processus défini ou organisé. Il peut s'agir d'un processus établi par la loi (par exemple les demandes formulées en vertu du Digital Millennium Copyright Act aux États-Unis, du droit à l'oubli européen, etc.) ou d'un système d'auto-réglementation (par exemple l'engagement des entreprises à bloquer certains types d'images). Cet indicateur n'examine pas les rapports des entreprises sur les contenus ou les

comptes soumis à des restrictions d'accès en vertu des mécanismes d'application des conditions d'utilisation (pour cela, se rapporter à l'indicateur F4).

**Sources possibles :**

- Rapport sur la transparence de l'entreprise

## **F8. Information aux utilisateurs sur la restriction d'accès à des contenus et des comptes**

L'entreprise doit **indiquer clairement** qu'elle **informe les utilisateurs** lorsqu'elle restreint l'accès à des **contenus** ou des **comptes**.

*Éléments :*

1. Si l'entreprise héberge du **contenu** généré par les utilisateurs, est-ce qu'elle **indique clairement** qu'elle informe les **utilisateurs** ayant généré le **contenu** lorsque l'accès à celui-ci est restreint ?
2. L'entreprise **indique-t-elle clairement** qu'elle avise les utilisateurs qui tentent d'accéder à du **contenu** dont l'accès est restreint ?
3. Dans ces notifications, l'entreprise **indique-t-elle clairement** la raison de la restriction d'accès au **contenu** (juridique ou autre) ?
4. L'entreprise **indique-t-elle clairement** qu'elle avise les utilisateurs lorsqu'elle restreint l'accès à leur compte ?

**Détails de l'indicateur:** L'indicateur F3 examine la divulgation par les entreprises des restrictions d'accès qui portent sur les publications ou les activités des utilisateurs du service. Cet indicateur F8 vise à établir si les entreprises indiquent clairement qu'elles avisent les utilisateurs en cas de mesures de ce type (que ce soit en raison de l'application des conditions d'utilisation ou de demandes de restriction d'accès de la part d'un tiers). La décision d'une entreprise de restreindre ou de supprimer l'accès à des contenus ou des comptes peut avoir une incidence significative sur la liberté d'expression et les droits d'accès à l'information des utilisateurs. Nous attendons donc des entreprises qu'elles déclarent aviser les utilisateurs lorsqu'elles suppriment des contenus, restreignent l'accès à un compte ou limitent de toute autre manière la capacité des utilisateurs d'accéder à un service. Si une entreprise supprime un contenu publié par un utilisateur, nous attendons d'elle qu'elle l'informe de sa décision. Si un autre utilisateur tente d'accéder à un contenu dont l'entreprise a restreint l'accès, nous attendons de l'entreprise qu'elle avise cet utilisateur de la restriction d'accès au contenu. Nous attendons également des entreprises qu'elles précisent les motifs de leurs décisions. Ces informations doivent faire partie intégrante des explications fournies par les entreprises sur leur contenu et leurs pratiques en matière de restriction d'accès.

**Sources possibles :**

- Conditions d'utilisation du service, politique d'utilisation acceptable, normes communautaires, directives relatives au contenu, politique sur les comportements abusifs ou document similaire qui explique les règles que les utilisateurs doivent suivre.
- Page d'assistance de l'entreprise, centre d'aide ou FAQ (par exemple les questions sur les motifs de suppression de contenu, de suspension de compte, etc.)
- Directives de l'entreprise à l'intention des développeurs
- Politique de l'entreprise en matière de droits de l'homme

## F9. Gestion du réseau (entreprises de télécommunications)

L'entreprise doit **indiquer clairement** qu'elle n'établit pas de priorité, ne bloque pas, ni ne retarde certains types de trafic, d'**applications**, de **protocoles** ou de **contenu** pour une raison autre que celle d'assurer la qualité du service et la fiabilité du réseau.

*Éléments :*

1. L'entreprise **indique-t-elle clairement** qu'elle n'établit pas de **hiérarchie**, ne bloque pas, ni ne retarde certains types de trafic, d'**applications**, de **protocoles** ou de **contenu** pour des raisons autres que l'assurance de la qualité du service et de la fiabilité du réseau ?
2. Si l'entreprise a recours à de telles pratiques, **indique-t-elle clairement** pourquoi ?

**Détails de l'indicateur:** Cet indicateur évalue si les entreprises de télécommunications indiquent clairement se livrer ou non à des pratiques qui affectent le flux de contenus sur leurs réseaux, comme la **limitation** ou la **régulation du trafic**. Nous attendons des entreprises qu'elles s'engagent publiquement à éviter la hiérarchisation ou la dégradation du contenu. Dans certains cas, une entreprise peut s'engager dans des pratiques légitimes de régulation du trafic afin de garantir le flux de trafic sur ses réseaux. Nous attendons des entreprises qu'elles annoncent publiquement de telles pratiques et en expliquent les motifs. Il est à noter que cet indicateur ne concerne pas le blocage de contenu, traité dans l'indicateur F3. Toutefois, cet indicateur inclut l'information relative au blocage de services, d'applications ou d'appareils, une pratique considérée comme un type de hiérarchisation.

**Sources possibles :**

- Explications de l'entreprise relatives à ses pratiques de gestion du réseau ou du trafic

## F10. Coupure de réseau (entreprises de télécommunications)

L'entreprise doit clairement indiquer les circonstances dans lesquelles elle **peut couper ou restreindre l'accès au réseau**, à des **protocoles**, des services, ou des **applications** spécifiques sur le réseau.

*Éléments :*

1. L'entreprise explique-t-elle clairement les motifs pour lesquels elle peut être amenée à interrompre le service pour une région spécifique ou un groupe particulier d'utilisateurs ?
2. L'entreprise explique-t-elle clairement pourquoi elle peut restreindre l'accès à des applications ou des protocoles spécifiques (par exemple appels VoIP, messagerie) dans une zone particulière ou pour un groupe d'utilisateurs spécifiques ?
3. L'entreprise explique-t-elle clairement sa procédure de réponse aux demandes de **d'interruption** ou de restriction d'accès à un service ?
4. L'entreprise s'engage-t-elle à refuser les demandes d'**interruption ou de restriction d'accès à un service** ?
5. L'entreprise **indique-t-elle clairement** qu'elle informe directement les utilisateurs lorsqu'elle **interrompt ou restreint l'accès à un service** ?
6. L'entreprise indique-t-elle le nombre de demandes d'**interruption du réseau** qu'elle reçoit ?
7. L'entreprise identifie-t-elle clairement l'autorité légale spécifique dont émane la demande ?
8. L'entreprise indique-t-elle le nombre de demandes auxquelles elle a accédé ?

**Détails de l'indicateur:** Les coupures de réseaux constituent une menace croissante pour les droits de l'homme. Le [Conseil des droits de l'homme des Nations Unies](#) condamne cette pratique qu'il considère comme une violation du droit international relatif aux droits de l'homme et a appelé les gouvernements à s'abstenir de prendre de telles mesures. Pourtant, les gouvernements [ordonnent toujours plus souvent](#) aux entreprises de télécommunications de procéder à des interruptions de réseau, ce qui les incite à prendre des mesures contraires à leur responsabilité en matière de respect des droits humains. Nous attendons des entreprises qu'elles communiquent pleinement les circonstances dans lesquelles elles pourraient prendre de telles mesures et qu'elles rendent compte de telles demandes.

**Sources possibles :**

- Conditions générales de l'entreprise, politique d'utilisation acceptable, normes communautaires, directives sur le contenu, politique sur les comportements abusifs ou document similaire qui explique les règles que les utilisateurs doivent suivre.
- Rapport sur la transparence de l'entreprise
- Directives de l'entreprise relatives à l'application du droit

## **F11. Politique relative à l'identité**

L'entreprise ne doit pas **exiger** des utilisateurs qu'ils prouvent leur identité avec une **pièce d'identité officielle** ou toute autre forme d'authentification susceptible de les identifier hors ligne.

1. L'entreprise **exige-t-elle** que les utilisateurs prouvent leur identité avec leur **pièce d'identité officielle** ou avec d'autres formes d'authentification susceptibles de les identifier hors ligne ?

**Détails de l'indicateur:** La capacité de communiquer de façon anonyme est essentielle à la liberté d'expression en ligne et hors ligne. L'utilisation d'un vrai nom en ligne ou l'obligation pour les utilisateurs de fournir à une entreprise des informations d'identification, établit un lien entre une personne spécifique et ses activités en ligne. Ces pratiques présentent des risques en matière de droits humains pour ceux qui, par exemple, expriment des opinions divergentes de leur gouvernement ou qui s'engagent en faveur de causes non autorisées par le gouvernement. Elles présentent également des risques pour les personnes persécutées en raison de leurs croyances religieuses ou de leur orientation sexuelle.

Nous attendons donc des entreprises qu'elles indiquent si les utilisateurs doivent prouver leur identité au moyen d'une pièce d'identité officielle ou toute autre forme d'identification susceptibles de les identifier hors ligne. Nous reconnaissons que les utilisateurs peuvent être amenés à fournir des informations susceptibles de les identifier hors ligne afin d'accéder aux fonctionnalités payantes de divers produits et services. Toutefois, les utilisateurs doivent pouvoir accéder aux fonctionnalités qui ne requièrent pas de paiement sans avoir à fournir d'informations susceptibles de les identifier hors ligne.

Cet indicateur s'applique aux entreprises Internet, aux entreprises de l'écosystème mobile et aux services mobiles prépayés (pour les entreprises de télécommunications).

**Sources possibles :**

- Conditions générales de l'entreprise ou document équivalent
- Centre d'aide de l'entreprise
- Page d'inscription auprès de l'entreprise

## Vie privée

Les indicateurs de cette catégorie étudient si, dans les politiques et les pratiques rendues publiques par l'entreprise, celle-ci présente des moyens concrets par lesquels elle protège le droit à la vie privée des utilisateurs tel qu'il est énoncé dans la [Déclaration universelle des droits de l'homme](#), le [Pacte international relatif aux droits civils et politiques](#) et d'autres instruments internationaux relatifs aux droits de l'homme. Les politiques et pratiques rendues publiques par l'entreprise montrent comment elle opère pour éviter de contribuer à des actions susceptibles de porter atteinte à la vie privée des utilisateurs, sauf lorsque de telles actions sont légales, proportionnées et justifiées. Les entreprises qui obtiennent de bons résultats sur ces indicateurs démontrent un engagement public ferme en faveur de la transparence non seulement en ce qui concerne la façon dont elles répondent aux demandes gouvernementales et d'autres intervenants, mais aussi la façon dont elles déterminent, communiquent et appliquent les règles internes et les pratiques commerciales qui touchent la vie privée des utilisateurs. Elles font également preuve d'un engagement ferme en faveur de la protection et de la défense de la sécurité numérique des utilisateurs.



## P1. Accès aux politiques de confidentialité

La **politique de confidentialité** de l'entreprise doit être **facilement accessible** et **facilement compréhensible**.

*Éléments :*

1. La politique de confidentialité de l'entreprise est-elle **facilement accessible** ?
2. La politique de confidentialité est-elle disponible dans la ou les langues les plus couramment utilisées par les utilisateurs de l'entreprise ?
3. La politique de confidentialité est-elle présentée de manière **facilement compréhensible** ?
4. Pour les **écosystèmes mobiles** : L'entreprise indique-t-elle qu'elle exige que les applications proposées dans son **app store** fournissent aux utilisateurs une politique de confidentialité ?

**Détails de l'indicateur:** Les politiques de confidentialité traitent de la façon dont les entreprises collectent, gèrent, utilisent et sécurisent les données sur les utilisateurs ainsi que les données fournies par les utilisateurs. Voilà pourquoi les entreprises devraient garantir que les utilisateurs puissent facilement trouver les informations relatives à la confidentialité et les aider comprendre leur signification.

Cet indicateur attend des entreprises qu'elles fournissent des politiques de confidentialité faciles à trouver, disponibles dans les langues des principaux marchés dans lesquels l'entreprise opère et s'assure qu'elles soient facilement compréhensibles. Si l'entreprise offre plusieurs produits et services, elle doit indiquer clairement à quels produits et services les politiques s'appliquent.

Un document facile à trouver doit se trouver sur la page d'accueil de l'entreprise ou du service, à un ou deux clics de celle-ci ou dans un endroit logique où les utilisateurs sont susceptibles de le trouver. Les conditions devraient également être disponibles dans la ou les langues principales du marché d'exploitation principal. De plus, nous attendons d'une entreprise qu'elle prenne des mesures pour aider les utilisateurs à comprendre les informations présentées dans ses documents. Il peut s'agir, entre autres, de fournir des résumés, des conseils ou des directives qui expliquent la signification des termes, en utilisant des en-têtes de section, une taille de police lisible ou d'autres caractéristiques graphiques pour aider les utilisateurs à comprendre le document ou de rédiger des documents avec une syntaxe lisible. Les conditions d'utilisation ne sont pas incluses dans cet indicateur puisqu'elles font l'objet d'indicateurs distincts dans la catégorie « Liberté d'expression ».

**Sources possibles :**

- Politique de confidentialité de l'entreprise
- Politique d'utilisation des données de l'entreprise

## P2. Modifications apportées à la politique de confidentialité

L'entreprise doit **indiquer clairement** qu'elle fournit des **avis** et de la **documentation** aux utilisateurs lorsqu'elle modifie ses **politiques de confidentialité**.

*Éléments :*

1. L'entreprise **indique-t-elle clairement** qu'elle informe les utilisateurs des changements apportés à ses politiques de confidentialité ?
2. L'entreprise **présente-t-elle clairement** la procédure utilisée pour informer les utilisateurs des changements ?
3. L'entreprise **indique-t-elle clairement** le délai dans lequel elle informe les utilisateurs avant l'entrée en vigueur des changements ?
4. L'entreprise tient-elle des **archives publiques** ou un **journal des modifications** ?
5. Pour les **écosystèmes mobiles** : L'entreprise **indique-t-elle clairement** qu'elle exige que les applications vendues par l'intermédiaire de son **app store** avertissent les utilisateurs lors de la modification de leur politique de confidentialité ?

**Détails de l'indicateur:** Les entreprises modifient fréquemment leurs politiques de confidentialité au fur et à mesure de l'évolution de leurs activités. Toutefois, ces changements peuvent avoir une incidence sur le droit à la vie privée des utilisateurs s'ils touchent aux données personnelles que les entreprises peuvent recueillir, partager et conserver. Nous attendons donc des entreprises qu'elles s'engagent à informer les utilisateurs lorsqu'elles modifient leurs politiques de confidentialité et à leur fournir des informations pour les aider à comprendre la signification de ces changements.

Cet indicateur recherche des informations claires des entreprises au sujet de leur méthode et du délai d'information des utilisateurs au sujet des changements apportés aux politiques de confidentialité. Nous attendons des entreprises qu'elles s'engagent à aviser directement les utilisateurs avant l'entrée en vigueur des changements. La méthode de notification directe peut différer selon le type de service. Pour les services qui nécessitent un compte utilisateur, la notification directe peut se traduire par l'envoi d'un courrier électronique ou d'un SMS. Pour les services qui ne nécessitent pas de compte utilisateur, la notification directe doit se faire au moyen d'un avis bien en vue sur la page principale du site Internet ou la plateforme d'accès au service. Cet indicateur vise à déterminer si une entreprise fournit publiquement des documents qui contiennent les politiques de confidentialité antérieures afin que le public puisse comprendre leur évolution.

**Sources possibles :**

- Politique de confidentialité de l'entreprise
- Politique d'utilisation des données de l'entreprise

### P3. Collecte des données utilisateurs

L'entreprise doit **communiquer clairement** quelles **données utilisateurs** elle **collecte** et comment.

*Éléments :*

1. L'entreprise **indique-t-elle clairement** les types de renseignements qu'elle **recueille** sur les utilisateurs ?
2. Pour chaque type de **données utilisateurs** recueillies, l'entreprise **indique-t-elle clairement** la façon dont les informations sont collectées ?
3. L'entreprise **indique-t-elle clairement** qu'elle limite la collecte de **données utilisateurs** aux informations directement pertinentes et nécessaires pour atteindre l'objectif de son service ?
4. Pour les **écosystèmes mobiles** : L'entreprise **indique-t-elle clairement** qu'elle évalue si les **politiques de confidentialité** des **applications** tierces mises à disposition via son **app store** divulguent les **données utilisateurs** que les applications collectent ?
5. Pour les **écosystèmes mobiles** : L'entreprise **indique-t-elle clairement** qu'elle évalue si les **applications** tierces mises à disposition via son **app store** limitent la collecte **d'informations sur les utilisateurs** à celles directement pertinentes et nécessaires pour atteindre l'objectif de l'application ?

**Détails de l'indicateur:** L'entreprise recueille un large éventail de renseignements personnels sur les utilisateurs, qu'il s'agisse de détails personnels, de profils de compte, d'activités ou de localisation de l'utilisateur. Nous attendons des entreprises qu'elles indiquent clairement les renseignements qu'elles collectent sur les utilisateurs (tels que définis par RDR ci-dessous) et comment. Nous attendons également des entreprises qu'elles s'engagent à respecter le principe de la **minimisation des données** et qu'elles démontrent comment ce principe façonne leurs pratiques en matière de données utilisateurs. Si les entreprises recueillent plusieurs types de renseignements, nous attendons d'elles qu'elles fournissent des détails sur la façon dont elles traitent chaque type de renseignements. Pour les écosystèmes mobiles, nous attendons des entreprises qu'elles indiquent clairement si les politiques de confidentialité des applications disponibles dans leur app store spécifient quelles informations sur les utilisateurs les applications collectent et si ces politiques sont conformes aux principes de minimisation des données.

RDR interprète largement l'expression **données utilisateurs** qui, selon notre définition, constitue « toute donnée associée à une personne identifiable ou pouvant être associée à une telle personne par la combinaison d'ensembles de données ou l'utilisation de techniques d'exploration de données. »

Pour plus de détails, les **données utilisateurs** correspondent à toute donnée qui fournit des renseignements sur les caractéristiques et/ou les activités d'un utilisateur. Ces informations

peuvent ou non être liées à un compte utilisateur spécifique. Ces informations incluent, sans s'y limiter, la correspondance personnelle, le contenu généré par l'utilisateur, les préférences et paramètres du compte, les données de connexion et d'accès, les données relatives aux activités d'un utilisateur ou les préférences recueillies auprès de tiers, au moyen du suivi comportemental ou de l'achat de données, ainsi que toute forme de métadonnées. Les données utilisateurs ne sont jamais considérées comme anonymes, sauf lorsqu'elles sont incluses dans le seul but de générer des mesures globales (par exemple, le nombre d'utilisateurs mensuels actifs). Par exemple, la déclaration « Notre service compte un million d'utilisateurs actifs par mois » fait état de données anonymes, car elle ne donne pas suffisamment d'informations pour savoir qui sont ces utilisateurs.

Les données anonymes sont « des données qui ne sont en aucune façon liées à un autre élément d'information susceptible d'identifier un utilisateur ».

Cette vision étendue est nécessaire pour refléter plusieurs faits. Tout d'abord, les analystes compétents peuvent « dés-anonymiser » de larges ensembles de données, ce qui rend presque toute promesse d'anonymisation impossible à tenir. En substance, les données liées à des « identifiants anonymes » ne sont en réalité pas anonymes. Elles correspondent plutôt à des données souvent pseudonymes qui peuvent être associées à l'identité hors ligne de l'utilisateur. Deuxièmement, les métadonnées peuvent s'avérer autant voire plus révélatrices des liens et des intérêts d'un utilisateur que les données de « contenu », ce qui les rend essentielles. Troisièmement, les entités qui ont accès à de nombreuses sources de données, comme les courtiers en données et les gouvernements, peuvent être en mesure de coupler plusieurs sources de données pour révéler des renseignements sur les utilisateurs. Ainsi, les acteurs à la pointe peuvent utiliser des données qui semblent anonymes pour établir un portrait plus large d'un utilisateur.

Dans certains cas, les lois ou règlements peuvent obliger les entreprises à collecter certaines informations, voire leur interdire ou les décourager de divulguer les renseignements qu'elles recueillent sur les utilisateurs. Les chercheurs documenteront ce type de situations, qui n'empêcheront pas les entreprises de perdre des points si elles ne respectent pas tous les éléments. Dans ces cas de figure, la législation va à l'encontre de la compétitivité des entreprises. Nous encourageons celles-ci à plaider en faveur de lois qui leur permettent de respecter pleinement les droits des utilisateurs à la liberté d'expression et à la vie privée.

#### **Sources possibles :**

- Politique de confidentialité de l'entreprise
- Site internet ou section du site de l'entreprise sur la protection ou la collecte des données

## **P4. Partage des données utilisateurs**

L'entreprise doit **indiquer clairement** quelles **données utilisateurs** elle **partage** et avec qui.

#### *Éléments :*

1. Est-ce que l'entreprise **communiquera clairement**, pour chaque type d'**informations sur les utilisateurs** collectées, si celles-ci sont partagées ?

2. Est-ce que l'entreprise **communiquera clairement**, pour chaque type d'**informations sur les utilisateurs** partagées, avec qui celles-ci sont partagées ?
3. L'entreprise **indique-t-elle clairement** qu'elle peut partager des renseignements sur les utilisateurs avec des gouvernements ou autorités judiciaires ?
4. Pour chaque type d'**informations sur les utilisateurs** que l'entreprise partage, l'entreprise **divulgue-t-elle clairement** le nom de tous les **tiers** avec lesquels elle les partage ?
5. Pour les **écosystèmes mobiles** : L'entreprise **indique-t-elle clairement** qu'elle évalue si les **politiques de confidentialité** des **applications** tierces mises à disposition via son **app store** indiquent quelles informations sont partagées par les applications ?
6. Pour les **écosystèmes mobiles** : L'entreprise **indique-t-elle clairement** qu'elle évalue si les **politiques de confidentialité** des **applications** tierces mises à disposition via son **app store** indiquent avec quels types de tiers elles partagent des informations sur les utilisateurs ?

**Détails de l'indicateur:** Les entreprises recueillent un large éventail de renseignements personnels à notre sujet : des informations personnelles des profils de nos comptes à nos activités de navigation et notre localisation. En outre, elles partagent souvent ces informations avec des tiers, y compris des annonceurs, des gouvernements et des autorités judiciaires. Nous attendons des entreprises qu'elles communiquent clairement quelles informations de ses utilisateurs (selon la définition de RDR) elles partagent et avec qui. De plus, les entreprises doivent préciser si elles partagent des renseignements sur les utilisateurs avec les gouvernements et les entités commerciales. Pour les écosystèmes mobiles, nous attendons des entreprises qu'elles indiquent clairement si les politiques de confidentialité des applications disponibles dans leur app store spécifient quelles informations sur les utilisateurs les applications partagent avec des tiers.

Dans certains cas, les lois ou règlements peuvent obliger les entreprises à collecter certaines informations, voire leur interdire ou les décourager de divulguer les renseignements qu'elles recueillent sur les utilisateurs. Les chercheurs documenteront ce type de situations, qui n'empêcheront pas les entreprises de perdre des points si elles ne respectent pas tous les éléments. Dans ces cas de figure, la législation va à l'encontre de la compétitivité des entreprises. Nous encourageons celles-ci à plaider en faveur de lois qui leur permettent de respecter pleinement les droits des utilisateurs à la liberté d'expression et à la vie privée.

**Sources possibles :**

- Politique de confidentialité de l'entreprise
- Politiques de l'entreprise relatives au partage des données, aux interactions avec les tiers

## **P5. Objectif de la collecte et du partage des données utilisateurs**

L'entreprise doit **indiquer clairement** pourquoi elle **collecte** et partage des **informations sur les utilisateurs**.

*Éléments :*

1. Pour chaque type d'**informations sur les utilisateurs** que l'entreprise collecte, l'entreprise **divulgue-t-elle clairement** l'objet de la collecte ?
2. L'entreprise **indique-t-elle clairement** si elle combine des **informations sur les utilisateurs** provenant de différents de ses services et, le cas échéant, pourquoi elle procède ainsi ?
3. Pour chaque type d'**information sur les utilisateurs** que l'entreprise partage, est-ce que l'entreprise **indique clairement** le motif du partage ?
4. L'entreprise **indique-t-elle clairement** qu'elle limite son utilisation des **données utilisateurs** aux fins pour lesquelles elles ont été collectées ?

**Détails de l'indicateur:** Nous attendons des entreprises qu'elles communiquent clairement le but de la collecte et du partage de chaque type d'informations sur les utilisateurs qu'elles recueillent et partagent. De plus, de nombreuses entreprises possèdent ou exploitent divers produits et services. Nous attendons d'elles qu'elles indiquent clairement comment les renseignements sur les utilisateurs peuvent être partagés ou combinés entre leurs services. Enfin, les entreprises doivent s'engager publiquement à respecter le principe de limitation de l'utilisation, qui fait partie, entre autres, des lignes directrices de l'OCDE en matière de protection de la vie privée.

**Sources possibles :**

- Politique de confidentialité de l'entreprise
- Site ou section du site internet de l'entreprise sur la protection et la collecte des données

## **P6. Conservation des données utilisateurs**

L'entreprise doit **indiquer clairement** la durée de **conservation des informations sur les utilisateurs**.

*Éléments :*

1. Pour chaque type d'**informations sur les utilisateurs** qu'elle recueille, l'entreprise **indique-t-elle clairement** combien de temps elle **conserve** cette information ?
2. L'entreprise **indique-t-elle clairement** les renseignements **dépersonnalisés** qu'elle conserve sur les utilisateurs ?

3. L'entreprise **présente-t-elle clairement** le processus de **dépersonnalisation des renseignements sur les utilisateurs** ?
4. L'entreprise **indique-t-elle clairement** qu'elle supprime toutes les **informations sur les utilisateurs** une fois leur compte résilié ?
5. L'entreprise **indique-t-elle clairement** le délai dans lequel elle supprime les **informations sur les utilisateurs** une fois leur compte résilié ?
6. Pour les **écosystèmes mobiles** : L'entreprise **indique-t-elle clairement** qu'elle vérifie si les politiques de confidentialité des **applications** tierces disponibles dans son **app store** spécifient combien de temps elles conservent les informations des utilisateurs ?
7. Pour les **écosystèmes mobiles** : L'entreprise **indique-t-elle clairement** qu'elle vérifie si les politiques de confidentialité des **applications** tierces disponibles dans son **app store** spécifient que toutes les informations des utilisateur sont effacées lorsqu'ils suppriment leur compte ou l'application ?

**Détails de l'indicateur:** Tout comme nous attendons des entreprises qu'elles communiquent quelles informations à notre sujet elles collectent et partagent, nous attendons aussi des entreprises qu'elles indiquent clairement la durée de conservation de ces informations et dans quelle mesure elles suppriment les données identificatrices des renseignements personnels conservés. De plus, les utilisateurs doivent être en mesure de comprendre ce qu'il advient de leurs informations lorsqu'ils suppriment leur compte. Dans certains cas, les lois ou règlements peuvent exiger des entreprises qu'elles conservent certaines informations pendant un temps donné. Le cas échéant, les entreprises doivent clairement indiquer ces contraintes légales aux utilisateurs. Les entreprises qui choisissent de conserver les informations sur les utilisateurs pour de longues périodes doivent s'assurer que ces données ne sont pas associées à un utilisateur en particulier. Malgré les débats actuels sur l'efficacité des processus d'anonymisation et du perfectionnement croissant des pratiques de ré-identification, nous considérons toujours l'anonymisation comme une mesure positive que les entreprises peuvent prendre pour protéger la vie privée de leurs utilisateurs.

De plus, si les entreprises recueillent plusieurs types d'informations, nous attendons d'elles qu'elles indiquent clairement la durée de conservation pour *chaque type d'informations*. Pour les écosystèmes mobiles, nous attendons des entreprises qu'elles indiquent si les politiques de confidentialité des applications disponibles dans leur boutique d'application spécifient combien de temps l'application conserve les informations des utilisateurs et si toutes les informations des utilisateurs sont supprimées lorsqu'ils suppriment leur compte ou l'application.

**Sources possibles :**

- Politique de confidentialité de l'entreprise
- Site ou section du site internet de l'entreprise sur la protection et la collecte des données



## P7. Contrôle des utilisateurs sur leurs propres informations

L'entreprise doit **communiquer clairement** aux utilisateurs les **options de contrôle** dont ils disposent au sujet de la **collecte**, la **conservation** et l'utilisation par l'entreprise de leurs renseignements personnels.

*Éléments :*

1. Pour chaque type d'**informations sur les utilisateurs** que l'entreprise recueille, **indique-t-elle clairement** si les utilisateurs peuvent contrôler la collecte de cette information ?
2. Pour chaque type d'**information sur les utilisateurs** que l'entreprise recueille, **indique-t-elle clairement** si les utilisateurs peuvent supprimer les informations en question ?
3. L'entreprise **indique-t-elle clairement** qu'elle offre aux utilisateurs des **options pour contrôler** la façon dont leurs renseignements personnels sont utilisés à des fins de publicité ciblée ?
4. L'entreprise **indique-t-elle clairement** que la publicité ciblée est désactivée par défaut ?
5. Pour les **écosystèmes mobiles** : L'entreprise **indique-t-elle clairement** qu'elle fournit aux utilisateurs des options pour contrôler les fonctionnalités de **géolocalisation** de l'appareil ?

**Détails de l'indicateur:** Nous attendons des entreprises qu'elles communiquent clairement les options dont disposent les utilisateurs pour contrôler les renseignements qu'elles recueillent et conservent à leur sujet. Permettre aux utilisateurs de contrôler les informations les concernant qu'une entreprise recueille et conserve signifie leur donner la possibilité de supprimer des types spécifiques d'informations à leur sujet sans qu'ils doivent supprimer l'intégralité de leur compte. Nous attendons donc des entreprises qu'elles indiquent clairement si les utilisateurs ont la possibilité de supprimer certains types d'informations.

En outre, nous attendons des entreprises qu'elles permettent aux utilisateurs de contrôler l'utilisation de leurs informations à des fins publicitaires ciblées. La publicité ciblée exige la collecte et la conservation d'une quantité considérable d'informations sur les utilisateurs, des pratiques qui équivalent à un pistage. Les entreprises devraient donc indiquer clairement si les utilisateurs ont la possibilité de contrôler la manière dont leurs informations sont utilisées à ces fins.

Pour les écosystèmes mobiles, nous attendons des entreprises qu'elles présentent clairement les options dont disposent les utilisateurs pour contrôler la collecte de leurs informations de localisation. L'emplacement d'un utilisateur change fréquemment et de nombreux utilisateurs transportent leurs appareils mobiles presque en permanence, ce qui rend la collecte de ce type d'informations particulièrement sensible. En outre, les paramètres de localisation des écosystèmes mobiles peuvent influencer sur la façon dont d'autres produits et services accèdent



aux données de localisation. Par exemple, les applications mobiles peuvent permettre aux utilisateurs de contrôler leurs informations de localisation. Toutefois, si les appareils sur lesquels ces applications mobiles s'exécutent collectent des données de géolocalisation par défaut et n'autorisent pas les utilisateurs à désactiver ce réglage, il se peut que les utilisateurs ne soient pas en mesure de limiter la collecte de leurs informations de localisation par les applications mobiles. Pour ces raisons, nous attendons des entreprises qu'elles indiquent comment les utilisateurs peuvent contrôler la façon dont leur appareil interagit avec leurs données de localisation.

**Sources possibles :**

- Politique de confidentialité de l'entreprise
- Page du site de l'entreprise relative aux paramètres du compte utilisateur

## **P8. Accès des utilisateurs à leurs propres données**

Les entreprises doivent permettre aux utilisateurs d'obtenir toutes les **données** qu'elles détiennent à leur sujet.

*Éléments :*

1. L'entreprise **indique-t-elle clairement** que les utilisateurs peuvent obtenir une copie de des **données** qu'elle possède à leur sujet ?
2. L'entreprise **indique-t-elle clairement** les informations sur les utilisateurs que ces derniers peuvent obtenir ?
3. L'entreprise **indique-t-elle clairement** que les utilisateurs peuvent obtenir les **données** qu'elle possède à leur sujet dans un format de **données structurées** ?
4. L'entreprise **indique-t-elle clairement** que les utilisateurs peuvent obtenir toutes les **informations** publiques et privées qu'elle détient à leur sujet ?
5. Pour les **écosystèmes mobiles** : L'entreprise **indique-t-elle clairement** qu'elle évalue si les politiques de confidentialité des **applications** tierces disponibles dans son **app store** indiquent que les utilisateurs peuvent obtenir toutes les **informations** détenues par l'application les concernant ?

**Détails de l'indicateur:** Les utilisateurs doivent être en mesure d'obtenir toutes les informations que les entreprises détiennent à leur sujet. Nous attendons des entreprises qu'elles indiquent clairement les options dont disposent les utilisateurs pour obtenir ces informations, les données contenues dans leurs journaux et les formats dans lesquels ils peuvent les obtenir. Pour les écosystèmes mobiles, nous attendons des entreprises qu'elles indiquent aux utilisateurs si les applications disponibles dans leur boutique d'applications spécifient que les utilisateurs peuvent obtenir toutes les informations que l'application détient à leur sujet.

**Sources possibles :**

- Politique de confidentialité de l'entreprise
- Page du site de l'entreprise relative aux paramètres du compte utilisateur
- Centre d'aide de l'entreprise
- Articles de blog de l'entreprise

## **P9. Collecte de données utilisateurs par des tiers (entreprises de l'écosystème Internet et mobile)**

L'entreprise doit **indiquer clairement** ses pratiques relatives aux **informations sur les utilisateurs** qu'elle recueille par des **moyens techniques** à partir de sites Internet ou d'applications tierces.

*Éléments :*

1. L'entreprise **indique-t-elle clairement** quelles **informations sur les utilisateurs** elle recueille par des moyens techniques sur des sites tiers ?
2. L'entreprise **explique-t-elle clairement** comment elle recueille les **informations sur les utilisateurs** auprès de tiers par des moyens techniques ?
3. L'entreprise **indique-t-elle clairement** les raisons pour lesquelles elle recueille par des moyens techniques **des informations sur les utilisateurs** auprès de tiers ?
4. L'entreprise **indique-t-elle clairement** le temps pendant lequel elle conserve les **informations sur les utilisateurs** qu'elle collecte par des moyens techniques auprès de tiers ?
5. L'entreprise **indique-t-elle clairement** qu'elle respecte les **signaux générés par les utilisateurs** (option de retrait) pour refuser la collecte des données ?

**Détails de l'indicateur:** Nous attendons des entreprises qu'elles indiquent clairement quelles informations elles collectent sur les utilisateurs auprès de tiers. Il s'agit généralement d'informations recueillies par des applications ou des sites web tiers par des moyens techniques tels que des cookies, des extensions ou des widgets. Les informations relatives à de telles pratiques aident les utilisateurs à comprendre si les entreprises suivent leurs activités et dans quelle mesure, même hors du site web de l'entreprise hôte ou lorsqu'ils utilisent une plateforme ou un service particulier.

**Sources possibles :**

- Politique de confidentialité de l'entreprise
- Politique de l'entreprise à l'égard des tiers

## **P10. Procédure de réponse à des demandes d'information sur les utilisateurs émanant de tiers**

L'entreprise doit **indiquer clairement** sa procédure de réponse aux **demandes de données utilisateurs** émanant de **gouvernements** ou d'autres **tiers**.

*Éléments :*

1. L'entreprise **indique-t-elle clairement** sa procédure de réponse aux **demandes non judiciaires** provenant de **gouvernements** ?
2. L'entreprise **indique-t-elle clairement** sa procédure de réponse aux **ordonnances judiciaires** ?
3. L'entreprise **indique-t-elle clairement** sa procédure de réponse aux demandes des gouvernements étrangers ?
4. L'entreprise **indique-t-elle clairement** sa procédure de réponse aux **demandes émanant de tiers privés** ?
5. Les explications de l'entreprise **indiquent-elles clairement** la base juridique sur laquelle elle peut accéder aux **demandes émanant de gouvernements** ?
6. Les explications de l'entreprise **indiquent-t-elles clairement** la base juridique sur laquelle elle peut accéder aux **demandes de tiers** ?
7. L'entreprise **indique-t-elle clairement** qu'elle applique une diligence raisonnable lors de l'étude des **demandes émanant de gouvernements** avant de décider de la façon d'y répondre ?
8. L'entreprise **indique-t-elle clairement** qu'elle applique une diligence raisonnable lors de l'étude des **demandes privées** avant de décider de la façon d'y répondre ?
9. L'entreprise s'engage-t-elle à refuser d'accéder aux **demandes gouvernementales** inappropriées ou dont la portée est excessive ?
10. L'entreprise s'engage-t-elle à refuser d'accéder aux **demandes privées** inappropriées ou dont la portée est excessive ?
11. L'entreprise fournit-elle des directives claires ou des exemples d'implémentation de sa procédure de réponse aux **demandes gouvernementales** ?
12. L'entreprise fournit-elle des directives claires ou des exemples d'implémentation de sa procédure de réponse aux **demandes privées** ?

**Détails de l'indicateur:** Les entreprises sont de plus en plus sollicitées pour fournir des informations sur les utilisateurs. Ces demandes peuvent émaner d'organismes gouvernementaux ou de tribunaux (nationaux ou étrangers) ainsi que d'entités privées (c'est à - à-dire d'entités non gouvernementales et non judiciaires). Nous attendons des entreprises

qu'elles communiquent publiquement leurs procédures de réponse à chaque type de demande ainsi que les raisons pour lesquelles elles se conforment à ces demandes. Les entreprises doivent également s'engager publiquement à refuser d'accéder aux demandes gouvernementales et privées inappropriées ou dont la portée est excessive.

Dans certains cas, la loi peut empêcher une entreprise de divulguer les informations mentionnées dans les éléments de cet indicateur. Les chercheurs documenteront ce type de situations, mais une entreprise perdra des points si elle ne respecte pas tous les éléments. De telles situations empêchent les entreprises de se conformer aux bonnes pratiques. Nous encourageons donc les entreprises à plaider en faveur de lois qui leur permettent de respecter pleinement les droits des utilisateurs à la liberté d'expression et à la vie privée.

#### **Sources possibles :**

- Rapport sur la transparence de l'entreprise
- Directives de l'entreprise relatives à l'application du droit
- Politique de confidentialité de l'entreprise
- Articles de blog de l'entreprise

### **P11. Données relatives aux demandes de données utilisateurs émanant de tiers**

L'entreprise doit publier régulièrement des données sur les **demandes d'informations sur les utilisateurs émanant de gouvernements** ou d'autres **tiers**.

#### *Éléments :*

1. L'entreprise indique-t-elle le nombre de demandes reçues par pays ?
2. L'entreprise indique-t-elle le nombre de demandes d'informations sur les utilisateurs stockées et d'**accès aux communications en temps réel** ?
3. L'entreprise indique-t-elle le nombre de comptes concernés ?
4. L'entreprise indique-t-elle si une demande porte sur le **contenu** des communications ou des informations **non relatives au contenu**, ou sur les deux ?
5. La compagnie identifie-t-elle l'autorité légale spécifique ou le type de processus juridique par lequel les requêtes d'application de la loi et de sécurité nationale sont formulées ?
6. L'entreprise inclut-elle les demandes reçues par **ordonnances judiciaires** ?
7. L'entreprise indique-t-elle le nombre de demandes reçues par des tiers privés ?
8. L'entreprise indique-t-elle le nombre de demandes auxquelles elle a accédé, ventilé par type de demande ?

9. L'entreprise indique-t-elle les types de demandes gouvernementales dont la divulgation lui est interdite par la loi ?
10. L'entreprise communique-t-elle ces données au moins une fois par an ?
11. Les données communiquées par l'entreprise peuvent-elles être exportées sous la forme d'un fichier de **données structurées** ?

**Détails de l'indicateur:** Les entreprises reçoivent fréquemment des demandes de tiers qui souhaitent obtenir des informations sur les utilisateurs. Ces demandes peuvent émaner d'organismes publics ou de tribunaux (nationaux ou étrangers) ainsi que d'entités privées (c'est à dire d'entités non gouvernementales et non judiciaires). Nous attendons des entreprises qu'elles publient régulièrement des données sur le nombre et le type de demandes reçues et le nombre de demandes auxquelles elles ont accédé. Les entreprises devraient divulguer les données relatives aux demandes qu'elles reçoivent par pays, y compris de leur gouvernement et de gouvernements étrangers, ainsi que d'agences de polices, de tribunaux et de procédures privées. Nous attendons également des entreprises qu'elles indiquent le nombre de comptes concernés par ces demandes et qu'elles décrivent par catégorie les demandes auxquelles elles ont accédé. Nous reconnaissons que les entreprises ne sont parfois pas autorisées à divulguer les demandes d'informations sur les utilisateurs émanant de gouvernements. Cependant, dans ces cas, nous attendons des entreprises qu'elles indiquent les types de demandes gouvernementales qu'elles ne sont pas autorisées à divulguer en vertu de la loi. Les entreprises doivent déclarer ces données une fois par an et s'assurer qu'elles peuvent être exportées dans des fichiers de données structurées.

Dans certains cas, la loi peut empêcher une entreprise de divulguer les informations mentionnées dans cet indicateur. Par exemple, nous attendons des entreprises qu'elles publient des chiffres exacts plutôt que des fourchettes. Nous reconnaissons que les lois empêchent parfois les entreprises de procéder ainsi. Les chercheurs documenteront donc les situations le cas échéant, mais une entreprise perdra néanmoins des points si elle ne respecte pas l'ensemble des critères spécifiés dans les éléments ci-dessus. De telles situations empêchent les entreprises de se conformer aux bonnes pratiques. Nous les encourageons à plaider en faveur de lois qui leur permettent de respecter pleinement les droits des utilisateurs à la liberté d'expression et à la vie privée.

**Sources possibles :**

- Rapport sur la transparence de l'entreprise

## **P12. Notification des utilisateurs à propos des demandes de données à leur sujet provenant de tiers**

Dans la mesure où cela est juridiquement possible, l'entreprise devrait **aviser** les utilisateurs, lorsque leurs **données personnelles** sont **réclamées par des gouvernements** ou d'autres tierces parties.

*Éléments :*

1. L'entreprise **indique-t-elle clairement** qu'elle informe les utilisateurs lorsque des **entités gouvernementales (y compris les tribunaux et autres organismes judiciaires)** réclament des **informations à leur sujet** ?
2. L'entreprise **indique-t-elle clairement** qu'elle informe les utilisateurs lorsque des entités privées lui réclament des **informations à leur sujet** ?
3. L'entreprise **indique-t-elle clairement** les situations où elle pourrait ne pas **aviser** les utilisateurs, y compris une description des types de **requêtes gouvernementales** qui lui est interdit par la loi de divulguer aux utilisateurs ?

**Détails de l'indicateur:** Nous attendons des entreprises qu'elles communiquent clairement leur engagement à aviser les utilisateurs lorsque des gouvernements et des entités privées demandent des données sur les utilisateurs. Nous reconnaissons que cette informations ne peut pas être communiquée dans des cas légitimes d'une enquête en cours. Toutefois nous attendons des entreprises qu'elles précisent le type de demandes gouvernementales dont la divulgation leur est interdite par la loi.

**Sources possibles :**

- Rapport sur la transparence de l'entreprise
- Lignes directrices de l'entreprise relatives à l'application du droit

### **P13. Contrôle de la sécurité**

L'entreprise doit **indiquer clairement** les informations sur ses processus institutionnels mis en place pour assurer la sécurité de ses produits et services.

*Éléments :*

1. L'entreprise **indique-t-elle clairement** qu'elle a mis en place des processus pour limiter et contrôler l'accès de ses employés aux renseignements sur les utilisateurs ?
2. L'entreprise **indique-t-elle clairement** qu'elle dispose d'une équipe de sécurité qui effectue des audits de sécurité sur ses produits et services ?
3. L'entreprise **indique-t-elle clairement** qu'elle commande des audits de sécurité auprès de tiers pour ses produits et services ?

**Détails de l'indicateur:** Au vu des immenses quantités d'informations sur les utilisateurs qu'elles gèrent et conservent, les entreprises doivent mettre en place des mesures de sécurité claires pour s'assurer que ces informations sont en sécurité. Nous attendons des entreprises qu'elles indiquent clairement disposer de systèmes pour limiter et surveiller l'accès des employés aux renseignements sur les utilisateurs. Nous attendons aussi des entreprises

qu'elles indiquent clairement déployer des équipes de sécurité interne et externe pour mener des audits de sécurité sur leurs produits et services.

**Sources possibles :**

- Politiques de confidentialité de l'entreprise
- Guide de sécurité de l'entreprise

## **P14. Mesures relatives aux failles de sécurité**

L'entreprise doit répondre aux **failles de sécurité** lorsqu'elle en découvre.

*Éléments :*

1. L'entreprise **indique-t-elle clairement** qu'elle dispose de mécanismes par lesquels les **chercheurs en sécurité** peuvent signaler les **failles** de sécurité qu'ils découvrent ?
2. L'entreprise **indique-t-elle clairement** le délai dans lequel elle examine les rapports de **failles de sécurité** ?
3. L'entreprise indique-t-elle clairement qu'elle s'engage à ne pas intenter d'action en justice contre les chercheurs qui signalent des **failles de sécurité** dans le cadre du mécanisme de signalement de l'entreprise ?
4. Pour les écosystèmes mobiles : L'entreprise **indique-t-elle clairement** que les **mises à jour logicielles**, les **correctifs de sécurité**, les **modules** ou les extensions sont téléchargés au moyen d'un canal **chiffré** ?
5. Pour les écosystèmes mobiles et les entreprises de télécommunications : L'entreprise **indique-t-elle clairement**, le cas échéant, quelles **modifications ont été apportées à un système d'exploitation mobile** ?
6. Pour les écosystèmes mobiles et les entreprises de télécommunications : L'entreprise **indique-t-elle clairement**, le cas échéant, les conséquences de telles modifications sur sa capacité à envoyer des **mises à jour de sécurité** aux utilisateurs ?
7. Pour les écosystèmes mobiles : L'entreprise **indique-t-elle clairement** la date jusqu'à laquelle elle continue de fournir des **mises à jour de sécurité** pour un **appareil ou un système d'exploitation** ?
8. Pour les écosystèmes mobiles : L'entreprise s'engage-t-elle à fournir des **mises à jour de sécurité** pour le système d'exploitation et d'autres logiciels critiques pendant au moins cinq ans après leur sortie ?
9. Pour les écosystèmes mobiles et les entreprises de télécommunications : Si l'entreprise utilise un système d'exploitation adapté d'un autre système, s'engage-t-elle à fournir des

**correctifs de sécurité** dans le mois suivant l'annonce d'une **faille de sécurité** au public ?

**Détails de l'indicateur:** Le code informatique n'est pas parfait. Lorsque les entreprises sont informées de failles de sécurité qui peuvent mettre en danger leurs utilisateurs et leurs données, elles doivent prendre des mesures pour atténuer ces préoccupations. Il s'agit notamment de s'assurer que les personnes sont en mesure de signaler les failles qu'elles découvrent avec l'entreprise. Nous pensons qu'il est particulièrement important pour les entreprises de fournir aux utilisateurs des informations claires sur la façon dont ils recevront les mises à jour de sécurité et le délai dans lequel ils les recevront. De plus, puisque les fournisseurs de services de télécommunications peuvent modifier les systèmes d'exploitation mobiles libres, nous attendons de ces entreprises qu'elles communiquent les informations qui pourraient affecter la capacité des utilisateurs à accéder à ces mises à jour essentielles.

**Sources possibles :**

- Politiques de confidentialité de l'entreprise
- Guide de sécurité de l'entreprise
- Forums d'aide de l'entreprise

## **P15. Atteintes à la protection des données**

L'entreprise doit communiquer publiquement les informations sur ses dispositifs de réponse aux **atteintes à la protection des données** (fuite de données).

*Éléments :*

1. L'entreprise **indique-t-elle clairement** qu'elle informe les autorités compétentes sans délai indu lorsqu'une **atteinte à la protection des données** se produit ?
2. L'entreprise **indique-t-elle clairement** son processus d'information des personnes susceptibles d'être concernées par une **atteinte à la protection des données** ?
3. L'entreprise **indique-t-elle clairement** les types de mesures qu'elle prend pour remédier aux conséquences d'une **atteinte à la protection des données** sur ses utilisateurs ?

**Détails de l'indicateur:** Les entreprises doivent mettre en place des mécanismes pour traiter les atteintes à la protection des données, y compris des politiques claires pour informer les utilisateurs affectés, et les communiquer clairement. En plus de dévoiler des informations personnelles, les atteintes à la protection des données peuvent constituer des menaces importantes pour la sécurité financière et personnelle des individus. Les entreprises doivent par conséquent rendre ces mécanismes accessibles au public. Ainsi, les utilisateurs peuvent prendre des décisions éclairées et tenir compte des risques potentiels avant de souscrire à un service ou de communiquer des données personnelle à une entreprise.



Nous attendons des entreprises qu'elles disposent de politiques officielles relatives à la gestion des atteintes à la protection des données et qu'elles les rendent publiques avant même qu'une telle atteinte ne survienne.

**Sources possibles :**

- Conditions générales ou politique de confidentialité de l'entreprise
- Guide de sécurité de l'entreprise

## **P16. Chiffrement des communications des utilisateur et du contenu privé (entreprises de l'écosystème mobile et d'Internet)**

L'entreprise doit **chiffrer** les communications des utilisateurs et leurs **contenus** privés afin qu'ils puissent contrôler qui y a accès.

*Éléments :*

1. L'entreprise **indique-t-elle clairement** que la transmission des communications des utilisateurs est **chiffrée** par défaut ?
2. L'entreprise **indique-t-elle clairement** que les transmissions des communications des utilisateurs sont **chiffrées** à l'aide de clés uniques ?
3. L'entreprise **indique-t-elle clairement** que les utilisateurs peuvent sécuriser leur contenus privés à l'aide d'un **chiffrement de bout en bout** ou d'un **chiffrement complet du disque** (lorsque c'est possible) ?
4. L'entreprise **indique-t-elle clairement** que le **chiffrement de bout en bout** ou le **chiffrement complet du disque** est activé par défaut ?

**Détails de l'indicateur:** Le chiffrement est un outil important pour protéger la liberté d'expression et la vie privée. Le [rapporteur spécial des Nations Unies sur la liberté d'expression](#) a déclaré sans équivoque que le chiffrement et l'anonymat sont essentiels à l'exercice et à la protection des droits de l'homme. Nous attendons des entreprises qu'elles indiquent clairement que les communications des utilisateurs sont chiffrées par défaut, que les transmissions sont protégées par la confidentialité persistante parfaite (*perfect forward secrecy*), que les utilisateurs ont la possibilité d'activer le chiffrement de bout en bout et qu'elles proposent un chiffrement de bout en bout par défaut. Pour les écosystèmes mobiles, nous attendons des entreprises qu'elles indiquent clairement que le chiffrement complet du disque est activé.

**Sources possibles :**

- Conditions d'utilisation ou politique de confidentialité de l'entreprise
- Guide de sécurité de l'entreprise
- Centre d'aide de l'entreprise
- Rapports sur le développement durable de l'entreprise
- Blog officiel de l'entreprise et/ou communiqués de presse

## P17. Sécurité des comptes (entreprises de l'écosystème mobile et d'Internet)

L'entreprise doit aider les utilisateurs à sécuriser leurs **comptes**.

*Éléments :*

1. L'entreprise **indique-t-elle clairement** qu'elle déploie des méthodes d'authentification avancées pour prévenir les accès frauduleux ?
2. L'entreprise **indique-t-elle clairement** que les utilisateurs peuvent consulter les activités récentes de leur compte ?
3. L'entreprise **indique-t-elle clairement** qu'elle avise les utilisateurs en cas de suspicion d'une activité inhabituelle sur leur compte ou d'un accès non autorisé à celui-ci ?

**Détails de l'indicateur:** Les entreprises doivent aider les utilisateurs à sécuriser leurs comptes. Elles doivent indiquer clairement qu'elles utilisent des techniques d'authentification avancées pour empêcher l'accès non autorisé aux comptes et aux informations des utilisateurs. Nous attendons également des entreprises qu'elles fournissent aux utilisateurs des outils qui leur permettent de sécuriser leurs comptes et de savoir quand leurs comptes peuvent être piratés.

**Sources possibles :**

- Centre de sécurité de l'entreprise
- Pages d'aide de l'entreprise ou pages de support communautaire
- Page de l'entreprise relative aux paramètres des comptes
- Blog de l'entreprise

## P18. Information et formation des utilisateurs sur les risques potentiels

L'entreprise doit publier des informations pour aider les utilisateurs à se défendre contre les **risques cybernétiques**.

1. L'entreprise publie-t-elle de la documentation pratique pour apprendre aux utilisateurs à se protéger contre les **risques cybernétiques** associés à ses produits et ses services ?

**Détails de l'indicateur:** Comme elles détiennent une immense quantité de données sur les utilisateurs, les entreprises sont souvent la cible d'acteurs malveillants. Nous attendons des entreprises qu'elles aident les utilisateurs à se protéger contre de tels risques. Elles peuvent notamment publier des documents sur la façon de configurer l'authentification avancée ou d'ajuster les paramètres de confidentialité, des conseils pour éviter les attaques au moyen de logiciels malveillants, de techniques d'hameçonnage ou d'ingénierie sociale, éviter ou répondre au harcèlement ou à l'intimidation en ligne ainsi que des explications au sujet de la « navigation sûre ». Les entreprises doivent dispenser ces conseils dans un langage clair, idéalement accompagné d'images, afin d'aider les utilisateurs à comprendre la nature des risques auxquels

les entreprises et les utilisateurs sont exposés. Les conseils peuvent se présenter sous forme d'astuces, de tutoriels, de guides pratiques ou d'autres ressources, dont la forme doit faciliter la compréhension pour les utilisateurs (par exemple grâce à des visuels, des graphiques, des listes, des listes à puces, etc.).

**Sources possibles :**

- Centre de sécurité de l'entreprise
- Page d'aide de l'entreprise ou page de support communautaire
- Blog de l'entreprise

## Glossaire

**Note :** *Il ne s'agit pas d'un glossaire général. Les définitions et explications fournies ci-dessous ont été rédigées spécifiquement pour guider les chercheurs dans l'évaluation des entreprises du secteur de la communication et de l'information selon les indicateurs de recherche de ce projet.*

**accès aux communications en temps réel :** surveillance d'une conversation ou de toute autre communication électronique en « temps réel », à savoir au moment où se déroule la communication, ou l'interception des données au moment même où elles sont transmises. Ce procédé est aussi parfois appelé « écoute téléphonique ». Il existe une différence entre une demande d'écoute téléphonique et une demande d'obtention de données stockées. L'écoute donne aux agences des forces de l'ordre le pouvoir d'accéder à des communications futures, tandis qu'une demande d'obtention de données stockées leur permet d'accéder aux dossiers des communications déjà effectuées. Le gouvernement des États-Unis peut avoir accès aux communications en temps réel conformément au Wire Tape Act et au Pen Register Act, des dispositions de l'Electronic Communications Privacy Act (loi nationale sur les communications électroniques). Le gouvernement russe peut le faire par le biais du System for Operative Investigative Activities » (SORM - système de recherche et de surveillance d'Internet).

**agent :** cadre supérieur responsable d'un ensemble explicite de risques et d'incidences, en l'occurrence la protection de la vie privée et de la liberté d'expression.

**algorithme :** ensemble d'instructions utilisées pour traiter l'information et fournir une sortie basée sur les stipulations des instructions. Les algorithmes peuvent être de simples morceaux de code, mais ils peuvent aussi être incroyablement complexes, « codant pour des milliers de variables à travers des millions de points de données ». Dans le contexte des entreprises d'Internet, de téléphonie mobile et de télécommunications, certains algorithmes, en raison de leur complexité, de la quantité et du type d'informations sur les utilisateurs qui leur sont fournies et de la fonction décisionnelle qu'ils remplissent, ont des implications importantes pour les droits fondamentaux des utilisateurs, notamment la liberté d'expression et la vie privée. Pour en savoir plus : *Algorithmic Accountability: A Primer*, Data & Society:

**app store :** plateforme sur laquelle une entreprise donne accès à ses propres applications ainsi que celles de développeurs tiers afin que les utilisateurs les téléchargent. Un app store (ou boutique d'applications) constitue une plateforme de distribution numérique de logiciels informatiques, souvent dans un contexte mobile.

**appareil / appareil portable / appareil mobile :** objet physique, tel qu'un smartphone ou un téléphone polyvalent, utilisé pour accéder aux réseaux de télécommunications et conçu pour être transporté par l'utilisateur et utilisé dans divers endroits.

**application :** programme autonome ou élément de logiciel conçu pour répondre à un besoin particulier ; une application logicielle, surtout lorsqu'elle est téléchargée par un utilisateur sur un appareil mobile.

**archive publique** : ressource accessible au public contenant les versions antérieures des politiques d'une entreprise, telles que ses conditions générales ou sa politique de confidentialité, ou expliquant en détail chaque série de modifications apportées à ces politiques par l'entreprise.

**atteinte à la protection des données** : se produit lorsqu'une partie non autorisée obtient l'accès à des renseignements sur les utilisateurs qu'une entreprise collecte, conserve ou traite et qui compromet l'intégrité, la sécurité ou la confidentialité de ces renseignements.

**avis, aviser** : communication ou information de l'entreprise à ses utilisateurs au sujet d'un élément en rapport avec l'entreprise ou un service.

**cadre supérieur** : PDG et/ou autre membre de l'équipe de direction présenté par la société sur son site Internet ou dans d'autres documents officiels tels qu'un rapport annuel. En l'absence d'une liste établie par l'entreprise de son équipe de direction, les autres postes de direction et les postes au plus haut niveau de la direction (par exemple : vice-président directeur ou vice-président principal, selon l'entreprise) sont considérés comme des cadres supérieurs.

**chercheur en sécurité** : personne qui étudie comment sécuriser les systèmes techniques et/ou les menaces à la sécurité des ordinateurs et des réseaux afin de trouver une solution.

**chiffrement** : ce procédé cache le contenu des communications ou des fichiers afin que seul le destinataire prévu puisse les voir. Le processus utilise un algorithme pour convertir le message (texte en clair) en un format codé (texte chiffré) de sorte que le message ressemble à une série aléatoire de caractères pour quiconque le visualise. Seule une personne qui possède la clé de chiffrement adéquate peut décrypter le message et repasser du texte chiffré au texte clair. Les données peuvent être chiffrées lors de leur stockage et lors de leur transmission.

Par exemple, les utilisateurs peuvent chiffrer les données sur leur disque dur afin que seul l'utilisateur en possession de la clé de chiffrement puisse déchiffrer le contenu du disque. De plus, les utilisateurs peuvent envoyer un message électronique chiffré, ce qui empêche quiconque de visualiser le contenu du message pendant sa circulation sur le réseau pour atteindre le destinataire prévu. Avec le chiffrement de données en transit (par exemple, lorsqu'un site web utilise HTTPS), la communication entre un utilisateur et un site web est cryptée, de sorte que les personnes extérieures, comme le fournisseur d'accès de l'utilisateur, ne peuvent voir que la visite d'origine du site, mais pas ce que l'utilisateur communique sur ce site, ni les sous-pages qu'il consulte. Pour en savoir plus : <https://www.explainthatstuff.com/encryption.html>

**chiffrement complet du disque** : chiffrement complet de toutes les données stockées sur un dispositif physique, de telle manière que seul l'utilisateur puisse accéder au contenu au moyen du ou des mots de passe générés par l'utilisateur et/ou d'autres moyens de déchiffrement (empreinte digitale, code d'authentification à deux facteurs, jeton physique, etc.).

**chiffrement de bout en bout** : avec le chiffrement de bout en bout, seuls l'expéditeur et le destinataire peuvent lire le contenu des communications chiffrées. Des tiers, y compris l'entreprise, ne sont pas en mesure de décoder le contenu.

**collecter, collecte** : tous moyens par lesquels une entreprise peut recueillir des informations sur les utilisateurs. Par exemple, une entreprise peut rassembler ces renseignements directement dans diverses situations, notamment lorsque les utilisateurs téléchargent du contenu à des fins de partage public, soumettent des numéros de téléphone pour vérification de compte, transmettent des renseignements personnels dans le cadre d'une conversation privée, etc. Une entreprise peut également rassembler ces informations indirectement, par exemple en enregistrant des données de journal, des informations de compte, des métadonnées et d'autres informations connexes qui décrivent les utilisateurs et/ou documentent leurs activités.

**compte / compte utilisateur** : ensemble de données associées à un utilisateur particulier d'un système informatique, d'un service ou d'une plateforme donnée. Le compte utilisateur comprend au minimum un nom d'utilisateur et un mot de passe, qui sont utilisés pour authentifier l'accès de l'utilisateur à ses données.

**conditions générales d'utilisation** : aussi appelées conditions d'utilisation, conditions générales. Comme indiqué par l'EFF, les conditions générales d'utilisation « fournissent souvent les règles de base nécessaire à l'utilisation des différents services en ligne ». Elles représentent un accord juridique entre l'entreprise et l'utilisateur. Les entreprises peuvent prendre des mesures à l'encontre des utilisateurs et de leur contenu sur la base des informations contenues dans les conditions d'utilisation. Source : Electronic Frontier Foundation, "Terms of (Ab)use" <https://www.eff.org/issues/terms-of-abuse>

**confidentialité persistante / confidentialité persistante parfaite** : méthode de chiffrement utilisée notamment dans le trafic web HTTPS et dans les applications de messagerie, dans laquelle une nouvelle paire de clés est générée pour chaque session (HTTPS) ou pour chaque message échangé entre les parties (applications de messagerie). Ainsi, si un adversaire obtient une clé de chiffrement, il n'est pas en mesure de décrypter les communications ou messages passés ou futurs. Elle se distingue du chiffrement de bout en bout, qui consiste à crypter les données « au repos » sur les serveurs distants de l'entreprise. Pour plus d'informations, consultez le document *Pushing for Perfect Forward Secrecy*, publié par Electronic Frontier Foundation : <https://www.eff.org/deeplinks/2013/08/pushing-perfect-forward-secrecy-important-web-privacy-protection>.

**conseil d'administration** : la surveillance au niveau du conseil d'administration doit impliquer des membres du conseil qui possède une vision générale directe des questions liées à la liberté d'expression et à la protection de la vie privée. Il n'est pas nécessaire qu'il s'agisse d'un comité officiel, mais la responsabilité des membres du conseil d'administration dans la supervision des pratiques de la société sur ces questions doit être clairement énoncée et communiquée sur le site web de la société.

**conservation des données utilisateurs** : Une entreprise peut collecter des données et les effacer par la suite. Si l'entreprise ne les efface pas, les données sont « conservées ». Le délai entre la collecte et la suppression est appelé « délai de conservation ». Ces données peuvent

relever de notre définition des « données utilisateurs » ou être anonymes. Gardez à l'esprit que des données réellement anonymes ne peuvent en aucun cas être liées à un utilisateur, son identité, son comportement ou ses préférences, ce qui est très rare.

Le « délai de conservation » constitue un sujet connexe. Par exemple, une entreprise peut collecter des données de journal de façon continue, mais purger (supprimer) les données une fois par semaine. Dans ce cas, le délai de conservation des données est d'une semaine. Cependant, si aucun délai de conservation n'est spécifié, l'hypothèse par défaut doit être que les données ne sont jamais supprimées et que la période de conservation est donc indéterminée. Dans de nombreux cas, les utilisateurs peuvent souhaiter que leurs données soient conservées pendant qu'ils utilisent activement le service, mais souhaiter qu'elles soient supprimées (et donc pas conservées) s'ils cessent d'utiliser le service. Par exemple, les utilisateurs peuvent vouloir qu'un service de réseau social conserve tous leurs messages privés, mais souhaiter que ceux-ci soient supprimés lorsqu'ils quittent ce service.

**contenu** : informations contenue dans les communications filaires, orales ou électroniques (par exemple : une conversation qui se déroule au téléphone ou en personne, un texte écrit et transmis par SMS ou un message électronique).

**cookie(s)** : « Les [cookies](https://ssd.eff.org/fr/glossary/t%C3%A9moins) (ou témoins) sont une technologie Web qui permet aux sites Web de reconnaître votre navigateur. Les témoins étaient à l'origine conçus pour permettre aux sites de vous offrir des paniers d'achats, d'enregistrer vos préférences ou d'assurer votre connexion à un site. Ils permettent aussi le suivi à la trace et le profilage afin que les sites puissent vous reconnaître et en apprendre davantage sur votre navigation, les appareils que vous utilisez et ce qui vous intéresse, même si vous n'avez pas de compte sur ce site et n'y êtes pas connecté. » Source : <https://ssd.eff.org/fr/glossary/t%C3%A9moins>

**correctif** : élément de logiciel conçu pour mettre à jour un programme informatique ou ses données d'appui pour le corriger ou l'améliorer. Cela inclut la correction des failles de sécurité et autres bogues et l'amélioration de l'utilisabilité ou des performances du programme, de l'application ou du système d'exploitation de l'ordinateur.

**coupure ou restriction de l'accès au réseau** : perturbation intentionnelle d'Internet ou des communications électroniques, y compris les services de télécommunications comme la téléphonie cellulaire et les SMS. Cela comprend la coupure générale de tous les services cellulaires ou Internet dans une zone géographique et le blocage ciblé de services particuliers, comme les médias sociaux ou les applications de messagerie.

**demande gouvernementale** : demande provenant de ministères ou d'organismes gouvernementaux, d'autorités de police ou d'ordonnances judiciaires dans les affaires pénales ou civiles.

**demande gouvernementale non judiciaire** : demande provenant d'entités gouvernementales qui ne soient ni organismes judiciaires, ni juges ni, tribunaux. Il peut s'agir de demandes émanant de ministères, d'organismes, de services de police, d'agents de police (agissant à titre officiel) ou d'autres services, autorités ou entités gouvernementaux non judiciaires.

**demande privée** : demande présentée dans le cadre d'un processus privé plutôt que d'un processus judiciaire ou gouvernemental. Les demandes privées de restriction d'accès peuvent émaner d'un organisme d'autorégulation comme l'Internet Watch Foundation (Fondation pour la surveillance d'Internet) ou d'un système d'avis/retrait comme le Digital Millennium Copyright Act (DMCA) aux États-Unis. Pour plus d'information sur la procédure d'avis/retrait ainsi que sur le DMCA, vous pouvez consulter le récent rapport de l'UNESCO intitulé [\*Fostering Freedom Online: The Role of Internet Intermediaries\*](#) (pages 40 à 52 sur 211).

**dépersonnalisées** : se dit de données utilisateurs qu'une entreprise collecte et conserve, seulement après en avoir retiré ou masqué toute information identifiable. Cela signifie qu'il faut supprimer les identificateurs explicites comme les noms, les adresses électroniques et tout numéro d'identification émis par un gouvernement, ainsi que les identificateurs tels que les adresses IP, les cookies et les numéros d'appareil uniques.

**déploiement** : série d'annonces de produits connexes qui s'échelonnent dans le temps ; processus de mise à disposition de correctifs, mises à jour et mises à niveau logicielles aux utilisateurs finaux.

**développeur / développeur tiers** : personne (ou groupe de personnes) qui crée un logiciel ou une application distribué sur la boutique d'applications (app store) d'une entreprise.

**direction (au niveau des équipes de direction)** : Le comité de direction ou un membre de l'équipe de direction de l'entreprise supervise directement les questions liées à la liberté d'expression et à la protection de la vie privée.

**documentation** : dossiers mis à disposition par l'entreprise que les utilisateurs peuvent consulter, tels qu'un journal des modifications apportées aux conditions générales ou aux documents de politique de confidentialité.

**donnée anonyme** : donnée qui n'est en aucune façon reliée à un autre élément d'information qui pourrait permettre d'identifier un utilisateur. Le caractère large de cette définition utilisée par le projet Ranking Digital Rights est nécessaire pour refléter plusieurs faits. Tout d'abord, les analystes compétents peuvent dés-anonymiser de larges ensembles de données. Cela rend presque toute promesse d'anonymisation impossible à tenir. En substance, les données liées à un « identifiant anonyme » ne sont pas réellement anonymes. Il s'agit plutôt de données souvent pseudonymes qui peuvent être liées à l'identité hors ligne de l'utilisateur. Deuxièmement, les métadonnées peuvent être autant voire plus révélatrices des liens et intérêts d'un utilisateur que les données de « contenu », ce qui leur confère un intérêt vital. Troisièmement, les entités qui ont accès à de nombreuses sources de données, comme les courtiers en données et les gouvernements peuvent être en mesure de coupler plusieurs sources de données pour révéler des renseignements sur les utilisateurs. Ainsi, les acteurs à la pointe peuvent utiliser des données qui semblent anonymes pour dessiner une image plus large d'un utilisateur.

**données de localisation** : informations recueillies par un réseau ou un service sur



l'emplacement du téléphone ou de tout autre appareil de l'utilisateur, par exemple la localisation d'un téléphone mobile à partir de données recueillies par des stations de base sur un réseau de téléphonie mobile ou par positionnement GPS ou Wi-Fi.

**données structurées** : « Données qui résident dans les champs désignés d'un enregistrement ou d'un fichier. Les bases de données relationnelles et les tableurs sont des exemples de données structurées. Bien que les données contenues dans les fichiers XML ne soient pas fixes comme les enregistrements de base de données traditionnels, elles sont néanmoins structurées, car elles sont étiquetées et peuvent être identifiées avec précision. » Inversement, les données non structurées sont des données qui « ne résident pas dans des champs fixes. » Le terme se réfère généralement à un texte de forme libre, ce qui est omniprésent. Exemples : documents de traitement de texte, fichiers PDF, messages électroniques, blogs, pages web et sites sociaux. »

Sources : PC Mag Encyclopedia:

« données structurées » <https://www.pcmag.com/encyclopedia/term/52162/structured-data>

« données non-structurées » <https://www.pcmag.com/encyclopedia/term/53486/unstructured-data>

**données utilisateurs** : voir informations sur l'utilisateur

**écosystème mobile** : ensemble indivisible de biens et services proposés par une entreprise d'appareils mobiles, comprenant l'appareil, le système d'exploitation, la boutique d'applications et le compte utilisateur.

**engagement politique** : déclaration publiquement disponible qui reflète la politique officielle de l'entreprise, approuvée au plus haut niveau de l'entreprise.

**équipe / programme** : unité définie au sein d'une entreprise qui a la responsabilité de la façon dont les produits ou services de l'entreprise interagissent avec, dans ce cas, la liberté d'expression et/ou la vie privée.

**études d'impact sur les droits de l'homme (EIDH)** : les EIDH constituent une approche systématique de diligence raisonnable. Une entreprise effectue ces études ou examens pour déterminer dans quelle mesure ses produits, services et pratiques commerciales affectent la liberté d'expression et la vie privée de ses utilisateurs.

Pour plus d'informations sur les EIDH et leurs bonnes pratiques, vous pouvez consulter cette page spéciale hébergée par le Business & Human Rights Resource Centre : <https://business-humanrights.org/en/un-guiding-principles/implementation-tools-examples/implementation-by-companies/type-of-step-taken/human-rights-impact-assessments>

L'institut danois des Droits de l'homme a mis au point un outil d'évaluation du respect des droits de l'homme (<https://hrca2.humanrightsbusiness.org/>) et le BSR a élaboré un guide pour réaliser

une EIDH : <https://www.bsr.org/en/our-insights/blog-view/how-to-conduct-an-effective-human-rights-impact-assessment>

Pour des orientations spécifiques au secteur des technologies de l'information et de la communication, vous pouvez consulter l'extrait du chapitre issu du livre *Business, Human Rights and the internet : A Framework for implementation* de Michael Samway sur le site Internet du projet : [http://rankingdigitalrights.org/resources/readings/samway\\_hria](http://rankingdigitalrights.org/resources/readings/samway_hria)

**exigence / exiger** : une exigence peut avoir lieu lorsqu'un utilisateur crée un compte ou plus tard, à la demande de l'entreprise.

**explicite** : L'entreprise affirme expressément son soutien à la liberté d'expression et à la protection de la vie privée.

**facilement accessible** : les conditions générales ou la politique de confidentialité sont situées à un ou deux clics de la page d'accueil de l'entreprise ou du service, ou dans un endroit logique où les utilisateurs sont susceptibles de les trouver facilement.

**facilement compréhensible** : l'entreprise a pris des mesures pour aider les utilisateurs à comprendre ses conditions générales et sa politique de confidentialité. Cela comprend, sans toutefois s'y limiter, la présence de résumés, de conseils ou d'explications sur la signification des termes, l'utilisation d'en-têtes de section, d'une taille de police lisible ou toute autre caractéristique graphique aidant les utilisateurs à comprendre le document et l'utilisation d'une syntaxe lisible.

**faille de sécurité** : faiblesse qui permet à un attaquant de réduire la protection de l'information d'un système. Une vulnérabilité correspond à l'intersection de trois éléments : une faille du système, l'accès de l'attaquant à la faille et la capacité de l'attaquant à exploiter la faille.

**fonctionnalité de base** : fonctions essentielles d'un produit ou d'un service. Par exemple, les fonctionnalités de base d'un smartphone comprennent la réception d'appels téléphoniques, de messages SMS et de courriers électroniques, le téléchargement et l'exécution d'applications et l'accès à Internet.

**géolocalisation** : identification de l'emplacement géographique réel d'un objet, tel qu'une source radar, un téléphone mobile ou un terminal informatique connecté à Internet. La géolocalisation peut se référer à la pratique d'évaluation de l'emplacement ou à l'emplacement réel évalué.

**gestion (au niveau des équipes de gestion)** : comité, programme, équipe ou dirigeant qui ne fait pas partie du conseil d'administration ou de l'équipe de direction de l'entreprise.

**hiérarchisation** : établissement de priorités effectué lorsqu'un opérateur de réseau « gère son réseau de façon à ce qu'il bénéficie à des contenus, des applications, des services ou des

dispositifs particuliers ». Aux fins de l'index, cette définition de la hiérarchisation inclut la décision d'une entreprise de bloquer l'accès à une application, un service ou un appareil particulier.

**implication / impliquer (des parties prenantes)** : interactions entre l'entreprise et les parties prenantes. Les entreprises ou les parties prenantes peuvent initier ces interactions. Elles peuvent prendre diverses formes, y compris des réunions, d'autres communications, etc.

**indiquer clairement** : action de la part d'une entreprise de présenter ou expliquer ses politiques ou ses pratiques dans des documents destinés au public d'une manière facile à trouver et à comprendre pour les utilisateurs.

**informations sur l'utilisateur** : toute donnée liée à une personne identifiable ou qui peut être liée à une telle personne en combinant des ensembles de données ou en utilisant des techniques d'extraction de données. Pour plus d'explications, les informations sur l'utilisateur correspondent à toute donnée qui documente les caractéristiques et/ou les activités de l'utilisateur. Ces informations peuvent ou non être liées à un compte utilisateur spécifique. Elles comprennent, sans s'y limiter, la correspondance personnelle, le contenu généré par l'utilisateur, les préférences et paramètres du compte, les données de connexion et d'accès, les données sur les activités d'un utilisateur ou les préférences recueillies auprès de tiers, soit par le suivi comportemental ou l'achat de données, et toute forme de métadonnées. Les informations sur les utilisateurs ne sont jamais considérées comme anonymes, sauf lorsqu'elles sont incluses uniquement comme base pour générer des mesures globales (par exemple, le nombre d'utilisateurs mensuels actifs). En effet, la déclaration « Notre service compte un million d'utilisateurs actifs par mois » contient des données anonymes, car elle ne donne pas suffisamment d'informations pour identifier ces utilisateurs.

**initiative multipartite** : une organisation multipartite crédible comprend et est dirigée par des membres d'au moins trois autres groupes de parties prenantes en plus de l'industrie : la société civile, les investisseurs, les universitaires, les représentants des utilisateurs ou des clients, la communauté technique et/ou le gouvernement. Son modèle de financement provient de plusieurs sources (sociétés, gouvernements, fondations, donations publiques, etc.). Elles présentent un niveau élevé d'indépendance, de rigueur et de professionnalisme et comptent une forte participation d'organisations de défense des droits de l'homme qui bénéficient elles-mêmes d'une solide réputation quant à leur indépendance à l'égard des sociétés et/ou des gouvernements. La Global Network Initiative est un exemple d'initiative multipartite qui porte sur la liberté d'expression et la protection de la vie privée dans le secteur des TIC.

**intelligence artificielle** : l'intelligence artificielle se distingue par un éventail d'utilisations et de significations. Dans le cas présent, l'intelligence artificielle désigne des systèmes qui ressemblent, exécutent ou imitent des fonctions qui sont généralement considérées comme nécessitant une intelligence. Nous pouvons citer en exemple, les logiciels de reconnaissance faciale et le traitement du langage naturel, dont l'utilisation par les entreprises Internet, de téléphonie mobile et de télécommunications a des répercussions sur la liberté d'expression et le droit à la vie privée. Voir : « [Privacy and Freedom of Expression in the Age of Artificial Intelligence](#) ».

**journal des modifications** : fichier qui détaille les modifications spécifiques d'un document, dans ce cas, des conditions d'utilisation ou une politique de confidentialité.

**limitation (de bande passante)** : forme brutale de régulation du trafic dans laquelle un opérateur de réseau ralentit le flux de paquets sur un réseau. Les opérateurs de téléphonie mobile peuvent limiter le trafic pour faire respecter les plafonds de données. Pour plus d'informations, consultez : Open Signal, [\*Data throttling: Why operators slow down your connection speed\*](#).

**limitation / finalité de l'utilisation** : selon le principe de limitation ou de finalité de l'utilisation, les entités qui traitent des renseignements sur les utilisateurs doivent indiquer leurs motifs et limiter l'utilisation de ces renseignements à toute autre fin, sauf si elles reçoivent le consentement de l'utilisateur. *Voir aussi le principe de minimisation des données (ci-dessous).*

**logiciel malveillant** : terme générique utilisé pour désigner diverses formes de logiciels hostiles ou intrusifs, comme les virus informatiques, les vers, les chevaux de Troie, les rançongiciels, les logiciels espions, les logiciels publicitaires, les alarmiciels et autres programmes malveillants. Il peut prendre la forme de code exécutable, de scripts, de contenu actif ou d'autres logiciels.

**minimisation des données** : selon le principe de la minimisation des données, les entreprises doivent limiter la collecte de renseignements sur les utilisateurs aux données pertinentes et nécessaires pour atteindre un objectif clairement défini. *Voir aussi : limitation d'utilisation (ci-dessus)*

**mise à jour (logicielle) critique** : correction largement diffusée d'une faille liée à la sécurité d'un produit spécifique. Ces failles sont évaluées en fonction de leur gravité : critique, importante, modérée ou faible.

**mise à jour de sécurité** : correction d'une faille liée à la sécurité d'un produit spécifique largement distribuée. Ces failles de sécurité sont évaluées en fonction de leur gravité : critique, importante, modérée ou faible.

**mise à jour logicielle** : parfois aussi appelé « correctif logiciel », il s'agit d'un téléchargement gratuit pour une application ou une suite logicielle qui corrige des fonctionnalités qui ne fonctionnent pas comme prévu ou propose des améliorations logicielles mineures et une compatibilité. Une mise à jour peut également inclure des mises à jour de pilotes qui améliorent le fonctionnement du matériel ou des périphériques, ou ajouter la prise en charge de nouveaux modèles de périphériques.

**mise à niveau logicielle** : nouvelle version d'un logiciel qui offre une amélioration ou un changement significatif par rapport à la version antérieure.

**modification apportée à un système d'exploitation mobile** : changement apporté à la version de stock d'un système d'exploitation mobile pouvant affecter la fonctionnalité de base, l'expérience utilisateur ou le processus de déploiement des mises à jour des logiciels. Par

exemple, les fonctionnalités de base d'un smartphone incluent l'envoi et la réception d'appels téléphoniques, de messages textes et de courriers électroniques, le téléchargement et l'exécution d'applications ainsi que l'accès à Internet. Cela s'applique aux smartphones Android produits par des entreprises autres que Google.

**moyens techniques** : les entreprises déploient diverses technologies, telles que les cookies, les widgets et les boutons pour suivre l'activité des utilisateurs sur leurs services et sur des sites et services tiers. Par exemple, une entreprise peut intégrer du contenu sur un site Internet tiers et collecter des renseignements lorsqu'un utilisateurs « aime » ou interagit avec ce contenu.

**« ne pas suivre »** : aussi connu sous l'acronyme « DNT » (*Do Not Track*), il s'agit d'un paramètre des préférences du navigateur d'un utilisateur qui indique aux entreprises ou aux tiers que l'utilisateur ne souhaite pas être « suivi ». En d'autres termes, chaque fois qu'un utilisateur charge un site Internet, toutes les parties impliquées dans l'affichage de la page (souvent nombreuses et principalement des publicitaires) sont invitées à ne pas collecter ou stocker d'informations sur la visite de l'utilisateur sur la page. Toutefois, il ne s'agit que d'une simple demande polie. Une entreprise peut ignorer une demande « DNT » et beaucoup le font.

**non relatif au contenu** : toute donnée sur une instance de communication ou sur un utilisateur. Les entreprises peuvent utiliser différents termes pour faire référence à ces données : métadonnées, renseignements de base sur les abonnés, données transactionnelles sans contenu, informations de compte ou renseignements sur les clients.

Aux États-Unis, le [Stored Communications Act](#) (loi sur les communications stockées) définit les communications ou dossiers clients non relatifs au contenu comme les « noms, adresses, enregistrements des connexions téléphoniques locales ou longues distances, enregistrements des heures et durées des sessions, durée du service (incluant la date de début) et types de services utilisés, numéro de téléphone, d'appareil ou tout autre numéro ou identité d'abonné (incluant toute adresse réseau temporairement assignée), ainsi que les moyens et sources de paiement pour ce service (incluant tout numéro de carte de crédit ou de compte bancaire) ». Le [Manuel de droit européen en matière de protection des données déclare](#) : « La confidentialité des communications électroniques porte non seulement sur le contenu d'une communication, mais aussi sur les données relatives au trafic (par exemple qui a communiqué avec qui, quand et pendant combien de temps) et sur les données de lieu (par exemple l'endroit depuis lequel les données ont été communiquées). »

**option de contrôle** : l'entreprise fournit à l'utilisateur un mécanisme direct et facile à comprendre pour accepter (« option d'adhésion ») ou refuser (« option de retrait ») la collecte, l'utilisation ou le partage des données. L'« option d'adhésion » signifie que la compagnie ne recueille, n'utilise, ni ne partage les données à des fins particulières jusqu'à ce que les utilisateurs l'acceptent explicitement. L'« option de retrait » signifie que par défaut l'entreprise utilise les données pour un objectif particulier, mais cessera de le faire dès que l'utilisateur demandera à l'entreprise de cesser. Il est à noter que cette définition est potentiellement controversée, car de nombreux défenseurs de la vie privée considèrent que l'option d'adhésion constitue un contrôle acceptable. Toutefois, pour cet index, nous avons choisi de considérer « l'option de retrait » comme une forme de contrôle.

**ordonnance judiciaire** : ordonnances rendues par un tribunal dans les affaires pénales et civiles.

**partage(s) / partager** : fait de permettre à un tiers d'accéder aux informations des utilisateurs, soit en les fournissant librement à un tiers (au public ou à d'autres utilisateurs), soit en les vendant à un tiers.

**parties prenantes** : personnes ayant un « intérêt » parce qu'elles sont concernées d'une façon ou d'une autre par les actions ou les décisions de l'entreprise. Notons que les parties prenantes ne sont pas les mêmes que les « détenteurs de droits » et qu'il existe différents types de parties prenantes : celles qui sont directement concernées et les « parties prenantes intermédiaires » dont le rôle est de défendre les droits des parties prenantes directes. Les titulaires de droits sont les personnes dont les droits humains pourraient être directement affectés. Ils interagissent avec l'entreprise, ses produits et ses services sur une base quotidienne, généralement en tant qu'employés, clients ou utilisateurs. « Les parties prenantes intermédiaires incluent des individus et des organisations informés et capables de parler au nom des détenteurs de droits, tels que les organisations de la société civile, les groupes d'activistes, les universitaires, les leaders d'opinion et les décideurs politiques. » (page 10 sur 28) Source : [Challenges and Solutions for ICT Companies by BSR, Sept. 2014](#)

**plateforme** : dans le sens le plus général du terme, logiciel ou objet de code pré-existant conçu pour fonctionner au sein d'un équipement en respectant les contraintes et en faisant usage de cet équipement. Ce terme peut se référer à différents niveaux d'abstraction comme une architecture informatique, un système d'exploitation ou des bibliothèques d'exécution. <sup>[1]</sup> Pour simplifier, disons qu'il s'agit de la structure sur laquelle les programmes informatiques peuvent fonctionner.

**politique de confidentialité** : documents qui décrivent les pratiques d'une entreprise en matière de collecte et d'utilisation de l'information, en particulier les informations sur les utilisateurs.

**prise de décision automatisée** : technologie qui prend des décisions sans surveillance humaine importante ou participation humaine au processus décisionnel, par exemple par l'utilisation d'une intelligence artificielle ou d'algorithmes.

**programme de lancement d'alerte** : programme qui permet aux employés de l'entreprise de signaler tout acte répréhensible présumé qu'ils constatent au sein de l'entreprise, y compris les questions liées aux droits de l'homme. Il s'agit généralement d'une ligne d'assistance téléphonique anonyme qui relève souvent d'un responsable de la conformité ou d'un responsable de l'éthique.

**protocole** : ensemble de règles gouvernant les échanges ou la transmission de données entre les appareils.

**publicité ciblée** : également appelée « publicité ciblée par centres d'intérêt » ou « publicité personnalisée », pratique consistant à diffuser des publicités personnalisées aux utilisateurs en



fonction de leur historique de navigation, de leur localisation, de leurs profils et activités sur les réseaux sociaux, de leurs caractéristiques démographiques et d'autres paramètres. La publicité ciblée repose sur de larges pratiques de collecte de données, qui peuvent impliquer le suivi des activités des utilisateurs sur Internet à l'aide de cookies, de widgets et d'autres outils de suivi afin de créer des profils détaillés des utilisateurs.

**réclamation** : RDR s'appuie sur la définition des Principes directeurs des Nations Unies :

« dénonciation de ce qui est perçu comme une injustice par un individu ou un groupe convaincu de son bon droit, qui peut se fonder sur une loi, un contrat, des promesses expresses ou tacites, une pratique coutumière ou sur ce qui est généralement considéré comme juste par les collectivités lésées. » (page 26 sur 33) Source : [Rapport du Représentant spécial du Secrétaire général chargé de la question des droits de l'homme et des sociétés transnationales et autres entreprises, John Ruggie. Principes directeurs relatifs aux entreprises et aux droits de l'homme : mise en œuvre du cadre de référence « protéger, respecter et réparer » des Nations Unies, 2011.](#)

**régulation du trafic** : ajustement du flux sur un réseau. Cela peut consister en un ralentissement conditionnel de certains types de trafic. Ce procédé peut être utilisé à des fins légitimes de gestion de réseau (par exemple, pour donner la priorité au trafic VoIP par rapport au trafic internet normal afin de faciliter les communications en temps réel) ou pour des raisons qui vont à l'encontre du principe de neutralité du réseau (par exemple : ralentir intentionnellement le trafic vidéo pour dissuader les utilisateurs de recourir aux applications à large bande).

**renseignements sur l'utilisateur** : voir **informations sur l'utilisateur**

**restriction d'accès à un compte / restreindre l'accès à un compte utilisateur** : limitation, suspension, désactivation, effacement ou suppression d'un compte utilisateur spécifique ou des permissions d'un compte utilisateur.

**risques cybernétiques** : situations dans lesquelles la sécurité, la vie privée ou d'autres droits connexes d'un utilisateur pourraient être menacés par un acteur malveillant (y compris, mais sans s'y limiter, des criminels, des initiés ou des gouvernements) susceptibles d'obtenir un accès non autorisé aux données des utilisateurs en utilisant le piratage, le hameçonnage ou d'autres techniques trompeuses.

**signaux générés par l'utilisateur** : De nombreuses entreprises permettent aux utilisateurs de refuser le suivi en définissant un ensemble de cookies spécifiques à l'entreprise. Si un utilisateur supprime des cookies afin de protéger sa vie privée, il est alors suivi jusqu'à ce qu'il redéfinisse l'option de retrait. De plus, certaines entreprises peuvent exiger qu'un utilisateur installe un module d'extension de navigateur pour empêcher le suivi. Ces deux scénarios présentent des situations où les utilisateurs sont forcés d'utiliser des signaux spécifiques à l'entreprise et qui ne comptent donc pas. Au contraire, un signal généré par l'utilisateur doit provenir de celui-ci. Il doit s'agir d'un message universel empêchant l'utilisateur d'être suivi. La principale option pour le signal généré par l'utilisateur aujourd'hui reste l'en-tête « Ne pas suivre » (voir ci-dessus), mais ce libellé laisse la porte ouverte à des moyens futurs pour les

utilisateurs de signaler qu'ils ne veulent pas être suivis.

**surveillance** : documents de gouvernance ou processus décisionnels de l'entreprise attribuant à un comité, un programme, une équipe ou un dirigeant un pouvoir de supervision officiel sur une fonction particulière. Ce groupe ou cette personne a la responsabilité de la fonction et est évalué en fonction de la mesure dans laquelle il s'acquitte de cette responsabilité.

**système d'exploitation** : logiciel supportant les fonctions de base d'un ordinateur, telles que la planification des tâches, l'exécution d'applications et le contrôle des périphériques. Un système d'exploitation mobile est un système d'exploitation pour un appareil mobile tel qu'un smartphone ou une tablette.

**tiers** : toute partie ou entité autre que l'utilisateur ou l'entreprise. Aux fins de la présente méthodologie, les tiers peuvent comprendre des organisations gouvernementales, des tribunaux ou d'autres structures privées (ex : une entreprise, une ONG, une personne physique).

**utilisateur** : individu utilisant un produit ou un service. Cela inclut les personnes qui publient ou transmettent des contenus en ligne ainsi que celles qui tentent d'accéder à ce contenu ou de le recevoir. Pour les indicateurs de la catégorie « Liberté d'expression », cela inclut les développeurs tiers qui créent des applications hébergées ou distribuées par le biais des produits ou services d'une entreprise.

**voies de recours / recours** : « Parmi [les] voies de recours peuvent figurer des excuses, une restitution, un redressement, des indemnités financières ou autres et des sanctions (soit pénales, soit administratives, sous forme d'amendes par exemple) ainsi que la prévention des pratiques abusives au moyen notamment d'injonctions ou de garanties de non-répétition. Les procédures de mise en œuvre des voies de recours devraient être impartiales, à l'abri de la corruption et des tentatives politiques ou autres d'influer sur l'issue du recours. » (page 26 sur 33)

Source : [Rapport du Représentant spécial du Secrétaire général chargé de la question des droits de l'homme et des sociétés transnationales et autres entreprises, John Ruggie. Principes directeurs relatifs aux entreprises et aux droits de l'homme: Mise en œuvre du](#), 2011

**widget** : code permettant à un utilisateur ou à une entreprise d'intégrer des applications et du contenu d'un site Internet ou d'un service sur un autre site ou service tiers. Dans certains cas, les entreprises utilisent des widgets sur un site Internet tiers et recueillent des informations sur les visiteurs de ce site à leur insu.