RANKING DIGITAL RIGHTS

Index de responsabilité des entreprises 2020

Indicateurs de recherche

Guide des indicateurs et glossaire inclus

Juin 2020

Remerciements

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

- Amy Brouillette, directrice de recherche
- Veszna Wessenauer, responsable de recherche
- Nathalie Maréchal, analyste principale en matière de politiques
- Afef Abrougui, analyste de recherche
- Zak Rogoff, analyste de recherche
- Jan Rydzak, responsable de l'engagement des entreprises et analyste de recherche
- Jie Zhang, analyste de recherche.

Pour consulter la liste complète des membres de l'équipe, référez-vous au site https://rankingdigitalrights.org/who/

RDR souhaite remercier les participants (plus de 100 parties prenantes) qui ont fourni des retours essentiels tout au long de ce processus d'élaboration de la méthodologie. Nous souhaitons également remercier les anciens membres de l'équipe de recherche du RDR, Laura Reed et Andrea Hackl, pour leurs contributions clefs durant la phase initiale de notre travail d'expansion de la méthodologie, entamée début 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 la Fondation 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.

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

1. À propos de Ranking Digital Rights

Ranking Digital Rights vise à promouvoir la liberté d'expression et la protection de la vie privée sur Internet en créant des normes internationales et en incitant les entreprises à respecter et à protéger les droits de leurs utilisateurs. Pour ce faire, nous produisons l'Index de responsabilité des entreprises, qui évalue les plateformes numériques et les entreprises de télécommunications les plus puissantes au monde en fonction de leurs engagements et de leurs politiques, sur la base des normes internationales en matière de droits humains. Nous collaborons avec des entreprises ainsi qu'avec des défenseurs des droits, des chercheurs, des investisseurs et des décideurs politiques pour établir et faire progresser les normes internationales en matière de responsabilité des entreprises.

L'Index de responsabilité des entreprises de Ranking Digital Rights (RDR) offre aux entreprises une feuille de route pour construire et opérer des plateformes Internet et des services qui respectent et protègent les droits de l'homme. L'Index 2019 classait 24 entreprises selon 35 indicateurs[1] selon un processus de recherche rigoureux en sept étapes et une méthodologie ouverte s'intéressant aux mécanismes de gouvernance des entreprises pour identifier et prévenir les menaces potentielles pour les droits des utilisateurs, ainsi que les politiques publiées par les entreprises qui affectent la liberté d'expression et la vie privée des utilisateurs.

2. Méthodologie de l'Index

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 humains, 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 affirmant qu'à l'instar des gouvernements qui doivent protéger les droits de l'homme, les entreprises portent elles 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 quand elles reçoivent de la part des gouvernements des demandes de restriction d'accès à des contenus ou qu'ils sollicitent des informations sur les utilisateurs. L'Index s'appuie en outre sur un ensemble de règles et de normes émergentes au niveau mondial en matière de protection des données, de sécurité et d'accès à l'information.

La méthodologie de l'Index publié par RDR a été élaborée suite à plusieurs années d'études, de mise à l'essai et de consultations. Depuis sa création, RDR collabore étroitement avec des chercheurs du monde entier. Pour l'élaboration de la première méthodologie, de l'étude pilote et de l'Index inaugural, nous avions également travaillé avec Sustainalytics, acteur réputé auprès des investisseurs en matière de recherche dans le domaine de la performance ESG (pratiques environnementales, sociales ou de gouvernance).

Précédentes révisions de l'Index RDR :

[1] Index RDR 2019, mai 2019, https://rankingdigitalrights.org/index2019/.

- En 2015, RDR lançait son premier Index qui classait 16 entreprises de l'Internet et des télécommunications selon 31 indicateurs.

- Pour l'Index 2017, RDR a étendu son classement à 22 entreprises incluant toutes celles évaluées en 2015 et 6 supplémentaires. L'Index s'est étoffé pour inclure en plus des entreprises de l'Internet et des télécommunications de nouveaux types de services, notamment ceux qui développent des logiciels et des appareils que nous appelons « écosystèmes mobiles ». Par conséquent, nous avons mis à jour la méthodologie en 2017 sur la base d'un examen approfondi des données brutes de l'Index 2015 ainsi que des consultations avec des acteurs de la société civile, des milieux universitaires, des investisseurs et les entreprises directement concernées.

- L'Index 2018 a appliqué 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.

- La méthodologie de l'Index RDR 2019 a proposé la modification de deux indicateurs de la catégorie Gouvernance[2]. Ces révisions visent à introduire des normes de base pour l'identification et la limitation des risques en matière de droits de l'homme dans le cadre de l'utilisation d'algorithmes par les entreprises ainsi que des risques liés à leurs politiques et pratiques en matière de publicités ciblées. Nous avons également révisé l'indicateur G6 afin de renforcer et clarifier notre évaluation des mécanismes et des procédures de réclamation et de recours des entreprises.[3] En outre, l'Index RDR 2019 inclut deux nouvelles entreprises[4] (Deutsche Telekom et Telenor) et cinq services supplémentaires de type « *cloud* ».

3. Méthodologie de la révision de l'Index 2020

Depuis son lancement en 2015, l'Index RDR contribue à améliorer la divulgation des politiques et pratiques des entreprises dans un certain nombre de domaines, notamment les rapports de transparence, les suppressions de contenu, les restrictions de comptes, les fermetures de réseaux, le traitement et la sécurisation des données utilisateurs. Toutefois, compte-tenu des développements géopolitiques et technologiques aux conséquences évidentes sur les droits de l'homme dans les années qui ont suivi le développement de la méthodologie de l'Index RDR, il est devenu clair que cette méthodologie doit être mise à jour si l'on souhaite tenir les entreprises pleinement responsables de l'éventail des menaces potentielles en ligne pour les droits de l'homme.

En janvier 2019, RDR a entamé un processus d'élargissement et de révision de la méthodologie afin d'y inclure de nouveaux domaines d'intérêt et de nouveaux types d'entreprises[5]. Ce travail se concentre principalement sur trois domaines :

---

[2] « Index de responsabilité des entreprises 2019 – Indicateurs de recherche » (en français) septembre 2019, https://rankingdigitalrights.org/wp-content/uploads/2018/12/2019-Index-Methodology-FRENCH.pdf

[3] « Proposed revisions to the 2019 Corporate Accountability Index methodology (consultation draft), » *Ranking Digital Rights,* juillet 2018, (en anglais) https://rankingdigitalrights.org/wp-content/uploads/2018/06/2019-Index-Methodology_-Consultation-Draft.pdf

[4] Voir la liste 2019 des entreprises (en anglais): https://rankingdigitalrights.org/2019-companies/.

[5] « RDR 2019 Index Launch Slated for May; Big Plans Ahead, »*Ranking Digital Rights,* février 2019, (en anglais) https://rankingdigitalrights.org/2019/02/13/rdr-2019-index-launch-plans/

- **Améliorer la méthodologie de l'Index RDR 2019 :** Nous avons examiné la méthodologie de l'Index RDR 2019 pour identifier les principaux domaines à réviser et à améliorer.

- **Intégrer de nouveaux indicateurs sur la publicité ciblée et les algorithmes :** Depuis le début de l'année 2019, RDR a développé de nouveaux indicateurs pour établir des normes internationales de responsabilité et de transparence sur la façon dont les entreprises peuvent garantir le respect des droits humains en ligne lorsqu'elles développent et déploient ces nouvelles technologies. En octobre 2019, RDR a publié un projet d'indicateurs sur la publicité ciblée et les algorithmes, fruit de près d'une année de recherche interne et des retours de plus de 90 experts. Ces projets d'indicateurs ont ensuite été testés par l'équipe de recherche du RDR. Les résultats de cette étude pilote ont été publiés en mars 2020.

- **Intégrer de nouvelles entreprises :** Au début de l'année 2019, nous avons commencé un processus de recherche et de consultations publiques sur les moyens d'élargir l'Index RDR pour inclure Amazon et Alibaba. Ce processus jette les bases de l'intégration de deux nouveaux types de services (les plateformes de commerce électronique et les écosystèmes d'assistants numériques personnels) dans la méthodologie de l'Index RDR 2020.

En avril 2020, RDR a publié une version préliminaire de cette méthodologie de l'Index RDR 2020 intégrant le travail effectué sur ces trois domaines[6]. Nous avons ensuite ouvert un dernier cycle de consultations publiques pour solliciter les retours clés des parties prenantes, qui ont alimenté les décisions prises lors de la finalisation de la méthodologie.

Pour lire un résumé des principaux changements apportés à la méthodologie de l'Index RDR 2020, consultez : https://rankingdigitalrights.org/wp-content/uploads/2020/06/2020-methodology-revision-final-summary.pdf

Pour plus d'informations sur le processus de développement de notre méthodologie, consultez : https://rankingdigitalrights.org/methodology-development/.

[6] « 2020 Ranking Digital Rights Corporate Accountability Index Draft Indicators, » *Ranking Digital Rights,* avril 2020, (en anglais) https://rankingdigitalrights.org/wp-content/uploads/2020/04/2020-draft-methodology-red-line-version.pdf

4. Entreprises incluses dans l'Index RDR 2020

L'Index RDR 2020 évalue 26 entreprises, énumérées ci-dessous. Les chercheurs examinent les politiques et pratiques générales des sociétés mères, en plus des politiques et pratiques divulguées de certains services et/ou sociétés d'exploitation locales (selon la structure de la société).

Entreprises de plateformes numériques : L'Index RDR 2020 évalue 14 entreprises de plateformes numériques, soit les 12 entreprises de plateformes numériques évaluées précédemment et deux nouvelles entreprises (Amazon et Alibaba). Comme indiqué ci-dessus, en raison de l'élargissement de l'Index RDR 2020 pour inclure les nouveaux services offerts par Amazon et Alibaba (en particulier les plateformes de commerce électronique et les écosystèmes d'assistants numériques personnels) nous avons renommé la catégorie « Internet et écosystème mobile » en « plateformes numériques », dont le champ d'application comprend une gamme de produits et services offerts par les entreprises Internet, ainsi que les écosystèmes mobiles, les plateformes de commerce électronique et les écosystèmes d'assistants numériques personnels.

Pour chacune de ces sociétés, nous évaluons les politiques globales au niveau du groupe pour les indicateurs pertinents, ainsi que les politiques du marché national de l'entreprise. (Par exemple, nous évaluons la politique de confidentialité de Facebook applicable aux utilisateurs aux États-Unis.)

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

- **Alibaba (Chine)** : Taobao.com (plateforme de commerce en ligne) ; AliGenie (assistant personnel numérique)
- **Amazon (États-Unis)** : Amazon.com (plateforme de commerce en ligne) ; Amazon Alexa (assistant personnel numérique), Amazon Drive
- **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 (Russia)** : Vkontakte, boîte électronique Mail.ru, agent de message Mail.ru, 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
- **Yandex (Russie) :** Yandex Mail, Yandex Search, Yandex Disk (stockage de données sur le cloud)

Entreprises de télécommunications : l'Index 2020 classe les 12 entreprises de télécommunications précédemment évaluées. Aucune nouvelle entreprise de ce secteur n'a été ajoutée au cycle de recherches effectuées en 2020.

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

5. Processus de recherche

L'Index RDR est produit selon un processus de recherche en sept étapes de collecte de données, de vérifications et de relecture. Les recherches sont menées par un réseau de plus de 30 chercheurs du monde entier. Les étapes de l'Index RDR 2020 sont présentées ci-dessous :

- **Étape 1 : Première collecte des données.** À cette étape, l'équipe de recherche primaire est chargée de vérifier les résultats de l'ancien Index RDR (2019). Si les politiques de l'entreprise ont changé, ou pour les nouveaux indicateurs et éléments, l'équipe de recherche primaire est responsable de l'évaluation. Les chercheurs de l'étape 1 compareront également les politiques actuelles et celles de l'Index précédent.

- **Étape 2 : Examen secondaire.** À cette étape, une deuxième équipe de relecteurs vérifie les évaluations fournies par les chercheurs de l'équipe primaire lors de l'étape 1, y compris l'analyse comparative avec les années précédentes.

- **Étape 3 : Examen et réconciliation.** L'équipe de RDR examine les résultats des étapes 1 et 2 et résout toute divergence.

- **Étape 4 : Retours des entreprises.** À cette étape, les entreprises ont la possibilité de consulter les résultats préliminaires et d'apporter des retours à l'équipe RDR. L'équipe étudie les commentaires des entreprises afin de déterminer s'ils justifient des modifications de l'évaluation.

- **Étape 5 : Prise en compte des retours des entreprises**. L'équipe de RDR prend en compte les retours des entreprises et apporte le cas échéant les ajustements nécessaires aux évaluations.

- **Étape 6 : Examen horizontal secondaire.** L'équipe de RDR conduit une relecture horizontale, à partir des retours des entreprises recueillis à l'étape 4 et procède à une contre-vérification de ces indicateurs pour assurer une évaluation cohérente pour chaque entreprise.

- **Étape 7 : Score final.** L'équipe de RDR définit les scores finaux. Les évaluations précisent si les politiques ou les informations communiquées par les entreprises ont changé par rapport à l'évaluation de l'année précédente.

6. Évaluations et résultats

L'Index 2020 évalue les politiques de l'entreprise en vigueur entre le 25 janvier 2019 et le 14 septembre 2020. 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 négative) pour chaque critère rempli. L'évaluation comprend une estimation de l'information disponible pour tous les éléments 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 d'informations sur le site web de l'entreprise 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

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[7] et consacrés dans le Pacte international relatif aux droits civils et politiques[8], ces droits s'appliquent aussi bien en ligne que hors ligne.[9] 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[10] 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.[11]

G1. Engagement politique

L'entreprise doit publier un **engagement formel** à respecter les droits des utilisateurs en matière de liberté d'expression, de liberté d'information et de droit à la vie privée.

Éléments :

1. L'entreprise prend-elle dans ses politiques un **engagement explicite** et clairement articulé à l'égard des droits de l'homme, y compris de la liberté d'expression et du droit à l'information ?

2. L'entreprise prend-elle dans ses politiques un **engagement explicite** et clairement articulé à l'égard des droits de l'homme, y compris du droit à la vie privée ?

3. L'entreprise prend-elle dans ses politiques un **engagement explicite** et clairement articulé à l'égard des droits de l'homme dans le développement et l'utilisation de ses **systèmes algorithmiques** ?

Détails de l'indicateur : Cet indicateur cherche à déterminer si l'entreprise a pris dans ses politiques des engagements 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

[7]Déclaration universelle des droits de l'homme, https://www.un.org/fr/universal-declaration-human-rights/index.html
[8]Pacte international relatif aux droits civils et politiques, *Haut-commissariat des Nations Unies aux droits de l'homme*, https://www.ohchr.org/FR/ProfessionalInterest/Pages/CCPR.aspx
[9]Conseil des droits de l'homme, Résolution adoptée par le conseil des droits de l'homme le 27 juin 2016 - *Promotion et protection de tous les droits de l'homme, civils, politiques, économiques, sociaux et culturels, y compris le droit au développement* : https://digitallibrary.un.org/record/845728
[10]« Principes directeurs relatifs aux entreprises et aux droits de l'homme », Haut-commissariat des Nations Unies aux droits de l'homme, https://www.ohchr.org/Documents/Publications/GuidingPrinciplesBusinessHR_FR.pdf.
[11]« The GNI Principles, »' *Global Network Initiative (en anglais)*, https://globalnetworkinitiative.org/gni-principles/.

de l'homme.[12] Les entreprises doivent également annoncer un engagement formel envers le respect des droits de l'homme lorsqu'elles développent, déploient des systèmes algorithmiques de prise de décisions comme le recommande le Conseil de l'Europe dans sa Recommandation sur les impacts des systèmes algorithmiques sur les droits de l'homme (2020). Les entreprises doivent clairement indiquer ces engagements dans les documents officiels des politiques de l'entreprise ou dans toute autre communication reflétant les politiques officielles de l'entreprise.

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 ou rapport de développement durable de l'entreprise
- Politiques de l'entreprise relatives aux principes directeurs sur l'IA

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, la liberté d'information et la vie privée.

Éléments :

1. L'entreprise **indique-t-elle clairement** que son **conseil d'administration** exerce une **surveillance** formelle de l'incidence des pratiques de l'entreprise sur la liberté d'expression et la liberté d'information ?

2. L'entreprise **indique-t-elle clairement** que son **conseil d'administration** exerce une **surveillance** formelle de l'incidence des pratiques de l'entreprise sur la vie privée ?

3. L'entreprise **indique-t-elle clairement** qu'un comité, une équipe, un programme ou un agent de **l'équipe de direction** **surveille** l'incidence des pratiques de l'entreprise sur la liberté d'expression et la liberté d'information ?

4. L'entreprise **indique-t-elle clairement** qu'un comité, une équipe, un programme ou un agent de **l'équipe de direction** **surveille** l'incidence des pratiques de l'entreprise sur la vie privée ?

5. L'entreprise **indique-t-elle clairement** qu'un comité, une équipe, un programme ou un agent de **l'équipe de gestion** **surveille** l'incidence des pratiques de l'entreprise sur la liberté d'expression et la liberté d'information ?

6. L'entreprise **indique-t-elle clairement** qu'un comité, une équipe, un programme ou un agent de **l'équipe de gestion** **surveille** l'incidence des pratiques de l'entreprise sur la vie privée ?

Détails de l'indicateur : Cet indicateur cherche à déterminer si l'entreprise dispose d'une gouvernance et d'une surveillance solides en matière de liberté d'expression, de liberté

[12] « Principes directeurs relatifs aux entreprises et aux droits de l'homme », Haut-commissariat des Nations Unies aux droits de l'homme, https://www.ohchr.org/Documents/Publications/GuidingPrinciplesBusinessHR_FR.pdf.

d'information et de respect de la vie privée à tous les niveaux de ses activités. Les entreprises doivent clairement indiquer que les dirigeants (depuis le conseil d'administration jusqu'aux équipes de management) supervisent et sont responsables de leurs politiques et pratiques en matière de droits de l'homme.

Pour obtenir le total des points, les entreprises doivent indiquer clairement qu'à chaque niveau de gouvernance (conseil d'administration, direction, responsables d'équipe de gestion), la liberté d'expression, la liberté d'information 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 par rapport à ces questions. Aux échelons inférieurs, il peut s'agir d'une unité, d'un programme 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, de liberté d'information 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 d'information ?

2. L'entreprise **indique-t-elle clairement** qu'elle offre aux employés une formation sur les questions de protection de la vie privée ?

3. 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 l'information ?

4. 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 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.

Une entreprise ne peut recevoir un score maximal pour cet indicateur que si elle divulgue clairement des informations sur la formation de ses employés en matière de liberté d'expression et d'information, de respect de la vie privée, ainsi que sur l'existence de programmes de lancements d'alertes sur ces questions. Elle doit préciser si la formation des employés et les programmes de lancement d'alerte couvrent la liberté d'expression et la protection de la vie privée. Les entreprises peuvent toujours recevoir des points sur cet indicateur si leur programme d'alerte ne mentionne pas spécifiquement les plaintes liées à la liberté d'expression et à la vie privée, à condition que l'entreprise ait pris des engagements envers ces principes ailleurs et d'une manière qui indique clairement que l'entreprise prendrait en compte 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 : Audits en matière de droits de l'homme

G4(a). Analyse d'impact : Gouvernements et réglementations

Les entreprises doivent mener des audits réguliers, complets et fiables, en utilisant des **études d'impact sur les droits de l'homme (EIDH),** afin de déterminer comment les réglementations gouvernementales affectent la liberté d'expression, la liberté d'information et la vie privée et d'atténuer tout risque posé par ces impacts dans les territoires où elles exercent leurs activités.

Éléments :

1. L'entreprise **tient-elle compte** de l'incidence des lois sur la liberté d'expression, la liberté d'information dans les territoires où elle exerce ses activités ?

2. L'entreprise **tient-elle compte** de l'incidence des lois sur la protection de la vie privée dans les territoires où elle exerce ses activités ?

3. L'entreprise **évalue-t-elle** les risques pour la liberté d'expression et la liberté d'information associés à ses produits et ses services existants dans les territoires où elle exerce ses activités ?

4. L'entreprise **évalue-t-elle** régulièrement les risques liés à la protection de la vie privée associés à ses produits et ses services dans les territoires où elle exerce ses activités ?

5. L'entreprise **évalue-t-elle** les risques pour la liberté d'expression et la liberté d'information liés 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 ou pays ?

6. L'entreprise **évalue-t-elle** les risques pour 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 ou pays ?

7. L'entreprise procède-t-elle à une évaluation supplémentaire chaque fois que ses **études d'impact** 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 d'impact** et des audits dans leur prise de décision ?

9. L'entreprise procède-t-elle à ces **études d'impact** selon un calendrier régulier ?

10. Les **études d'impact** de l'entreprise sont-elles assurées par une tierce partie externe ?

11. La **tierce partie** chargée de l'étude d'impact est-elle reconnue pour ses principes et renommée en matière de droits de l'homme par une organisation fiable ?

Détails de l'indicateur : Cet indicateur examine si les entreprises procèdent à des audits réguliers, solides et responsables des risques en matière de droits de l'homme liés aux réglementations et politiques gouvernementales dans les juridictions où elles opèrent. Ces évaluations doivent faire partie des activités de diligence raisonnable, formelle et systématique de l'entreprise, qui visent à garantir que leurs décisions et pratiques ne causent pas, ne contribuent pas ou n'exacerbent pas les atteintes aux droits de l'homme. Les évaluations permettent aux entreprises d'identifier les risques potentiels pour la liberté d'expression et le droit à la vie privée des utilisateurs et de prendre des mesures pour atténuer les préjudices éventuels, s'ils sont identifiés.

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.

Sources possibles :
- Rapports RSE ou de durabilité de l'entreprise
- Politique de l'entreprise en matière de droits de l'homme
- Rapports de la Global Network Initiative

G4(b). Analyse d'impact : Processus d'application des politiques

Les entreprises doivent mener des audits réguliers, complets et fiables, en utilisant des **études d'impact sur les droits de l'homme** (EIDH), pour déterminer les impacts de ses

processus d'applications des lois sur les droits fondamentaux de ses utilisateurs (liberté d'expression, liberté d'information, droit à la vie privée et droit à la non-discrimination) et pour limiter tout risque posé par ceux-ci.

Éléments :

1. L'entreprise **évalue**-t-elle les risques liés à la liberté d'expression et d'information en lien avec l'application de ses conditions d'utilisation ?

2. L'entreprise procède-t-elle à une **étude de risques** sur l'application de ses politiques de protection de la vie privée ?

3. L'entreprise **évalue**-t-elle les risques de discrimination associés à ses processus de mise en œuvre de ses **conditions d'utilisation** ?

4. L'entreprise **évalue**-t-elle les risques de **discrimination** associés à ses processus de mise en œuvre de sa **politique de protection de la vie privée** ?

5. L'entreprise procède-t-elle à une évaluation supplémentaire chaque fois qu'une **étude de risques** de l'entreprise soulève des inquiétudes ?

6. 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 lors de leur prise de décision ?

7. L'entreprise procède-t-elle à ces **études** selon un calendrier régulier ?

8. Les **études d'impact** de l'entreprise sont-elles assurées par une **tierce partie** externe ?

9. La **tierce partie** chargée de l'étude d'impact est-elle reconnue pour ses principes et renommée en matière de droits de l'homme par une organisation fiable ?

Détails de l'indicateur : Cet indicateur examine si les entreprises indiquent si elles procèdent à des audits solides, réguliers et responsables des risques en matière de droits de l'homme concernant l'impact de leurs propres politiques sur les droits fondamentaux des utilisateurs à la liberté d'expression, à la vie privée et à la non-discrimination. Ces évaluations doivent faire partie des activités de diligence raisonnable formelles et systématiques de l'entreprise, qui visent à garantir que leurs décisions et pratiques ne causent pas, ne contribuent pas ou n'exacerbent pas les atteintes aux droits de l'homme. Les évaluations permettent aux entreprises d'identifier les risques potentiels pour la liberté d'expression et le droit à la vie privée des utilisateurs et de prendre des mesures pour atténuer les préjudices éventuels, s'ils sont identifiés.

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.

Sources possibles :
- Rapports RSE ou de durabilité de l'entreprise
- Politique de l'entreprise en matière de droits de l'homme
- Rapports de la Global Network Initiative

G4(c) Analyse d'impact : Publicité ciblée

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 politiques et pratiques en matière de **publicités ciblées** affectent les droits fondamentaux de ses utilisateurs à la liberté d'expression, la liberté d'information, la protection de la vie privée, la non-discrimination et d'atténuer tout risque posé par ces impacts.

Éléments :

1. L'entreprise **évalue**-t-elle les risques pour la liberté d'expression et la liberté d'information associés à l'application de ses politiques et pratiques **en matière de publicité ciblée** ?

2. L'entreprise **évalue**-t-elle régulièrement les risques pour la protection de la vie privée associés à l'application de ses politiques et pratiques en **matière de publicités ciblées**?

3. L'entreprise **évalue**-t-elle régulièrement les risques de discrimination associés à l'application de ses politiques et pratiques en matière de **publicité ciblée** ?

4. L'entreprise procède-t-elle à une évaluation supplémentaire chaque fois qu'une **études d'impact** de l'entreprise soulève des préoccupations ?

5. 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 d'impact** et des audits lors de leur prise de décision ?

6. L'entreprise procède-t-elle à ces **études d'impact** selon un calendrier régulier ?

7. Les **études d'impact** de l'entreprise sont-elles assurées par une **tierce partie** externe ?

8. La **tierce partie** chargée de l'étude d'impact est-elle reconnue pour ses principes pertinents et renommés en matière de droits de l'homme par une organisation fiable ?

Détails de l'indicateur : La publicité ciblée peut avoir des effets négatifs sur les droits de l'homme, en particulier sur les droits des utilisateurs à la liberté d'expression, d'information

et à l'absence de discrimination[13]. Il y a discrimination lorsque des plateformes permettent à des annonceurs tiers de montrer des publicités différentes à des utilisateurs différents sur la base d'informations divulguées et inférées, y compris l'appartenance à des catégories protégées (race, ethnicité, âge, identité et expression de genre, orientation sexuelle, santé, handicap, etc.) Il n'est pas nécessaire que la discrimination soit illégale ou immédiatement préjudiciable pour provoquer des effets néfastes à grande échelle, par exemple au niveau d'une population ou de la vie d'un individu. En considérant le fait que les publicités ciblées sont moins transparentes que d'autres formes de publicité et les importantes incitations financières pour les entreprises à déployer rapidement la technologie, ces préjudices potentiels doivent être pris en compte dans les études de risques.

Cet indicateur examine si les entreprises indiquent si elles procèdent à des audits solides, réguliers et responsables des risques en matière de droits de l'homme concernant l'impact de leurs propres politiques relatives aux publicités ciblées sur les droits fondamentaux des utilisateurs à la liberté d'expression, à la vie privée et à la non-discrimination. Ces évaluations doivent faire partie des activités de diligence raisonnable formelles et systématiques de l'entreprise, qui visent à garantir que leurs décisions et pratiques ne causent pas, ne contribuent pas ou n'exacerbent pas les atteintes aux droits de l'homme. Les évaluations permettent aux entreprises d'identifier les risques potentiels pour la liberté d'expression et le droit à la vie privée des utilisateurs et de prendre des mesures pour atténuer les préjudices éventuels, s'ils sont identifiés.

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.

Sources possibles :

- Rapports RSE ou de durabilité de l'entreprise
- Politique de l'entreprise en matière de droits de l'homme
- Rapports de la Global Network Initiative

G4(d). Analyse d'impact : Systèmes algorithmiques

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 politiques et pratiques en matière de développement et d'utilisation de **systèmes algorithmiques** affectent les droits fondamentaux de ses utilisateurs à la liberté d'expression, d'information, à la protection de la vie privée, à la non-discrimination et d'atténuer tout risque posé par ces impacts.

Éléments :

1. L'entreprise **évalue**-t-elle les risques pour la liberté d'expression et d'information associés au développement et à l'utilisation de ses **systèmes algorithmiques** ?

2. L'entreprise **évalue**-t-elle les risques pour la liberté d'expression et la liberté d'information associés au développement et à l'utilisation de ses **systèmes algorithmiques** ?

[13] « Human Rights Risk Scenarios: Targeted advertising, » *Ranking Digital Rights*, février 2019, (en anglais) https://rankingdigitalrights.org/wp-content/uploads/2019/02/Human-Rights-Risk-Scenarios-targeted-advertising.pdf.

3. L'entreprise **évalue**-t-elle régulièrement les risques de discrimination associés au développement et à l'utilisation de ses **systèmes algorithmiques**?

4. L'entreprise procède-t-elle à une évaluation supplémentaire chaque fois qu'une **étude de risques** de l'entreprise soulève des préoccupations ?

5. 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 ?

6. L'entreprise procède-t-elle à ces **études** selon un calendrier régulier ?

7. Les **études d'impact** de l'entreprise sont-elles assurées par une **tierce partie** externe ?

8. La **tierce partie** chargée de l'étude d'impact est-elle reconnue par une organisation fiable et réputée pour ses principes en matière de droits de l'homme ?

Détails de l'indicateur : Les systèmes algorithmiques peuvent porter atteinte aux droits de l'homme de diverses manières[14]. Le développement de ces systèmes peut reposer sur des informations fournies par l'utilisateur, souvent à l'insu ou sans le consentement explicite et éclairé de la personne concernée, ce qui constitue alors une violation de sa vie privée. De tels systèmes peuvent également entrainer ou contribuer à causer des préjudices en matière d'expression et d'information. Par ailleurs, l'objectif de nombreux systèmes décisionnels algorithmiques est d'automatiser la personnalisation des expériences utilisateurs sur la base d'informations collectées et inférées sur les utilisateurs, ce qui peut causer ou contribuer à une forme de discrimination. Les entreprises doivent donc procéder à des études de risques en matière de droits de l'homme sur leur développement et leur utilisation d'algorithmes, comme le recommande le Conseil de l'Europe dans sa recommandation sur les impacts des systèmes algorithmiques sur les droits de l'homme (2020).

Cet indicateur examine si les entreprises indiquent procéder à des audits solides, réguliers et responsables des risques en matière de droits de l'homme pour ce qui concerne l'impact de leurs propres politiques relatives au développement et au déploiement de systèmes algorithmiques. Ces évaluations doivent faire partie des procédure de diligence raisonnables, formelles et systématiques de l'entreprise, et viser à garantir que leurs décisions et pratiques ne causent pas, ne contribuent pas ou n'exacerbent pas les atteintes aux droits de l'homme. Les évaluations permettent aux entreprises d'identifier les risques potentiels pour la liberté d'expression et le droit à la vie privée des utilisateurs et de prendre des mesures pour atténuer les préjudices éventuels, s'ils sont identifiés.

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.

Sources possibles :

- Rapports RSE ou de durabilité de l'entreprise

[14] "Human Rights Risk Scenarios: Algorithms, machine learning and automated decision-making," *Ranking Digital Rights*, juillet 2019, (en anglais) https://rankingdigitalrights.org/wp-content/uploads/2019/07/Human-Rights-Risk-Scenarios_-algorithms-machine-learning-automated-decision-making.pdf.

- Politique de l'entreprise en matière de droits de l'homme
- Rapports de la Global Network Initiative

G4(e) Analyse d'impact : zero-rating

Si l'entreprise s'engage dans des programmes « ***zero-rating*** », elle 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 politiques et pratiques en matière de programme *zero-rating* affectent les droits fondamentaux de ses utilisateurs à la liberté d'expression, la liberté d'information, la protection de la vie privée, la non-discrimination et d'atténuer tout risque posé par ces impacts.

Éléments :

1. L'entreprise évalue-t-elle les risques pour la liberté d'expression et d'information associés à ses programmes ***zero-rating*** ?
2. L'entreprise évalue-t-elle les risques pour la vie privée associés à ses programmes ***zero-rating*** ?
3. L'entreprise évalue-t-elle régulièrement les risques de discrimination associés à ses programmes ***zero-rating*** ?
4. L'entreprise procède-t-elle à une évaluation supplémentaire chaque fois qu'une **étude de risques** de l'entreprise identifie des problèmes ?
5. 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 lors de leur prise de décisions ?
6. L'entreprise procède-t-elle à ces études selon un calendrier régulier ?
7. Les études d'impact de l'entreprise sont-elles assurées par une **tierce partie** externe ?
8. La **tierce partie** chargée de l'étude d'impact est-elle accréditée par une organisation fiable qui certifie sa pratique pertinente et réputée en matière de droits de l'homme ?

Détails de l'indicateur : Les programmes *zero-rating* sont des programmes qui peuvent être offerts à la fois par des sociétés de télécommunications et des plateformes, en partenariat avec des sociétés de télécommunications et donnent accès à certains services ou plateformes en ligne sans augmenter le coût de la consommation de données sur l'abonnement d'une personne. De nombreux fournisseurs de télécommunications, y compris les entreprises évaluées par RDR, proposent de tels programmes, soit en tant que fournisseur unique du programme, soit en partenariat avec des plateformes de médias sociaux, comme le programme « Free Basics » de Facebook. Ces types de programmes constituent une forme de hiérarchisation des réseaux qui porte atteinte aux principes de neutralité du Net et

peut déclencher toute une série d'autres préjudices aux droits de l'homme, notamment en restreignant le droit à la liberté d'expression et d'information. Le site Global Voices Advox a par exemple identifié le programme Free Basics de Facebook comme « un mécanisme de collecte lucrative de données auprès des utilisateurs » (Global Voices, 2017), ce qui soulève de sérieuses inquiétudes quant au respect de la vie privée par ce programme. Les programmes « *zero-rating* » peuvent également être discriminatoires en ce sens qu'ils donnent la priorité à certains types de données, soit en fonction du protocole utilisé (HTTP, HTTPS, VoIP, etc.), soit en fonction du contenu (c'est-à-dire en donnant la priorité à un site de réseautage social par rapport à un autre). Cette discrimination (à l'encontre de certains types de données) peut à son tour entraîner des atteintes aux droits de l'homme qui affectent les personnes en fonction de leurs caractéristiques personnelles, notamment leur sexe, leur race ou leur appartenance ethnique, leur(s) langue(s) parlée(s) et une multitude d'autres particularités.

Cet indicateur examine si les entreprises indiquent si elles procèdent à des audits solides, réguliers et responsables des risques en matière de droits de l'homme concernant l'impact de leurs programmes *zero-rating*. Ces évaluations doivent faire partie des activités de diligence raisonnable formelles et systématiques de l'entreprise, qui visent à garantir que leurs décisions et pratiques ne causent pas, ne contribuent pas ou n'exacerbent pas les atteintes aux droits de l'homme. Les évaluations permettent aux entreprises d'identifier les risques potentiels pour la liberté d'expression et le droit à la vie privée des utilisateurs et de prendre des mesures pour atténuer les préjudices éventuels, s'ils sont identifiés.

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.

Sources possibles :

- Rapports RSE ou de durabilité de l'entreprise
- Politique de l'entreprise en matière de droits de l'homme
- Rapports de la Global Network

G5. Implication et responsabilité des parties prenantes

L'entreprise doit **s'engager** auprès de diverses **parties prenantes** sur son impact sur la liberté d'expression et d'information, la vie privée et les risques potentiels d'atteinte aux droits de l'homme tels que la **discrimination**.

Éléments :

1. L'entreprise est-elle membre d'une ou plusieurs **initiatives multipartites** qui traitent de l'ensemble des façons dont les droits fondamentaux des utilisateurs à la liberté d'expression et d'information, à la vie privée et à la non-discrimination peuvent être affectés dans le cadre de ses activités ?

2. Si l'entreprise n'est pas membre d'au moins une de ces **initiatives multipartites**, est-elle membre d'une organisation qui s'engage systématiquement et régulièrement avec des parties prenantes non gouvernementales (et qui ne sont liées à ce secteur d'activité) sur les questions de liberté d'expression et de respect de la vie privée ?

3. Si l'entreprise n'est pas membre d'une telle organisation, indique-t-elle qu'elle organise ou participe à des réunions avec des **parties prenantes** qui représentent, défendent, ou sont des individus dont les droits à la liberté d'expression et d'information, 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 s'engage auprès d'elles, 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 avec des parties prenantes soit une composante centrale du processus d'élaboration des politiques et des études d'impact d'une entreprise. L'implication des parties prenantes doit porter sur l'ensemble des questions liées à la liberté d'expression, à la liberté d'information, à la protection de la vie privée des utilisateurs ainsi que les droits associés, y compris le processus d'élaboration des conditions générales, des politiques relatives à l'identité et à la vie privée d'une entreprise ainsi que l'application de ces politiques. Pour recevoir l'intégralité des points pour cet indicateur, les entreprises doivent s'engager non seulement auprès des parties prenantes, mais aussi dans des processus de responsabilisation tels que des audits indépendants supervisés par un organisme dont les décisions finales ne sont pas contrôlées par les seules entreprises.

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 soit réticente à 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 encouragions les entreprises à fournir les détails non sensibles sur ces collaborations, nous cherchons néanmoins 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 et qu'ils produisent de réels résultats est son implication dans une initiative multipartite. Son but ne doit pas simplement être de créer un espace sécurisé et propice à l'engagement mais aussi de permettre aux entreprises de prendre ces engagements, de les soutenir pour les respecter et de les tenir responsables. Des mécanismes de responsabilité complets et fiables nécessitent une gouvernance multipartite, dans laquelle les entreprises ne contrôlent pas seules la prise de décision en matière de processus et d'engagements de responsabilité, mais partagent plutôt le pouvoir de décision avec les représentants des autres parties prenantes.

Si une société se voit décerner tous les points pour l'élément 1, elle recevra automatiquement tous les points pour les éléments 2 et 3. Compte tenu du périmètre des travaux de la Global Network Initiative (limité aux demandes gouvernementales), et qu'au moins la moitié de la méthodologie du RDR traite des menaces pour les droits de l'homme qui ne proviennent pas des gouvernements, il conviendra de noter que l'appartenance à la GNI n'entraînera qu'un crédit partiel pour l'élément 1 de cet indicateur sans une preuve d'engagement et de responsabilité concernant d'autres risques pour les droits de l'homme que ceux posés par les gouvernements.

Sources possibles :

- Rapport RSE/de durabilité de l'entreprise
- Rapport annuel de l'entreprise
- Blog de l'entreprise
- FAQ ou centre d'aide de l'entreprise

G6. Voies de recours et appels

G6(a). 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 **indique-t-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 leur liberté d'information ?

2. L'entreprise **indique-t-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 vie privée ?

3. L'entreprise **présente-t-elle clairement** ses procédures de **recours** pour les **réclamations** relatives à la liberté d'expression et à la liberté d'information ?

4. L'entreprise **présente-t-elle clairement** ses procédures de **recours** pour les réclamations relatives à la protection de la vie privée ?

5. L'entreprise **indique-t-elle clairement** les délais de traitement des **réclamations** et des **recours** ?

6. L'entreprise **indique-t-elle clairement** le nombre de plaintes reçues relatives à la liberté d'expression ?

7. L'entreprise **indique-t-elle clairement** le nombre de plaintes reçues relatives à la protection de la vie privée ?

8. L'entreprise **présente-t-elle clairement** ses procédures de **recours** pour les **réclamations** relatives à la liberté d'expression ?

9. L'entreprise **présente-t-elle clairement** ses procédures de **recours** pour les **réclamations** relatives à la protection de la vie privée ?

Détails de l'indicateur : Les droits de l'homme ne peuvent être protégés et respectés que si les personnes disposent d'un recours lorsqu'elles 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 soient 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 traitement 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. [15]

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/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)
- Politiques de l'entreprise en matière de publicité

G6(b). Procédures de recours en matière de modération du contenu

Les mécanismes et procédures d'**appel** pour les **actions de modération de contenu** proposés par l'entreprise doivent être clairs et stables.

Éléments :

1. L'entreprise **indique-t-elle clairement** qu'elle propose aux utilisateurs concernés la possibilité de faire appel des mesures de modération du contenu ?

2. L'entreprise **indique-t-elle clairement** qu'elle informe les utilisateurs concernés par une action de modération de contenu ?

3. L'entreprise **indique-t-elle clairement** le délai dans lequel elle avise les utilisateurs concernés par une action de modération de contenu ?

4. L'entreprise **indique-t-elle clairement** les cas où les **recours** ne sont pas autorisés ?

5. L'entreprise **indique-t-elle clairement** ses procédures de traitement des **recours** ?

6. L'entreprise **indique-t-elle clairement** les délais de traitement des **recours** ?

7. L'entreprise **indique-t-elle clairement** que ces appels sont examinés par au moins une personne n'ayant pas participé à **l'action initiale de modération du contenu** ?

8. L'entreprise **indique-t-elle clairement** le rôle joué par l'automatisation dans l'examen des **recours** ?

[15] « Principes directeurs relatifs aux entreprises et aux droits de l'homme », Haut-commissariat des Nations Unies aux droits de l'homme, *2011,* https://www.ohchr.org/Documents/Publications/GuidingPrinciplesBusinessHR_FR.pdf.

9. L'entreprise **indique-t-elle clairement** que les **utilisateurs concernés** ont la possibilité de présenter des informations supplémentaires qui seront prises en compte lors de l'examen du recours ?

10. L'entreprise **indique-t-elle clairement** qu'elle fournit aux **utilisateurs concernés** une déclaration exposant les raisons de sa décision ?

11. L'entreprise fournit-elle des preuves qu'elle traite les **recours** suite à des modérations de contenu ?

Détails de l'indicateur : Quelle que soit la minutie avec laquelle une plateforme élabore ses conditions de service, les erreurs sont inévitables. La modération de contenu est un exercice exigeant et subjectif. C'est particulièrement vrai lorsque la modération de contenu est rapidement déployée à grande échelle grâce à l'automatisation. Pour respecter la liberté d'expression et les droits à l'information des utilisateurs, les entreprises doivent fournir un système de recours solide et transparent qui permet aux utilisateurs de faire appel des décisions prises par l'entreprise qui influencent directement la capacité des utilisateurs à exercer ces droits. Les entreprises doivent donc clairement indiquer leur procédure de recours suite à des actions de modération de contenu, notamment en permettant aux utilisateurs concernés de faire immédiatement appel de cette action. Une procédure d'appel solide doit inclure la supervision d'un examinateur humain et donner aux utilisateurs concernés la possibilité de présenter des informations supplémentaires. Les entreprises doivent également proposer un délai précis pour l'examen des appels et indiquer clairement les circonstances dans lesquelles les appels ne sont pas possibles.

Pour recevoir l'intégralité des points, les entreprises doivent informer les utilisateurs sur la manière de soumettre un appel et décrire le processus de traitement de cet appel. Il s'agit notamment d'informer les utilisateurs de la possibilité de déposer un recours dès que l'entreprise prend une première mesure sur leur contenu, de clarifier le rôle des modérateurs automatisés et des modérateurs humains dans la procédure de recours, d'indiquer clairement la raison d'une décision en appel, d'indiquer clairement les délais impliqués, et de préciser les circonstances dans lesquelles la procédure de recours n'est pas disponible. Les entreprises doivent également démontrer clairement qu'elles répondent à ces recours en publiant des données sur les recours reçus et le résultat de ces décisions.

Sources possibles :

- Conditions générales de l'entreprise ou contrat d'utilisation
- Politiques de confidentialité de l'entreprise
- Rapport de développement durable de l'entreprise

Liberté d'expression et liberté d'information

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[16], le Pacte international relatif aux droits civils et politiques[17] 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 à celles d'autres acteurs, mais aussi dans leur façon de déterminer, de communiquer et d'appliquer les règles privées et les pratiques commerciales qui touchent aux droits fondamentaux des utilisateurs que sont la liberté d'expression et la liberté d'information.

F1: Accès aux politiques

F1(a). 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 principales parlées par les utilisateurs dans la juridiction d'origine 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 qui 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 trouver 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. L'utilisation d'un positionnement ou de couleurs rendant un

[16]Déclaration universelle des droits de l'homme https://www.un.org/fr/universal-declaration-human-rights/index.html

[17]Pacte international relatif aux droits civils et politiques, *Haut-commissariat des Nations Unies aux droits de l'homme*, https://www.ohchr.org/FR/ProfessionalInterest/Pages/CCPR.aspx

texte ou un lien moins visible, ou difficile à trouver sur une page Internet, signifie que le document n'est pas facilement accessible. Les conditions de service d'une application ne doivent jamais être à plus de « deux tapotements » de l'application (par exemple en incluant une option « Vie privée » ou « Protection des données » dans le menu de l'application). 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 sections, d'une taille de police lisible ou de toute autre caractéristique graphique qui favorise la compréhension, et l'utilisation d'une syntaxe compréhensible.

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

F1(b). Accès aux politiques en matière de contenu publicitaire

Les **politiques relatives au contenu publicitaire** de l'entreprise doivent être **facilement accessibles** et **facilement compréhensibles**.

Éléments :

1. Les **politiques relatives au contenu publicitaire** de l'entreprise sont-elles **facilement accessibles** ?

2. Les **politiques relatives au contenu publicitaire** de l'entreprise sont-elles disponibles dans la ou les langues principales parlées par les utilisateurs dans la juridiction d'origine de l'entreprise ?

3. Les **politiques relatives au contenu publicitaire** sont-elles présentées de manière **facilement compréhensible** ?

4. Pour les **écosystèmes mobiles** : L'entreprise **indique-t-elle clairement** qu'elle exige que les applications proposées par l'intermédiaire de son **app store** fournissent aux utilisateurs les **politiques relatives au contenu publicitaire** ?

5. Pour les **écosystèmes d'assistants personnels numériques** : L'entreprise **indique-t-elle** clairement qu'elle exige que les **skills** (fonctions) proposées par l'intermédiaire de son **skill store** fournissent aux utilisateurs les **politiques relatives au contenu publicitaire** ?

Détails de l'indicateur : Les entreprises qui autorisent tout type de publicité sur leurs services ou plateformes doivent clairement indiquer les règles relatives aux types de contenu publicitaire interdits, par exemple les publicités discriminatoires envers des individus ou des groupes selon des caractéristiques personnelles (âge, religion, sexe et origine ethnique).

Les entreprises doivent être transparentes sur ces règles afin que les utilisateurs et les annonceurs comprennent quels types de contenu publicitaire sont interdits et qu'ils puissent être responsables du contenu publicitaire qui apparaît sur leurs services ou plateformes.

Par conséquent, les entreprises doivent s'assurer de rendre ces règles faciles à trouver (E1), faciles à comprendre (E3) et disponibles dans les principales langues du marché d'origine de l'entreprise (E2). Les entreprises qui exploitent des écosystèmes mobiles (Apple iOS, Google Android, et l'implémentation d'Android par Samsung) et des écosystèmes d'assistants personnels numériques (Alexa pour Amazon, AliGenie pour Alibaba) doivent permettre aux utilisateurs de choisir les applications ou les skills à télécharger en fonction de leur participation (ou non) aux réseaux publicitaires. Ainsi, les éléments 4 et 5 vérifient si l'entreprise indique le besoin de télécharger une applications ou des skills mises à disposition sur sa plateforme pour fournir aux utilisateurs l'accès à la politique de contenu publicitaire.

Sources possibles :

- Politiques de l'entreprise en matière de publicité
- Centre d'aide de l'entreprise
- Conditions d'utilisation de l'entreprise

F1(c). Accès aux politiques en matière de publicité ciblée

Les **politiques relatives aux publicités ciblées** de l'entreprise doivent être **facilement accessibles** et **facilement compréhensibles**.

Éléments :

1. Les **politiques relatives aux publicités ciblées** de l'entreprise sont-elles **facilement accessibles** ?

2. Les **politiques relatives aux publicités ciblées** de l'entreprise sont-elles disponibles dans la ou les langues principales parlées par les utilisateurs dans la juridiction d'origine de l'entreprise ?

3. Les **politiques relatives aux publicités ciblées** sont-elles présentées de **manière facilement compréhensible** ?

4. Pour les **écosystèmes mobiles** : L'entreprise indique-t-elle clairement qu'elle exige que les applications proposées par l'intermédiaire de son **app store** fournissent aux utilisateurs les **politiques relatives aux publicités ciblées** ?

5. Pour les **écosystèmes d'assistants personnels numériques** : L'entreprise indique-t-elle clairement qu'elle exige que les **skills** proposées par l'intermédiaire de son **skill store** fournissent aux utilisateurs l'accès aux **politiques relatives aux publicités ciblées** ?

Détails de l'indicateur : En plus de rendre accessibles leur politiques de contenu publicitaire (Indicateur F1b), les entreprises doivent également publier clairement leurs politiques de ciblage publicitaire. La capacité des annonceurs ou d'autres tiers à cibler les utilisateurs avec un contenu personnalisé selon leurs comportements de navigation, les informations de

localisation et d'autres données et caractéristiques inférées à leur sujet[18] peut considérablement façonner (ou dans certains cas, déformer) l'écosystème en ligne d'un utilisateur. Le ciblage, qui peut inclure des contenus payants et non payants, peut amplifier les inégalités sociales hors ligne et peut être ouvertement discriminatoire. Il peut également entraîner des bulles de filtrage et amplifier les contenus problématiques, y compris les contenus destinés à induire en erreur ou à répandre des mensonges.[19]

Par conséquent, les entreprises qui permettent aux annonceurs et à d'autres tiers de cibler leurs utilisateurs avec des annonces ou des contenus personnalisés doivent publier leurs politiques de ciblage et les rendre faciles à trouver et faciles à comprendre par les utilisateurs et disponibles dans les principales langues du marché d'origine de l'entreprise. Les utilisateurs doivent pouvoir accéder à ces règles et les comprendre afin de prendre des décisions éclairées en utilisant les informations sur le contenu publicitaire qu'ils reçoivent. Pour les écosystèmes mobiles et les écosystèmes d'assistants numériques personnels, les entreprises doivent indiquer la nécessité pour les applications ou les skills mis à disposition par leurs magasins d'applications ou de skills de fournir aux utilisateurs une politique de ciblage publicitaire accessible.

Sources possibles :

- Politiques de l'entreprise en matière de publicité
- Centre d'aide de l'entreprise
- Conditions d'utilisation de l'entreprise

F1(d). Accès aux politiques en matière d'utilisation de système algorithmique

Les politiques relatives à l'utilisation d'**algorithmes** par l'entreprise doivent être **facilement accessibles** et **facilement compréhensibles par les utilisateurs**.

Éléments :

1. Les **politiques de l'entreprise relatives à l'utilisation d'un système algorithmique** sont-elles **facilement accessibles** ?

[18] Pour plus d'information sur les politiques d'inférence de données, consultez le paragraphe 6.2. du document « 2020 Pilot Study and Lessons Learned, » *Ranking Digital Rights*, 16 mars 2020, disponible en anglais https://rankingdigitalrights.org/wp-content/uploads/2020/03/pilot-report-2020.pdf.
[19] « Draft Indicators: Transparency and accountability standards for targeted advertising and algorithmic decision-making systems, » *Ranking Digital Rights*, octobre 2019, disponible en anglais https://rankingdigitalrights.org/wp-content/uploads/2019/10/RDR-Index-Draft-Indicators_-Targeted-advertising-algorithms.pdf.

2. Les **politiques de l'entreprise relatives à l'utilisation d'un système algorithmique** sont-elles disponibles dans la ou les langues principales parlées par les utilisateurs dans la juridiction d'origine de l'entreprise ?

3. Les **politiques de l'entreprise relatives à l'utilisation d'un système algorithmique** sont-elles présentées de manière **facilement compréhensible** ?

Détails de l'indicateur : L'utilisation de systèmes algorithmiques peut avoir des effets négatifs sur les droits fondamentaux, en particulier sur le droit à la liberté d'expression et d'information ainsi que sur le droit à la non-discrimination[20] En plus de s'engager clairement à respecter et à protéger les droits de l'homme lorsqu'elles développent et déploient ces technologies (voir l'indicateur G1, élément 3), les entreprises doivent également publier des politiques décrivant clairement les modalités d'utilisation des systèmes algorithmiques dans l'ensemble de leurs services et de leurs plates-formes. Tout comme les politiques de service ou les accords d'utilisation décrivent les types de contenu ou d'activités interdits, les entreprises utilisant des systèmes algorithmiques susceptibles de porter atteinte aux droits de l'homme doivent publier une politique claire et accessible indiquant la nature et les fonctions de ces systèmes. Comme recommandé par le Conseil de l'Europe dans sa Recommandation sur les impacts des systèmes algorithmiques sur les droits de l'homme (2020), cette politique doit être facile à trouver, présentée dans un langage simple et contenir des options permettant aux utilisateurs de gérer les paramètres.

Notez que dans cet indicateur, nous recherchons une politique qui explique les termes relatifs à la manière dont l'entreprise déploie les systèmes algorithmiques sur ses plateformes et services. Nous recherchons également toute précision des entreprises sur les conditions de développement et de test des systèmes algorithmiques, ce qui est abordé dans l'indicateur P1b.

Sources possibles

- Politiques relatives à l'utilisation de systèmes algorithmiques
- Directives pour le développement de systèmes algorithmiques
- Politique de confidentialité ou politiques des données
- Centre d'aide

F2 : Information sur les modifications de politiques

F2(a). Modifications des conditions d'utilisation

L'entreprise doit **indiquer clairement** que les utilisateurs sont **directement informés** lorsqu'elle modifie ses conditions d'utilisation avant que ces modifications n'entrent en vigueur.

Éléments :

[20] « Human Rights Risk Scenarios: Algorithms, machine learning and automated decision-making, »' *Ranking Digital Rights*, juillet 2019, disponible en anglais, https://rankingdigitalrights.org/wp-content/uploads/2019/07/Human-Rights-Risk-Scenarios -algorithms-machine-learning-automated-decision-making.pdf **2019 doit exister e francais)**

1. L'entreprise **indique-t-elle clairement** qu'elle **informe directement** les utilisateurs de tout changement relatifs aux **conditions d'utilisations** ?

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 directement** les **utilisateurs** de modifications avant l'entrée en vigueur de ces 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 et d'information des utilisateurs. Nous attendons donc des entreprises qu'elles s'engagent à informer les utilisateurs lorsqu'elles modifient ces modalités et à leur fournir des informations qui les aident à comprendre la signification de ces changements.

Cet indicateur évalue si les entreprises indiquent clairement la méthode et le délai de notification des utilisateurs concernant les modifications de leurs conditions de service. Nous attendons des entreprises qu'elles s'engagent à notifier directement les utilisateurs de ces changements avant leur entrée en vigueur. La méthode de notification directe pouvant varier selon le type de service, nous attendons des entreprises qu'elles informent directement les utilisateurs de façon à ce que ces derniers soient sûrs d'y accéder. Pour les services qui impliquent des comptes utilisateurs, la notification directe peut se traduire par 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 visible sur la page principale d'accès au service. Cet indicateur recherche aussi les 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

F2(b). Modifications des politiques en matière de contenu publicitaire

L'entreprise doit **indiquer clairement** que **les utilisateurs sont directement informés** lorsqu'elle modifie ses politiques en matière de contenu publicitaire avant que ces modifications n'entrent en vigueur.

Éléments :

1. L'entreprise **indique-t-elle clairement** qu'elle **informe directement** les **utilisateurs** des changements apportés à ses politiques de contenu publicitaire ?

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 directement** les **utilisateurs** de modifications avant l'entrée en vigueur de ces changements ?

4. L'entreprise possède-t-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** proposées par l'intermédiaire de son **app store** **avertissent** les **utilisateurs** lors de la modification des **politiques relatives au contenu publicitaire** ?

6. Pour les **écosystèmes d'assistants personnels numériques** : L'entreprise indique-t-elle clairement qu'elle exige que les **skills** proposées par l'intermédiaire de son **skill store** **avertissent** les **utilisateurs** lors de la modification des **politiques relatives au contenu publicitaire** ?

Détails de l'indicateur : Il est courant pour les entreprises de modifier leurs politiques relatives au contenu publicitaire au fur et à mesure que leurs activités et services 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 et d'information des utilisateurs, ainsi que sur leur droit à la non-discrimination. Nous attendons donc des entreprises qu'elles s'engagent à informer les utilisateurs lorsqu'elles modifient ces modalités et à leur fournir des informations qui les aident à comprendre la signification de ces changements.

Cet indicateur évalue si les entreprises indiquent clairement la méthode et le délai de notification des utilisateurs concernant les modifications avant leur entrée en vigueur. La méthode de notification directe pouvant varier selon le type de service, nous attendons des entreprises qu'elles informent directement les utilisateurs de façon à ce que ces derniers soient sûrs d'y accéder. Pour les services qui impliquent des comptes utilisateurs, la notification directe peut se traduire par 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 visible sur la page principale d'accès au service. Cet indicateur recherche aussi les 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 :
- Politiques en matière de publicité, directives, conditions générales, etc.
- Publicités de l'entreprise ou centre d'aide de l'entreprise

F2(c). Modifications des politiques en matière de publicité ciblée

L'entreprise doit **indiquer clairement** que les **utilisateurs** sont **directement informés** lorsqu'elle modifie ses **politiques en matière de publicité ciblée** avant que ces modifications n'entrent en vigueur.

Éléments :

1. L'entreprise **indique-t-elle clairement** qu'elle informe les utilisateurs des changements apportés à ses **politiques de publicité ciblée** ?

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 directement** les **utilisateurs** de modifications avant l'entrée en vigueur de ces changements ?

4. L'entreprise possède-t-elle des **archives publiques** ou un **journal des modifications** ?

5. Pour les **écosystèmes d'assistants personnels numériques** : L'entreprise indique-t-elle clairement qu'elle exige que les **applications** proposées par l'intermédiaire de son **app store** avertissent directement les utilisateurs lors de la modification de leurs **politiques relatives aux publicités ciblées** ?

6. Pour les **écosystèmes d'assistants personnels numériques** : L'entreprise indique-t-elle clairement qu'elle exige que les **skills** proposées par l'intermédiaire de son **skill store** avertissent les utilisateurs lors de la modification des **politiques relatives aux publicités ciblées** ?

Détails de l'indicateur : Il est courant pour les entreprises de modifier leurs politiques relatives aux publicités ciblées au fur et à mesure que leurs activités et services évoluent. Toutefois, ces changements peuvent avoir une incidence significative sur le droit à la liberté d'expression et d'information des utilisateurs, ainsi que sur leur droit à la non-discrimination. Nous attendons donc des entreprises qu'elles s'engagent à informer les utilisateurs lorsqu'elles modifient ces modalités et à leur fournir des informations qui les aident à comprendre la signification de ces changements.

Cet indicateur évalue si les entreprises indiquent clairement la méthode et le délai de notification des utilisateurs concernant les modifications avant leur entrée en vigueur. La méthode de notification directe pouvant varier selon le type de service, nous attendons des entreprises qu'elles informent directement les utilisateurs de façon à ce que ces derniers soient sûrs d'y accéder. Pour les services qui impliquent des comptes utilisateurs, la notification directe peut se traduire par 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 visible sur la page principale d'accès au service. Cet indicateur recherche aussi les 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 :

- Politiques en matière de publicité, directives, conditions générales, etc.
- Publicité de l'entreprise ou centre d'aide de l'entreprise

F2(d). Modifications des politiques en matière d'utilisation de système algorithmique

L'entreprise doit **indiquer clairement** que les **utilisateurs** sont **directement informés** lorsqu'elle modifie ses **politiques relatives à l'utilisation de systèmes algorithmiques** avant que ces modifications n'entrent en vigueur.

Éléments :

1. L'entreprise **indique-t-elle clairement** qu'elle **informe directement** les **utilisateurs** des changements apportés à **ses politiques d'utilisation de systèmes algorithmiques** ?

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 directement** les **utilisateurs** de modifications avant l'entrée en vigueur de ces changements ?

4. L'entreprise possède-t-elle des **archives publiques** ou un **journal des modifications** ?

Détails de l'indicateur : Lorsque les entreprises modifient leurs politiques d'utilisation des algorithmes, ces changements peuvent affecter le droit à la liberté d'expression et d'information des utilisateurs ainsi que leur droit à la non-discrimination. Nous attendons donc des entreprises qu'elles s'engagent à informer les utilisateurs lorsqu'elles modifient ces modalités et à leur fournir des informations qui les aident à comprendre la signification de ces changements. Cette norme est conforme à la recommandation du Conseil de l'Europe sur les impacts des systèmes algorithmiques sur les droits de l'homme (2020).

Cet indicateur évalue si les entreprises indiquent clairement la méthode et le délai de notification des utilisateurs concernant les modifications avant leur entrée en vigueur. La méthode de notification directe pouvant varier selon le type de service, nous attendons des entreprises qu'elles informent directement les utilisateurs de façon à ce que ces derniers soient sûrs d'y accéder. Pour les services qui impliquent d'ouvrir des comptes utilisateurs, la notification directe peut se traduire par 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 visible sur la page principale d'accès au service. Cet indicateur recherche aussi les preuves qu'une entreprise fournit des documents publics qui contiennent les conditions d'utilisation antérieures afin que le public puisse comprendre l'évolution de ces conditions.

Sources possibles :
- Politiques relatives à l'utilisation de systèmes algorithmiques
- Directives pour le développement de systèmes algorithmiques
- Politique de confidentialité ou politiques des données
- Centre d'aide

F3 : Processus d'application des politiques

F3(a). 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 **indique-t-elle clairement** les procédures qu'elle utilise pour **signaler** les **contenus** ou les comptes qui enfreignent son règlement ?
4. L'entreprise **indique-t-elle clairement** comment les **systèmes algorithmiques** sont utilisés pour **signaler** les **contenus** qui pourraient enfreindre son règlement ?
5. 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 ?
6. 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 ?
7. L'entreprise **indique-t-elle clairement** son processus pour appliquer son règlement une fois que son règlement est enfreint ?

Détails de l'indicateur : Il est juste d'attendre des entreprises qu'elles établissent des règlements interdisant certains contenus ou activités, comme les discours toxiques ou les comportements malveillants. Toutefois, lorsque les entreprises élaborent et mettent en application des règlements sur ce que les utilisateurs peuvent faire ou dire sur Internet : ou sur leur accès à un service- elles doivent le faire de manière transparent et responsable.

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 utiliser les services de sous-traitants pour examiner le contenu et/ou l'activité des utilisateurs. Elles peuvent aussi 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. Elles peuvent également déployer des systèmes algorithmiques pour détecter et signaler les infractions, auquel cas, les entreprises doivent expliquer comment ces systèmes sont utilisés et quels types de contenus ils utilisent. 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. Pour les écosystèmes d'assistants personnels numériques, nous attendons des entreprises qu'elles indiquent les types de skills et les résultats de recherche 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 générales de l'entreprise, contrat d'utilisation
- 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

F3(b). Règles relatives au contenu publicitaire et leur application

L'entreprise doit **indiquer clairement** ses politiques définissant quels types de contenu publicitaire sont interdits.

Éléments :

1. L'entreprise **indique-t-elle clairement** quels types de **contenu publicitaire** ne sont pas autorisés ?

2. L'entreprise **indique-t-elle clairement** si elle **exige** que tout le **contenu publicitaire** soit identifié comme tel ?

3. L'entreprise **indique-t-elle clairement** les processus et technologies qu'elle utilise pour identifier les **contenus publicitaires** ou les **comptes** qui enfreignent son règlement ?

Détails de l'indicateur : Les entreprises doivent clairement indiquer les politiques relatives aux types de contenus publicitaires interdits sur leur plateforme ou service, ainsi que les processus de mise en œuvre de ces règles. Plus précisément, cet indicateur vérifie si l'entreprise indique clairement les types de contenus publicitaires interdits, si elle indique une disposition selon laquelle tous les contenus publicitaires doivent être clairement indiqués comme tels, et si elle indique ses processus pour faire respecter ces règles

Sources possibles :
- Portail des annonceurs de l'entreprise, politiques publicitaires, politiques relatives aux publicités politiques
- Conditions d'utilisation de l'entreprise, contrat avec l'utilisateur
- Politique d'utilisation acceptable par l'entreprise, normes communautaires, lignes directrices sur le contenu
- Support de l'entreprise, centre d'aide ou FAQ

F3(c). Règles relatives à la publicité ciblée et leur application

L'entreprise doit **indiquer clairement** ses politiques définissant quels types de **ciblage publicitaire** sont interdits.

Éléments :

1. L'entreprise **indique-t-elle clairement** si des **tierces parties** sont autorisés à cibler ses **utilisateurs** avec du **contenu publicitaire** ?

2. L'entreprise **indique-t-elle clairement** quels types de **paramètres de ciblage** ne sont pas autorisés ?

3. L'entreprise **indique-t-elle clairement** qu'elle ne permet pas aux annonceurs de cibler des personnes spécifiques ?

4. L'entreprise **indique-t-elle clairement** que les **catégories d'audience publicitaire** générées par **algorithme** sont évaluées par des évaluateurs humains avant de pouvoir être utilisées ?

5. L'entreprise **indique-t-elle clairement** les informations relatives aux processus et aux technologies qu'elle utilise pour identifier les **contenus publicitaires** ou les **comptes** qui enfreignent son règlement ?

Détails de l'indicateur : La capacité des annonceurs ou d'autres tiers à cibler les utilisateurs avec un contenu adapté (s'appuyant sur leurs habitudes de navigation, sur les informations de localisation et sur d'autres données et caractéristiques inférées les concernant[21]), peut considérablement influencer l'écosystème en ligne d'un utilisateur. Le ciblage, pouvant inclure à la fois du contenu payant et non payant, peut amplifier les inégalités sociales hors ligne et peut être ouvertement discriminatoire. Il peut également entraîner ce que l'on appelle des « bulles de filtrage » et diffuser des contenus problématiques, y compris des contenus destinés à induire en erreur l'utilisateur ou à répandre des mensonges[22].

Par conséquent, les entreprises qui permettent aux annonceurs et à d'autres tiers de cibler leurs utilisateurs avec des annonces ou des contenus adaptés doivent disposer de politiques claires décrivant les règles de ciblage des annonces. Les entreprises doivent indiquer clairement si elles permettent à des tiers de cibler leurs utilisateurs au moyen de publicités ciblées ou d'autres types de contenus sponsorisés, et préciser clairement quels paramètres de ciblage ne sont pas autorisés (utilisation de certains types de catégories de public, comme l'âge, le lieu ou d'autres caractéristiques de l'utilisateur par exemple). Les entreprises doivent également indiquer leurs procédures de détection des infractions aux règles de ciblage.

Sources possibles :

- Portail des annonceurs de l'entreprise, politiques publicitaires, politiques relatives aux publicités politiques
- Politiques d'utilisation acceptable de l'entreprise
- Support de l'entreprise, centre d'aide ou FAQ de l'annonceur

[21] Pour plus d'information sur les politiques d'inférence de données, consultez le paragraphe 6.2. du document « 2020 Pilot Study and Lessons Learned, » *Ranking Digital Rights*, 16 mars 2020, disponible en anglais https://rankingdigitalrights.org/wp-content/uploads/2020/03/pilot-report-2020.pdf.

[22] « Draft Indicators: Transparency and accountability standards for targeted advertising and algorithmic decision-making systems, » *Ranking Digital Rights*, octobre 2019, disponible en anglais, https://rankingdigitalrights.org/wp-content/uploads/2019/10/RDR-Index-Draft-Indicators_-Targeted-advertising-algorithms.pdf.

F4: Données sur l'application des politiques

F4(a). Données sur les restrictions de contenu pour 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** qui enfreignent son règlement.

Éléments :

1. L'entreprise publie-t-elle les données relatives au nombre de **contenus restreints** pour infraction à son règlement ?

2. L'entreprise publie-t-elle les données relatives au nombre de **contenus restreints** par règle enfreinte ?

3. L'entreprise publie-t-elle des données sur le nombre de **contenus** qu'elle a limités en fonction du format de ces contenus ? (Par exemple, texte, image, vidéo, vidéo en direct) ?

4. L'entreprise publie-t-elle des données sur le nombre de **contenus** qu'elle a **restreints** en fonction de la méthode utilisée pour identifier la violation ?

5. L'entreprise publie-t-elle ces données au moins quatre fois par an ?

6. Les données peuvent-elles être exportées sous la forme d'un fichier de **données structurées** ?

Détails de l'indicateur : Les entreprises peuvent et doivent fixer des règles claires sur les types de contenu non autorisés sur leurs plateformes ou services. Cet indicateur attend des entreprises qu'elles publient des données sur les mesures qu'elles prennent pour restreindre ou, dans le cas contraire, censurer les contenus en raison de violations des règles de l'entreprise. La publication de ces données est une première étape essentielle pour tenir les entreprises responsables de l'application de leurs propres règles et des mesures qu'elles prennent pour modérer les contenus sur leurs plateformes et services.

Les entreprises doivent publier des données sur le nombre total de contenus qu'elles restreignent, suppriment ou, dans le cas des entreprises de télécommunications, de contenus qu'elles bloquent ou filtrent, en raison de violations des conditions de service. Elles doivent également ventiler ces données par violation et par méthode avec laquelle la violation des règles a été détectée (programme de signalement communautaire ou automatisation). Les entreprises doivent également publier ces données au moins quatre fois par an, conformément aux principes de Santa Clara. Ce fichier de données doit être structuré.

Sources possibles :

- Rapport sur la transparence de l'entreprise

- Rapport sur l'application des normes communautaires de l'entreprise,

F4(b). Données sur les restrictions de compte pour 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 aux comptes** qui enfreignent son règlement.

Éléments :

1. L'entreprise publie-t-elle les données relatives au nombre de **comptes** dont l'accès est **restreint** pour infraction à son règlement ?
2. L'entreprise publie-t-elle les données relatives au nombre de **comptes** dont l'accès est **restreint** par règle enfreinte ?
3. L'entreprise publie-t-elle les données relatives au nombre de comptes dont l'accès est restreint en fonction de la méthode utilisée pour identifier l'infraction au règlement ?
4. L'entreprise publie-t-elle ces données au moins quatre fois par an ?
5. Les données peuvent-elles être exportées sous la forme d'un fichier de **données structurées** ?

Sources possibles :

- Rapport sur la transparence de l'entreprise

Détails de l'indicateur : Les entreprises peuvent et doivent fixer des règles claires sur les types de contenu non autorisés sur leurs plateformes ou services. Cet indicateur attend des entreprises qu'elles publient des données sur les mesures qu'elles prennent pour appliquer ces règles. La publication de ces données est une première étape essentielle pour tenir les entreprises responsables de l'application de leurs propres règles et des mesures qu'elles prennent pour modérer les contenus sur leurs plateformes et services.

Les entreprises doivent publier des données sur le nombre de comptes utilisateurs qu'elles restreignent en raison de violations de leurs conditions de service. Elles doivent également ventiler ces données par violation et par méthode avec laquelle la violation des règles a été détectée (programme de signalement communautaire ou automatisation). Les entreprises doivent également publier ces données au moins quatre fois par an, conformément aux principes de Santa Clara. Ce fichier de données doit être structuré.

Sources possibles :

- Rapport sur la transparence de l'entreprise

F4(c). Données sur le contenu publicitaire et application des politiques de ciblage publicitaire

L'entreprise doit **communiquer clairement** et régulièrement des données sur le volume et la nature des mesures prises pour **restreindre les contenus publicitaires** qui enfreignent ses **politiques relatives au contenu publicitaire** et **au ciblage publicitaire**.

Eléments

1. L'entreprise publie-t-elle le nombre total d'**annonces publicitaires** qu'elle a **limitées** pour faire respecter sa **politiques relatives au contenu publicitaire** ?
2. L'entreprise publie-t-elle le nombre total d'**annonces publicitaires** qu'elle a **limitées** en fonction de l'infraction à son règlement relatif au **ciblage publicitaire** ?
3. L'entreprise publie-t-elle le nombre total d'annonces publicitaires qu'elle a limitées pour faire respecter **sa politique en matière de contenu ciblé** ?
4. L'entreprise publie-t-elle le nombre total de publicités qu'elle a **limitées** en fonction de l'infraction au règlement relatif au **ciblage publicitaire** ?
5. L'entreprise publie-t-elle ces données au moins une fois par an ?
6. Les données peuvent-elles être exportées sous la forme d'un fichier de **données structurées** ?

Détails de l'indicateur : Les indicateurs F3c et F3d demandent aux entreprises de divulguer clairement les règles relatives aux types de contenu publicitaire et au ciblage publicitaire qui sont respectivement interdits, et de décrire leurs processus de mise en œuvre de ces règles. L'indicateur F4c demande aux entreprises de publier des preuves qu'elles appliquent ces règles. Les entreprises doivent publier des données sur le nombre total de publicités qu'elles suppriment à la suite de violations des politiques de contenu publicitaire, et elles doivent également ventiler ces données en fonction de la règle qui a été enfreinte. Les entreprises doivent également fournir la preuve qu'elles appliquent leurs politiques de ciblage des publicités en publiant des données sur le nombre d'annonces supprimées pour violation des règles de ciblage, et en indiquant la règle qui a été enfreinte. Les entreprises doivent également publier ces données au moins une fois par an et dans un fichier de données structuré.

Sources possibles :

- Rapport sur la transparence de l'entreprise

F5. Réponse aux demandes de tiers de restriction d'accès à des contenus ou des comptes

F5(a). Processus de réponse aux demandes gouvernementales

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

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. Les explications de l'entreprise **indiquent-elles clairement** la base juridique sur laquelle elle peut accéder aux **demandes émanant de gouvernements** ?
5. L'entreprise indique-t-elle clairement qu'elle applique une diligence raisonnable lors de l'étude des **demandes gouvernementales** avant de décider de la façon d'y répondre ?
6. L'entreprise s'engage-t-elle à refuser les **demandes** inappropriées ou excessives **formulées par les gouvernements** ?
7. L'entreprise fournit-elle des indications claires ou des exemples pour expliquer l'application de sa procédure de réponse aux **demandes gouvernementales** ?

Détails de l'indicateur : Les entreprises reçoivent souvent de la part de gouvernements des demandes de suppression, de filtrage ou de restriction d'accès pour des contenus ou des comptes. Ces demandes émanent d'organismes publics, des forces de l'ordre ou de tribunaux (nationaux ou étrangers). Nous attendons des entreprises qu'elles communiquent publiquement leurs procédures de réponse à ce type de demandes. L'entreprise doit notamment indiquer les motifs juridiques qui l'obligerait à accéder à ces demandes gouvernementales et s'engager à rejeter les demandes dont la portée est excessive.

Il est à noter que notre définition des « demandes gouvernementales » inclut les demandes émanant d'un processus non judiciaire, comme une ordonnance des forces de l'ordre, ou d'affaires civiles engagées par des entités privées qui passerait par des tribunaux civils. Les demandes déposées par le biais de processus organisés comme le Digital Millenium Copyright Act (loi sur les droits d'auteur) aux États-Unis ou le jugement sur le droit européen à l'oubli sont définis comme des « processus privés » et sont évalués dans l'indicateur F5b ci-dessous.

Sources possibles :

- Rapport sur la transparence de l'entreprise
- Directives de l'entreprise relatives à l'application de la législation
- Rapports annuels de l'entreprise

F5(b). Processus de réponse aux demandes privées

L'entreprise doit **indiquer clairement** ses procédures de réponse aux **demandes** de restriction d'accès, de filtrage ou de blocage de **contenus** ou de **comptes** émanant d'un **processus de demande privé**.

Éléments :

1. L'entreprise **indique-t-elle clairement** ses procédures de réponse aux **demandes** de restriction d'accès, de filtrage ou de blocage de **contenus** ou de **comptes** par le biais d'un **processus de demande privée** ?

2. L'entreprise **indique-t-elle clairement** sur quelle base elle accède aux **demandes** émanant d'un **processus privé** ?

3. L'entreprise **indique-t-elle clairement** qu'elle s'astreint à une diligence raisonnable lors de l'étude des **demandes** émanant d'un **processus privé** avant de décider de la façon d'y répondre ?

4. L'entreprise s'engage-t-elle à refuser les **demandes** inappropriées ou excessives émanant d'un **processus privé** ?

5. L'entreprise fournit-elle des explications claires ou des exemples pour expliquer l'application de sa procédure de réponse aux **demandes** émanant d'un **processus privé** ?

Détails de l'indicateur : Outre les demandes des gouvernements et d'autres autorités, les entreprises peuvent recevoir des demandes de suppression ou de restriction d'accès pour des contenus ou des comptes via un processus dit privé. Ces types de demandes peuvent émaner de procédures officielles établies par la loi (par exemple les demandes faites en vertu de la loi américaine Digital Millennium Copyright Act, du Droit européen à l'oubli, etc.) ou par le biais d'accords d'autorégulation (par exemple les accords d'entreprise visant à bloquer certains types de contenu ou d'images, comme le Code de bonnes pratiques contre la désinformation en ligne de l'UE). Il est à noter que cet indicateur ne considère pas les demandes privées comme des demandes émanant d'un tribunal ou toute entité judiciaire considérées ici comme des « demandes gouvernementales » (indicateur F5a)

Cet indicateur évalue si les entreprises indiquent clairement comment elles répondent aux demandes de suppression, filtrage ou restriction d'accès ou de contenu qui leur parviennent via un processus de demande privé (Eléments 1). L'entreprise doit indiquer les raisons pour lesquelles elle se conforme à ces demandes (élément 2), si elle fait preuve de diligence raisonnable à l'égard de ces demandes avant de décider de la manière d'y répondre (élément 3). Nous attendons également des entreprises qu'elles s'engagent à repousser les demandes trop générales de suppression de contenus ou de comptes qui proviendrait d'un

processus privés (élément 4), et qu'elles publient des exemples clairs illustrant la manière dont elle traite ces types de demandes (élément 5).

Sources possibles :

- Rapport sur la transparence 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 indique-t-elle le nombre de **demandes** reçues 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 de représentants du gouvernement pour restreindre l'accès à des **contenus** ou des **comptes** par des **canaux non officiels** ?
7. L'entreprise indique-t-elle le nombre de **demandes** auxquelles elle s'est conformée ?
8. L'entreprise publie-t-elle une copie des **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 souvent de la part de gouvernements des demandes de suppression, de filtrage ou de restriction d'accès pour des contenus ou des comptes. Nous attendons des entreprises qu'elles publient régulièrement les données relatives au nombre et aux types de demandes gouvernementales reçus, ainsi que le nombre de demandes auxquelles elles accèdent. Les entreprises peuvent recevoir ces demandes par le biais de procédures officielles, telles qu'une ordonnance du tribunal, ou par

des canaux informels, comme un système de signalement destiné à permettre aux particuliers de signaler les contenus enfreignant les conditions d'utilisation. 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'identifier comme appartenant aux demandes gouvernementales. La divulgation de ces données aide le public à mieux comprendre la relation entre les entreprises et les gouvernements dans la régulation du contenu en ligne. Cela aide également le public à tenir les entreprises responsables de leurs obligations en matière de respect et de protection du droit à la liberté d'expression.

Dans certains cas, la loi peut empêcher une entreprise de divulguer les informations mentionnées dans les éléments de cet indicateur. Nous attendons par exemple 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 ces 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** de suppression, de filtrage ou de restriction d'accès à des **contenus** ou des **comptes** émanant d'un **processus privé**.

Éléments :

1. L'entreprise indique-t-elle le nombre de **demandes** de **restriction de contenu** ou de **compte** qu'elle reçoit via un **processus privé** ?
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 énumère-t-elle les motifs de suppression associés aux demandes qu'elle reçoit ?
5. L'entreprise **indique-t-elle clairement** les demandes émanant d'un **processus privé** ?
6. L'entreprise indique-t-elle le nombre de demandes auxquelles elle a accédé ?
7. L'entreprise publie-t-elle une copie des requêtes 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 qu'elle reçoit par le processus de 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 via un processus privé (telles que les demandes effectuées en vertu de la loi américaine Digital Millenium Copyright Act ou du Droit européen à l'oubli) ou par le biais d'accords d'autorégulation (par exemple les accords d'entreprise visant à bloquer certains types de contenu ou d'images). Nous attendons des entreprises qu'elles publient régulièrement des données sur le nombre et le type de demandes reçues via ces processus privés et sur le nombre de demandes auxquelles elles se sont conformées.

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, **indique-t-elle 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 notifie 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 générales de l'entreprise,
- Normes de l'entreprise pour sa communauté
- Page de support de l'entreprise, centre d'aide ou FAQ
- 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 pour une raison autre que celle d'assurer la qualité du service et la fiabilité du réseau.

Éléments :

1. L'entreprise **affiche-t-elle un engagement clair** 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. L'entreprise a-t-elle recours à des pratiques, comme des **programmes zero-rating**, qui **priorise l**e trafic du réseau pour des raisons autres que l'assurance de la qualité du service et la fiabilité du réseau ?

3. Si l'entreprise a recours à des pratiques de **hiérarchisation** pour des raisons autres que l'assurance de la qualité du service et la fiabilité du réseau, **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 impactant 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. Les entreprises peuvent avoir recours à des pratiques rémunérées de hiérarchisation ou à des programmes *zero-rating* qui ne relèvent pas des pratiques légitimes de gestion de réseau. En effet, une entreprise peut afficher sur son site Internet une déclaration d'engagement envers la neutralité du Net mais proposer parallèlement un programme *zero-rating*.

Sources possibles :

- Politiques de l'entreprise relatives à la gestion du réseau ou du trafic
- Rapports annuels de l'entreprise

F10. Coupure de réseau (entreprises de télécommunications)

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

Éléments :

1. L'entreprise **indique-t-elle clairement** les motifs pour lesquels elle peut être amenée à interrompre le service pour une région géographique 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 gouvernementales** d'**interruption de réseau ou de restriction d'accès à un service** ?

4. L'entreprise **indique-t-elle clairement** son engagement à refuser les **demandes d'interruption ou de restriction d'accès à un service émanant d'un gouvernement** ?

5. L'entreprise **indique-t-elle clairement** qu'elle informe directement les utilisateurs lorsqu'elle interrompt l'accès à un réseau ou restreint l'accès à un service ?

6. L'entreprise **indique-t-elle clairement** le nombre de **demandes d'interruption du réseau** qu'elle reçoit ?

7. L'entreprise **indique-t-elle clairement** l'autorité spécifique dont émane la **demande** ?

8. L'entreprise **indique-t-elle clairement** le nombre de **demandes gouvernementales** auxquelles elle s'est conformée ?

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. [23] Pourtant, les gouvernements ordonnent toujours plus fréquemment aux entreprises de télécommunications de procéder à des interruptions de réseau[24], 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, qu'elles rendent compte de telles demandes et qu'elles indiquent leurs engagements à rejeter ou limiter les effets des ordres émanant des gouvernements.

Sources possibles :

- Conditions d'utilisation de l'entreprise
- Rapport sur la transparence de l'entreprise
- Directives de l'entreprise relatives à l'application de la législation
- Politique de l'entreprise en matière de droits de l'homme

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 permettre 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 permettre 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 patronyme 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 celles 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 permettre de les identifier hors ligne. Les autres formes d'identification peuvent être des cartes bancaires de payement ou des numéros de téléphone enregistrés. 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 ne nécessitant pas de paiement sans avoir à fournir d'informations susceptibles de permettre de les identifier hors ligne. Dans certains cas, les numéros de téléphone peuvent être liés à l'identité hors ligne d'un utilisateur, par exemple dans des contextes juridiques où les

[23] « Promotion et protection de tous les droits de l'homme, civils, politiques, économiques, sociaux et culturels, y compris le droit au développement », Haut-commissariat des Nations-Unies aux droits de l'homme (trente-deuxième session), 27 juin 2016, https://documents-dds-ny.un.org/doc/UNDOC/LTD/G16/131/89/PDF/G1613189.pdf?OpenElement.

[24] "*#KeepItOn*", Access Now, https://www.accessnow.org/keepiton/, consulté le 2 avril 2020.

utilisateurs de services prépayés doivent s'enregistrer avec leurs identifiants. Lorsqu'un numéro de téléphone est nécessaire à la prestation du service (dans le cas d'applications de messagerie instantanée par exemple), les entreprises recevront une appréciation complète, sauf si elles exigent également des utilisateurs qu'ils utilisent leur vrai nom, ou qu'ils soumettent des documents qui relieraient leur nom à leur identité hors ligne. Les services exigeant des utilisateurs qu'ils fournissent un numéro de téléphone sans que cela soit nécessaire à la fourniture du service ne recevront aucun point. Par exemple, certains services peuvent nécessiter un numéro de téléphone à des fins d'identification à deux facteurs, mais cela doit rester facultatif et les utilisateurs doivent disposer d'autres options d'identification à deux facteurs.

Cet indicateur s'applique aux entreprises de plateformes numériques 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

F12. Systèmes algorithmiques de curation de contenu, de recommandation et/ou d'évaluation

Les entreprises doivent **indiquer clairement** comment le **contenu** en ligne de leurs utilisateurs est **organisé, évalué ou recommandé**.

Éléments :

1. L'entreprise **indique-t-elle clairement** si elle utilise des **systèmes algorithmiques** pour **organiser, recommander, et/ou évaluer** le **contenu** auquel les **utilisateurs** ont accès via ses plateformes ?

2. L'entreprise **indique-t-elle clairement** comment les **systèmes algorithmiques** sont déployés pour **organiser, recommander, et/ou évaluer** le **contenu** ? Indique-t-elle également les variables prises en compte par ces systèmes ?

3. L'entreprise **indique-t-elle clairement** de quelles options les utilisateurs disposent pour contrôler les variables que les **systèmes algorithmiques** prennent en compte pour **organiser, recommander, et/ou évaluer le contenu** ?

4. L'entreprise **indique-t-elle clairement** si des **systèmes algorithmiques** sont automatiquement utilisés pour **organiser, recommander, et/ou évaluer** le **contenu** par défaut ?

5. L'entreprise **indique-t-elle clairement** que les utilisateurs peuvent choisir ou refuser de participer à des systèmes automatisés **d'organisation de contenu, de recommandation et/ou de classement** ?

Détails de l'indicateur : Les systèmes algorithmiques de curation de contenu, de recommandation et d'évaluation jouent un rôle crucial dans la définition du contenu et des informa-

tions auxquels les utilisateurs ont accès en ligne. De plus, les systèmes optimisés pour l'engagement des utilisateurs peuvent avoir pour effet de prioriser les contenus controversés et incendiaires, y compris des contenus qui ne sont pas protégés par le droit international des droits de l'homme. Avec le temps, le recours à des systèmes de curation et de recommandation algorithmiques, optimisés pour l'engagement des utilisateurs, peut modifier les écosystèmes d'informations d'un pays ou de communautés entières. Ces systèmes peuvent être manipulés pour propager la désinformation, fausser l'écosystème de l'information et alimenter les atteintes aux droits de l'homme.

Les entreprises doivent donc être transparentes quant à l'utilisation des systèmes automatisés de curation, de recommandation et de classement, y compris les variables qui influencent ces systèmes. Les entreprises doivent indiquer si elles utilisent de tels systèmes, préciser leur fonctionnement et les options dont disposent les utilisateurs pour contrôler l'utilisation de leurs propres données utilisateurs par ces systèmes, et indiquer si ces systèmes sont automatiquement activés par défaut ou si les utilisateurs peuvent choisir d'autoriser leur contenu à être automatiquement géré par un système algorithmique.

Sources possibles :

- Politiques de l'entreprise en matière de droits de l'homme
- Politiques de l'entreprise relatives aux intelligences artificielles (IA), y compris les principes directeurs, les lignes directrices et les directives relatives aux IA
- Pages d'aide décrivant comment les paramètres des flux, les paramètres de la page d'accueil, les résultats de recherche, les recommandations, les intérêts des utilisateurs ou les sujets sont influencés par les algorithmes

F13. Agents logiciels automatisés (« bots »)

Les entreprises doivent **clairement indiquer** les politiques régissant l'utilisation d'**agents logiciels automatisés** (**bots**) sur leurs plateformes, produits et services, et la manière dont elles appliquent ces politiques.

Éléments :

1. L'entreprise **indique-t-elle clairement** les règles régissant l'utilisation des **bots** informatiques sur sa plateforme ?

2. L'entreprise **indique-t-elle clairement** qu'elle exige des **utilisateurs** qu'ils étiquettent clairement tous les **contenus** et **comptes** générés, diffusés ou exploités avec l'aide d'un **bot** ?

3. L'entreprise **indique-t-elle clairement** son processus pour appliquer sa **politique relative aux bots informatiques** ?

4. L'entreprise **indique-t-elle clairement** les données relatives au volume et à la nature du **contenu** et des **comptes** utilisateurs dont l'accès est restreint pour violation de sa politique relative aux bots informatiques ?

Détails de l'indicateur : Les plateformes de médias sociaux permettent souvent aux utilisateurs de créer des agents logiciels automatisés, ou « bots », qui automatisent diverses actions qu'un compte utilisateur peut effectuer, comme la publication ou le renforcement du contenu (re-tweeter, par exemple). Il existe de nombreuses utilisations inoffensives ou même positives des bots : par exemple, les artistes utilisent les bots de Twitter à des fins de parodie.[25] Il existe également des utilisations plus problématiques que de nombreuses entreprises interdisent ou découragent, comme lorsque les partis politiques ou leurs représentants utilisent des botnets pour promouvoir certains messages ou pour augmenter artificiellement l'influence d'un candidat et ainsi manipuler le débat public et les résultats. Sur certaines plateformes de médias sociaux, des robots ou des réseaux coordonnés de robots (« *botnets* ») peuvent être utilisés pour harceler des utilisateurs (« *brigading* »), amplifier artificiellement certains éléments de contenu (retweeting de masse, etc.) et déformer les discussions publiques sur la plateforme. Certains experts demandent aux entreprises d'exiger des utilisateurs utilisant des bots qu'ils les étiquettent explicitement comme tels, afin de faciliter la détection de ces distorsions[26].

Les entreprises qui autorisent les robots doivent donc avoir des politiques claires régissant l'utilisation de ces robots sur leurs plateformes. Elles doivent indiquer si elles exigent que les contenus et les comptes produits, diffusés ou exploités avec l'aide d'un robot soient étiquetés comme tels. Elles devraient également clarifier leur processus d'application de leurs politiques relatives aux robots, notamment en publiant des données sur le volume et la nature du contenu et des comptes qui sont restreints pour avoir enfreint ces règles.

Sources possibles :

- Politiques à l'intention des développeurs
- Règles relatives à l'automation ou aux bots informatiques
- Rapport sur la transparence 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[27], le Pacte international relatif aux droits civils et politiques[28] 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 juridiquement fondées, proportionnées et justifiées. Les entreprises qui obtiennent de bons résultats sur ces indicateurs ont démontré 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

[25] *Thinkpiece Bot*, Twitter, https://twitter.com/thinkpiecebot, consulté le 2 avril 2020.

[26] Engler, A. (22 janvier 2020). The case for AI transparency requirements. Brookings Institution. https://www.brookings.edu/research/the-case-for-ai-transparency-requirements/, en anglais, consulté le 2 avril 2020

[27] Déclaration universelle des droits de l'homme, consulté le 2 avril 2020, https://www.un.org/fr/universal-declaration-human-rights/index.html

[28] Pacte international relatif aux droits civils et politiques, *Haut-commissariat des Nations Unies aux droits de l'homme*, consulté le 2 avril 2020, https://www.ohchr.org/FR/ProfessionalInterest/Pages/CCPR.aspx.

qui touche à 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 affectant la vie privée des utilisateurs

P1(a). Accès aux politiques de confidentialité

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

Éléments :

1. **Les politiques de confidentialité** de l'entreprise sont-elles **facilement accessibles** ?

2. Les **politiques relatives à la protection de la vie privée** de l'entreprise sont-elles disponibles dans la ou les langues principales parlées par les utilisateurs dans la juridiction d'origine 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** ?

5. Pour les **écosystèmes d'assistants personnels numériques** : L'entreprise indique-t-elle qu'elle exige que les **skills** proposées dans son **skill 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 principales parlées du marché principal d'exploitation de l'entreprise et s'assurent 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 devrait figurer sur la page d'accueil de l'entreprise ou du service. Sinon, il devrait être situé à un ou deux clics de la page d'accueil, ou bien être accessible depuis un emplacement 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 politiques. Il peut s'agir, entre autres, de fournir des résumés, des conseils ou des directives expliquant la signification des termes, en utilisant des en-têtes de sections, 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 compréhensible.

Sources possibles :

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

P1(b). Accès aux politiques de développement des systèmes algorithmiques

Les **politiques de développement des systèmes algorithmiques** de l'entreprise doivent être **facilement accessibles** et **facilement compréhensibles**.

Éléments :

1. Les **politiques relatives au développement du système algorithmique** de l'entreprise sont-elles **facilement accessibles** ?

2. Les **politiques relatives au développement du système algorithmique** sont-elles disponibles dans la ou les langues principales des utilisateurs.

3. Les **politiques relatives au développement du système algorithmique** sont-elles présentées de manière facilement compréhensible ?

Détails de l'indicateur : Le développement et les tests de systèmes algorithmiques peuvent présenter des risques importants pour la vie privée, en particulier lorsque les entreprises utilisent ensuite les informations recueillies sur les utilisateurs pour développer, former, et tester ces systèmes sans le consentement éclairé[29] de la personne concernée. Les entreprises doivent clairement indiquer leurs politiques en décrivant le développement et les tests relatifs aux systèmes algorithmiques. Elles doivent être accessibles et facilement compréhensibles afin que les utilisateurs prennent des décisions éclairées quant à leur utilisation des produits ou services de l'entreprise.

Sources possibles :
- Politiques relatives à l'utilisation de systèmes algorithmiques
- Directives pour le développement de systèmes algorithmiques
- Politique de confidentialité ou politiques des données

P2 : Notification des modifications

P2(a). Modifications apportées à la politique de confidentialité

L'entreprise doit **indiquer clairement** que les utilisateurs sont **directement notifiés** lorsqu'elle modifie ses **politiques de confidentialité** avant que ces modifications n'entrent en vigueur.

Éléments :

[29] Zuboff, S. (2019). The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power. New York, NY, USA: PublicAffairs; Nathalie Maréchal. Targeted Advertising Is Ruining the Internet and Breaking the World, https://www.vice.com/en_us/article/xwjden/targeted-advertising-is-ruining-the-Internet-and-breaking-the-world, *Vice Motherboard,* November 16, 2018; "Human Rights Risk Scenarios: Algorithms, machine learning and automated decision-making," *Ranking Digital Rights*, July 2019, https://rankingdigitalrights.org/wp-content/uploads/2019/07/Human-Rights-Risk-Scenarios_-algorithms-machine-learning-automated-decision-making.pdf.

1. L'entreprise **indique-t-elle clairement** qu'elle **notifie directement** les utilisateurs des changements apportés à ses **politiques de protection de la vie privée** ?

2. L'entreprise **indique-t-elle clairement** comment elle procède pour **notifier directement** les **utilisateurs** de ces changements ?

3. L'entreprise **indique-t-elle clairement** le délai dans lequel elle **notifie directement** les **utilisateurs** de modifications avant l'entrée en vigueur de ces changements ?

4. L'entreprise possède-t-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** ?

6. Pour les **écosystèmes d'assistants personnels numériques** : L'entreprise **indique-t-elle clairement** qu'elle exige que les **skills** vendues par l'intermédiaire de son **skill 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 d'information 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 la création d'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 visible sur la page principale d'accueil du site Internet ou la plateforme d'accès au service. Cet indicateur vise à déterminer si une entreprise fournit des documents publics 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

P2(b). Modifications apportées aux politiques de développement du système algorithmique

L'entreprise doit **indiquer clairement** que les **utilisateurs** sont **directement informés** lorsqu'elle modifie ses **politiques relatives au développement de système algorithmique** avant que ces modifications n'entrent en vigueur.

Éléments :

1. L'entreprise **indique-t-elle clairement** qu'elle informe directement les utilisateurs de tout changements relatifs aux politiques de développement de système algorithmique privé ?

2. L'entreprise **indique-t-elle clairement** comment elle procède pour **notifier directement** les utilisateurs de ces changements ?

3. L'entreprise **indique-t-elle clairement** le délai dans lequel elle **notifie directement** les utilisateurs de modifications avant l'entrée en vigueur de ces changements ?

4. L'entreprise possède-t-elle des **archives publiques** ou un **journal des modifications** ?

Détails de l'indicateur : Les entreprises peuvent modifier leurs politiques relatives au développement de systèmes algorithmique au fur et à mesure que leurs activités évoluent. Toutefois, ces changements peuvent avoir une incidence sur le droit à la vie privée des utilisateurs. Nous attendons donc des entreprises qu'elles s'engagent à informer les utilisateurs lorsqu'elles modifient leurs politiques et à leur fournir des informations qui les aident à comprendre la signification de ces changements comme le recommande le Conseil de l'Europe dans sa Recommandation sur les impacts des systèmes algorithmiques sur les droits de l'homme (2020).

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 la création d'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 visible sur la page principale d'accueil du site Internet ou la plateforme d'accès au service. Cet indicateur vise à déterminer si une entreprise fournit des documents publics qui contiennent les politiques de confidentialité antérieures afin que le public puisse comprendre leur évolution.

Sources possibles :
- Politiques relatives à l'utilisation d'algorithmes
- Politique de confidentialité ou politiques des données

P3 : Collecte et inférence des données utilisateurs

P3(a). Collecte des données utilisateurs

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

Éléments :

1. L'entreprise **indique-t-elle clairement** les types **d'informations** qu'elle **collecte** sur les **utilisateurs** ?

2. Pour chaque type de **données utilisateurs** **collectées**, 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 ?

6. Pour les **écosystèmes d'assistants personnels numériques** : L'entreprise **indique-t-elle clairement** qu'elle évalue si les **politiques de confidentialité** des **skills** tierces mises à disposition via son **skill store** indiquent les **données utilisateurs** que les skills collectent ?

7. Pour les **écosystèmes d'assistants personnels numériques** : L'entreprise **indique-t-elle clairement** qu'elle évalue si les **skills** tierces mises à disposition via son **skill store** limitent la collecte d'**informations sur les utilisateurs** à celles directement pertinentes et nécessaires pour atteindre l'objectif de la skill ?

Détails de l'indicateur : Les entreprises recueillent 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 donc 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 et les écosystèmes d'assistants personnels numériques, nous attendons des entreprises qu'elles indiquent clairement si les politiques de confidentialité des applications ou des skills disponibles dans leur app store ou leur skill store spécifient quelles informations sur les utilisateurs les applications collectent et si ces politiques sont conformes aux principes de minimisation des données.

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

P3(b). Inférence des données utilisateurs

L'entreprise doit **indiquer clairement** quelles **données utilisateurs** elle **infère** et comment.

Éléments :

1. L'entreprise **indique-t-elle clairement** tous les types d'informations qu'elle **infère** sur la base des **informations collectées sur les utilisateurs** ?

2. Pour chaque type de **données utilisateurs** inférées, l'entreprise indique-t-elle clairement la façon dont les informations sont inférées ?

3. L'entreprise **indique-t-elle clairement** qu'elle limite l'**inférence des données utilisateurs** aux informations directement pertinentes et nécessaires pour atteindre l'objectif de son service ?

Détails de l'indicateur : En plus de la collecte d'informations sur les utilisateurs, les entreprises effectuent également des analyses approfondies de données permettant de faire des déductions (aussi appelé inférences) ou des prévisions sur les utilisateurs, sur la base des informations collectées. Ces méthodes peuvent être utilisées pour faire des déductions sur les préférences ou les attributs des utilisateurs (comme la race, le sexe, l'orientation sexuelle), leurs opinions (y compris les opinions politiques) ou pour prédire les comportements des consommateurs. Sans une transparence suffisante et un contrôle par les utilisateurs sur l'inférence des données, les inférences portant atteinte à la vie privée et non vérifiables ne peuvent être prévues, comprises ou réfutées par les utilisateurs. [30]

Les entreprises doivent préciser les informations collectées, et indiquer également quelles informations elles en déduisent et comment elles les infèrent. Elles doivent aussi s'engager à n'inférer que les informations pertinentes et nécessaires pour fournir leur service. Par exemple, les entreprises ne doivent pas essayer de déduire la religion, l'orientation sexuelle ou l'état de santé de leurs utilisateurs (par exemple en les classant dans une catégorie de de population en fonction de cette caractéristique) à moins que ces informations ne soient directement nécessaires pour atteindre l'objectif de leur service.

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. L'entreprise indique-t-elle clairement, pour chaque type de **données utilisateurs** collectées, si celles-ci sont **partagées** ?

[30] Pour plus d'informations, consultez « A Right to Reasonable Inferences: Re-Thinking Data Protection Law in the Age of Big Data and AI » par Sandra Wachter et Brent Mittelstadt, 5 octobre 2018. Columbia Business Law Review, 2019(2), https://ssrn.com/abstract=3248829. Disponible en anglais.

2. Pour chaque type de **données utilisateurs** partagées, l'entreprise **indique-t-elle clairement** avec qui ces informations sont **partagées** ?

3. L'entreprise **indique-t-elle clairement** qu'elle peut **partager** des **données utilisateurs** avec des gouvernements ou des autorités judiciaires ?

4. Pour chaque type d'**informations sur les utilisateurs** que l'entreprise **partage**, l'entreprise **indique-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** précisent quelles **données utilisateurs** 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** ?

7. Pour les **écosystèmes d'assistants personnels numériques** : L'entreprise **indique-t-elle clairement** qu'elle évalue si les **politiques de confidentialité** des **skills** tierces mises à disposition via le **skill store** précisent quelles informations sont partagées par les **skills** ?

8. Pour les **écosystèmes d'assistants personnels numériques** : L'entreprise **indique-t-elle clairement** qu'elle évalue si les **politiques de confidentialité** des **skills** **tierces** mises à disposition via son **skill store** précisent 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, depuis les informations personnelles des profils de nos comptes jusqu'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 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. Les entreprises des écosystèmes d'assistant numériques personnels doivent exiger que les skills de tiers mises à disposition dans leur skills *store* indiquent clairement les types d'informations utilisateurs qui sont partagées, les types de tiers avec lesquels elles les partagent.

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, de l'inférence et du partage des données utilisateurs

L'entreprise doit **indiquer clairement** pourquoi elle **collecte**, **infère** et **partage** les **données utilisateurs**.

Éléments :

1. Pour chaque type **d'informations sur les utilisateurs** que l'entreprise **collecte**, l'entreprise **indique-t-elle clairement** l'objet de la **collecte** ?

2. Pour chaque type de **données utilisateurs inférées**, l'entreprise **indique-t-elle clairement** pourquoi ces informations sont **inférées** ?

3. L'entreprise **indique-t-elle clairement** si elle rassemble des **informations sur les utilisateurs** provenant de ses différents services et, le cas échéant, pourquoi elle procède ainsi ?

4. Pour chaque type **d'information sur les utilisateurs** que l'entreprise **partage**, l'entreprise **indique-t-elle clairement** le motif du **partage** ?

5. L'entreprise **indique-t-elle clairement** qu'elle limite son utilisation des **données utilisateurs** aux fins pour lesquelles elles ont été **collectées** ou **inférées** ?

Détails de l'indicateur: Nous attendons des entreprises qu'elles communiquent clairement le but de la collecte, du partage et de l'inférence de chaque type de données utilisateurs qu'elles recueillent, partagent et infèrent. De plus, de nombreuses entreprises possèdent ou exploitent différents produits et services. Nous attendons d'elles qu'elles indiquent clairement comment les renseignements sur les utilisateurs peuvent être partagés ou groupés entre leurs différents services. Les entreprises doivent aussi s'engager publiquement à respecter le principe de limitation de l'utilisation, ce qui signifie qu'elles déclarent dans les documents publics sur leurs politiques qu'elles n'utilisent les données qu'aux fins spécifiées, en accord avec les lignes directrices de l'OCDE en matière de protection de la vie privée, avec le RGPD, et autres guides de conduite sur les informations qu'elles collectent et également celles qu'elles infèrent.

Sources possibles :

- Politique de confidentialité de l'entreprise

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 **indique-t-elle clairement** le processus de **dépersonnalisation** des **renseignements recueillis 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 sur les utilisateurs** sont effacées lorsque ceux-ci suppriment leur compte ou l'**application** ?

8. Pour les **écosystèmes d'assistants personnels numériques**: L'entreprise **indique-t-elle clairement** qu'elle vérifie si les **politiques de confidentialité** des **skills tierces** disponibles dans son **skill store** spécifient combien de temps elles conservent les **informations des utilisateurs** ?
9. Pour les **écosystèmes d'assistants personnels numériques** : L'entreprise **indique-t-elle clairement** qu'elle vérifie si les **politiques de confidentialité** des **skills tierces** disponibles dans son **skill store** spécifient que toutes les informations des utilisateurs sont effacées lorsqu'ils suppriment leur compte ou la **skill** ?

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 communiquer ces contraintes juridique 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 le perfectionnement croissant des pratiques de réidentification, 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 et les écosystèmes d'assistants numériques personnels (PDA), nous attendons des entreprises qu'elles indiquent si les politiques de confidentialité des applications et des skills disponibles dans leur boutique spécifient combien de temps l'application ou la skill conserve les informations des utilisateurs et si toutes les informations des utilisateurs sont supprimées lorsqu'ils suppriment leur compte, l'application ou la skill.

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

P7. Contrôle des utilisateurs sur leurs propres informations

L'entreprise doit **indiquer clairement** aux **utilisateurs** quelles **options ils ont pour contrôler** la **collecte, l'inférence, la rétention** et l'utilisation de leurs **données utilisateurs** par l'entreprise.

Éléments :

1. Pour chaque type de **données utilisateurs** que l'entreprise **collecte**, indique- t-elle clairement si les utilisateurs peuvent contrôler la collecte de cette information ?

2. Pour chaque type de **données utilisateurs** que l'entreprise **collecte**, **indique- t-elle clairement** si les **utilisateurs** peuvent supprimer les **informations** en question ?

3. Pour chaque type de **données utilisateurs** que l'entreprise **infère** à partir des **informations collectées**, **indique- t-elle clairement** si les **utilisateurs** peuvent contrôler l'**inférence** de cette **information** par l'entreprise ?

4. Pour chaque type de **données utilisateurs** que l'entreprise **infère** à partir des **informations collectées**, **indique- t-elle clairement** si les **utilisateurs** peuvent supprimer cette **donnée utilisateur** ?

5. L'entreprise **indique-t-elle clairement** qu'elle offre aux **utilisateurs** des **possibilités pour contrôler** comment leurs **informations utilisateurs** sont utilisées pour la **publicité ciblée** ?

6. L'entreprise **indique-t-elle clairement** que la **publicité ciblée** est désactivée par défaut ?

7. L'entreprise **indique-t-elle clairement** qu'elle fournit aux **utilisateurs** des **options pour contrôler** comment leurs **données utilisateurs** sont utilisées pour le **développement des systèmes algorithmiques** ?

8. L'entreprise **indique-t-elle clairement** si elle utilise par défaut ou non les **données utilisateurs** pour développer des **systèmes algorithmiques** ?

9. Pour les **écosystèmes mobiles** et les **écosystèmes d'assistants personnels numériques** : L'entreprise **indique-t-elle clairement** qu'elle fournit aux **utilisateurs** des **options de contrôle** des 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, conservent et infèrent 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 avoir à 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 de publicités ciblées ou de développement de systèmes algorithmiques. La publicité ciblée exige la collecte, la conservation et l'inférence d'une quantité considérable d'informations sur les utilisateurs. 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 et les écosystèmes d'assistants personnels numériques, 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 et des écosystèmes d'assistants personnels numériques peuvent influer sur la façon dont d'autres produits et services accèdent aux données de localisation. Par exemple, les applications mobiles ou les skills des assistants numériques peuvent permettre aux utilisateurs de contrôler leurs informations de localisation. Toutefois, si les appareils sur lesquels ces applications mobiles ou ces skills 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 ou par les skills. 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, tableau de bord de gestion de la vie privée
- Centre d'aide de l'entreprise

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 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. L'entreprise **indique-t-elle clairement** que les **utilisateurs** peuvent accéder à la liste des catégories publicitaires **de publics-cibles** auxquelles l'entreprise les a affectés ?

6. L'entreprise **indique-t-elle clairement** que les **utilisateurs** peuvent obtenir l'intégralité des données que l'entreprise a **inférées** à leur sujet ?

7. 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** les concernant détenues par l'**application** ?

8. Pour les **écosystèmes d'assistants personnels numériques** : L'entreprise **indique-t-elle clairement** qu'elle évalue si les **politiques de confidentialité** des **skills tierces** disponibles dans son **skill store** indiquent que les **utilisateurs** peuvent obtenir toutes les **informations** les concernant détenues par la **skill** ?

Détails de l'indicateur : Les utilisateurs doivent être en mesure d'obtenir toutes les informations internes et publiques que les entreprises détiennent à leur sujet, y compris les informations qu'une entreprise a utilisées pour faire des déductions ou des prédictions 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 de connexion et les formats dans lesquels ils peuvent les obtenir. Les entreprises doivent également permettre aux utilisateurs d'accéder à la liste des catégories de publicités qui leur ont été attribuées. Afin de cibler les publicités, les entreprises attribuent généralement à chaque utilisateur un nombre quelconque de catégories d'audience. Les annonceurs peuvent ensuite sélectionner les catégories d'audience qu'ils souhaitent cibler. Les utilisateurs doivent être en mesure de savoir dans quelles catégories d'audiences l'entreprise les a affectés, sur la base des informations recueillies ou déduites par l'entreprise sur les utilisateurs.

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 qu'une application détient à leur sujet. Nous attendons des entreprises qui opèrent les skill stores pour assistants personnels numériques qu'elles fixent des normes minimales auxquelles doivent répondre les skills tierces proposées par leur plateforme. Tout comme nous attendons des entreprises qu'elles indiquent elles-mêmes que les utilisateurs peuvent obtenir de leur part un enregistrement de leurs propres données utilisateurs, les skill stores devraient exiger des skills disponibles dans leur magasin qu'elles fournissent les mêmes possibilités.

Sources possibles :
- Politique de confidentialité de l'entreprise
- Paramètres du compte utilisateur

- Centre d'aide de l'entreprise
- Articles de blog de l'entreprise

P9. Collecte de données utilisateurs par des tiers.

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

Éléments :

1. (Pour les **plateformes numériques**) L'entreprise **indique-t-elle clairement** quelles **informations sur les utilisateurs** elle recueille par des **moyens techniques** depuis des sites tiers ?

2. (Pour **les plateformes numériques**) L'entreprise **indique-t-elle clairement** comment elle recueille les **informations sur les utilisateurs** auprès de **tiers** par des **moyens techniques** ?

3. (Pour les **plateformes numériques**) 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. (Pour les **plateformes numériques**) 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 ?

6. L'entreprise **indique-t-elle clairement** quelles **données utilisateurs** elle collecte par des **moyens non-techniques** auprès de **tiers**?

7. L'entreprise **indique-t-elle clairement** comment elle collecte des **données utilisateurs** par des **moyens non-techniques** auprès de **tiers** ?

8. L'entreprise **indique-t-elle clairement** les raisons pour lesquelles elle collecte des **informations sur les utilisateurs** par des **moyens non-techniques** auprès de **tiers**?

9. L'entreprise **indique-t-elle clairement** le temps pendant lequel elle conserve les **informations sur les utilisateurs** qu'elle collecte par des **moyens non-techniques** auprès de **tiers**?

Détails de l'indicateur : Nous attendons des entreprises qu'elles indiquent clairement quelles informations elles collectent sur les utilisateurs auprès de tiers, que ce soit les informations collectées sur des sites Internet tiers ou des applications tierces par des moyens techniques tels que des cookies, des extensions ou des widgets, ou par des moyens non-techniques comme des accords contractuels. Les entreprises peuvent également acquérir des données utilisateurs par des moyens non-techniques notamment grâce à des accords. Ces données ainsi acquises peuvent faire partie d'un « dossier numérique » que les entreprises détiennent sur leurs utilisateurs, pouvant ensuite servir de base au partage ou à l'inférence de données utilisateurs. Les entreprises doivent faire preuve de transparence et de responsabilité concernant ces pratiques afin que les utilisateurs puissent comprendre si

et comment leurs activités sont suivies par les entreprises, même hors du site Internet de l'entreprise hôte ou lorsqu'ils visitent une plateforme ou un service particulier dont ils ne sont pas utilisateurs enregistrés.

Sources possibles :
- Politique de confidentialité de l'entreprise
- Politique de l'entreprise à l'égard des tiers ou politiques relatives aux cookies.

P10. Processus de réponse aux demandes de données utilisateurs

P10(a). Processus de réponse aux demandes gouvernementales

L'entreprise doit **indiquer clairement** ses processus de réponse aux **demandes gouvernementales d'informations sur les utilisateurs**.

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. Les explications de l'entreprise **indiquent-elles clairement** la base juridique sur laquelle elle peut accéder aux **demandes émanant de gouvernements** ?

5. 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 ?

6. L'entreprise s'engage-t-elle à refuser d'accéder aux **demandes gouvernementales** inappropriées ou excessives ?

7. L'entreprise fournit-elle des **indications claires** ou des exemples pour expliquer l'application de sa procédure de réponse aux **demandes gouvernementales** ?

Détails de l'indicateur : Les entreprises sont de plus en plus sollicitées par les gouvernements pour fournir des informations sur les utilisateurs. Ces demandes peuvent émaner d'organismes gouvernementaux ou de tribunaux (nationaux ou étrangers). Nous attendons des entreprises qu'elles communiquent publiquement leurs procédures de réponse à chaque type de demande gouvernementales ainsi que les raisons pour lesquelles elles se conforment le cas échéant à ces demandes. Les entreprises doivent également s'engager publiquement à refuser d'accéder aux demandes gouvernementales 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. Nos 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 de la législation
- Politique de confidentialité de l'entreprise
- Rapport sur le développement durable de l'entreprise
- Articles de blog de l'entreprise

P10(b). Processus de réponse aux demandes privées

L'entreprise doit **indiquer clairement** ses procédures de réponse aux demandes d'**informations sur les utilisateurs** émanant d'un **processus de demande privé**.

Éléments :

1. L'entreprise **indique-t-elle clairement** sa procédure de réponse aux demandes émises dans le cadre de **procédures privées** ?

2. Les explications de l'entreprise **indiquent-elles clairement** la base juridique sur laquelle elle peut accéder aux **demandes émanant d'un processus privé** ?

3. L'entreprise **indique-t-elle clairement** qu'elle applique une diligence raisonnable lors de l'étude des **demandes émanant d'un processus privé** avant de décider de la façon d'y répondre ?

4. L'entreprise s'engage-t-elle à refuser d'accéder aux demandes inappropriées ou exagérées **émanant d'un processus privé** ?

5. L'entreprise fournit-elle des explications claires ou des exemples pour expliquer l'application de sa procédure de réponse aux **demandes émanant d'un processus privé** ?

Détails de l'indicateur : Les entreprises reçoivent de plus en plus de demandes privées pour fournir des informations sur les utilisateurs. Il s'agit souvent de demandes informelles de données utilisateurs émanant d'une entité non gouvernementale, qui n'impliquent ou ne passent par aucune procédure juridique officielle. Selon la Wikimedia Foundation, qui publie des rapports de transparence avec des données électroniques sur le nombre de demandes qu'elle reçoit ventilées par type, les demandes dites privées concernent notamment les cas où une autre entreprise leur envoie un courrier postal ou un courriel demandant des « informations non publiques » sur l'un de ses utilisateurs. Il peut s'agir de l'adresse IP ou de l'adresse électronique d'un utilisateur.

Cet indicateur attend des entreprises qu'elles indiquent les processus de traitement de ce type de demandes. Les entreprises doivent expliquer les raisons pour lesquelles elles se conforment à ces types de demandes et s'engager à rejeter les demandes trop générales.

Sources possibles :

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

P11. Données relatives aux demandes de données utilisateurs

P11(a). Données relatives aux demandes de données utilisateurs émanant de gouvernement

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

Éléments :

1. L'entreprise indique-t-elle le nombre de **demandes gouvernementales** reçues par pays ?

2. L'entreprise indique-t-elle le nombre de **demandes gouvernementales** 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 gouvernementales** reçues par **ordonnances judiciaires** ?

7. L'entreprise indique-t-elle le nombre de **demandes gouvernementales** auxquelles elle a accédé, ventilé par type de demande ?

8. L'entreprise indique-t-elle les types de **demandes gouvernementales** dont la divulgation lui est interdite par la loi ?

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 sont de plus en plus sollicitées par les gouvernements pour fournir des informations sur les utilisateurs. Ces demandes peuvent émaner d'organismes gouvernementaux ou de tribunaux (nationaux ou étrangers). Nous attendons des entreprises qu'elles publient régulièrement des données sur le nombre et le type de demandes qu'elles reçoivent, ainsi que sur le nombre de demandes auxquelles elles se conforment. Les entreprises doivent publier des données sur les demandes qu'elles reçoivent par pays, y compris les demandes reçues par de leur propre gouvernement et des gouvernements étrangers, ainsi que des services de police et tribunaux. Nous attendons aussi des

entreprises qu'elles indiquent le nombre de comptes concernés par ces demandes et qu'elles ventilent par catégorie les demandes auxquelles elles ont répondu. Nous avons conscience que les entreprises ne sont parfois pas autorisées légalement à divulguer les demandes d'informations formulées par les gouvernements. Toutefois, dans de tels cas, nous attendons des entreprises qu'elles indiquent les types de demandes gouvernementales qu'elles ne sont pas autorisées à divulguer. Elles doivent également publier ces données une fois par an et s'assurer que ces données peuvent être exportées sous la forme d'un fichier 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
- Rapport de l'entreprise sur l'application de la législation
- Rapport de développement durable de l'entreprise

P11(b). Données relatives aux demandes de données utilisateurs émanant d'un processus privé

L'entreprise doit publier régulièrement des données sur les demandes de **données utilisateurs** **émanant d'un processus privé**.

Éléments :

1. L'entreprise indique-t-elle le nombre de demandes de **données utilisateurs** reçues émanant d'un **processus privé** ?
2. L'entreprise indique-t-elle le nombre de demandes de **données utilisateurs** émanant d'un **processus de demandes privées** auxquelles elle a accédé ?
3. L'entreprise communique-t-elle ces données au moins une fois par an ?
4. 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 de plus en plus de demandes privées d'informations sur les utilisateurs. Il s'agit souvent de demandes informelles de données utilisateurs émanant d'une entité non gouvernementale, qui n'impliquent ou ne passent par aucune procédure juridique officielle. Selon la Wikimedia Foundation, qui publie des rapports de transparence avec des données électroniques sur le nombre et les types de demandes qu'elle reçoit, les demandes privées concernent notamment les cas où une autre entreprise leur adresse une lettre ou un courriel demandant des « informations non publiques » sur l'un des utilisateurs. Il peut s'agir de l'adresse IP ou de l'adresse électronique d'un utilisateur.

Tout comme les entreprises doivent publier des données sur les demandes reçues de gouvernements, requérant des données utilisateurs, elles doivent aussi publier des données sur les demandes d'informations qu'elles reçoivent (et auxquelles elles se conforment) émanant d'un processus privé. Nous attendons des entreprises qu'elles publient régulièrement des données sur le nombre et le type de telles demandes reçues et sur le nombre de demandes auxquelles elles accèdent. Les entreprises doivent également publier ces données une fois par an et s'assurer qu'elles peuvent être exportées dans un fichier de données structuré.

Sources possibles :
- Rapport sur la transparence de l'entreprise
- Rapport de développement durable de l'entreprise
- Rapport sur la responsabilité sociale de l'entreprise

P12. Notification des utilisateurs à propos des demandes de données provenant de tiers

Dans la mesure où cela est juridiquement possible, l'entreprise devrait **notifier** les utilisateurs, lorsque leurs **données personnelles** sont **exigées 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** lorsqu'elle reçoit des **demandes informations** à leur sujet via des **demandes privées** ?

3. L'entreprise **indique-t-elle clairement** les situations où elle pourrait ne pas aviser les utilisateurs, y compris une description des types de **demandes gouvernementales** qu'il 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 eux. Nous reconnaissons que cette information ne peut pas être communiquée dans des cas légitimes comme une enquête en cours. Toutefois, nous attendons des entreprises qu'elles précisent le type de demandes gouvernementales que la loi leur interdit de divulguer.

Sources possibles :
- Rapport sur la transparence de l'entreprise
- Directives de l'entreprise relatives à l'application de la législation
- Politique de confidentialité de l'entreprise
- Politique de l'entreprise en matière de droits de l'homme

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 de leurs 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 traiter les **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** et **écosystèmes d'assistants personnels numériques** : 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 son système d'exploitation mobile ?

6. Pour les **écosystèmes mobiles, les écosystèmes d'assistants personnels numériques** 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** et les **entreprises de télécommunications** : 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** et les **écosystèmes d'assistants personnels numériques** : L'entreprise s'engage-t-elle à fournir des **mises à jour de sécurité** pour le système d'exploitation et d'autres logiciels indispensables pendant au moins cinq ans après leur commercialisation ?

9. Pour les **écosystèmes mobiles**, les **assistants personnels numériques** 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 publique d'une faille de sécurité ?

10. Pour les **écosystèmes d'assistants personnels numériques** : L'entreprise **indique-t-elle clairement**, le cas échéant, quelles modifications ont été apportées au **système d'exploitation** d'assistants personnels numériques ?

11. Pour les **écosystèmes d'assistants personnels numériques** : 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** ?

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 y remédier. Il s'agit notamment de s'assurer que les personnes sont en mesure de signaler à l'entreprise les failles qu'elles découvrent. Nous pensons qu'il est particulièrement important pour les entreprises de fournir aux utilisateurs des politiques 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 procédures 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 **atteintes 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 **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** de 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 de façon intelligible. Les atteintes à la protection des données dévoilent des informations personnelles et 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 personnelles 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 utilisateurs et des contenus privés (plateformes numériques)

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 leurs contenus privés à l'aide d'un **chiffrement de bout en bout** ou d'un **chiffrement complet du disque** (lorsque cela 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. [31] 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 que cette option est activée 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 générales 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 (plateformes numériques)

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.

[31] « Rapport sur le chiffrement, l'anonymat et le cadre juridique », Haut-Commissaire des Nations Unies aux droits de l'homme, en anglais, consulté le 2 avril 2020. https://www.ohchr.org/en/issues/freedomopinion/pages/callforsubmission.aspx

Sources possibles :
- Centre de sécurité de l'entreprise
- Pages d'aide de l'entreprise ou pages de support communautaire
- Page du site de l'entreprise relative aux paramètres du compte utilisateur
- 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**.

Éléments :

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 : Les entreprises détiennent une immense quantité de données sur les utilisateurs et peuvent par conséquence souvent être la cible d'actes 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, sur la façon d'éviter les attaques par des logiciels malveillants, des techniques d'hameçonnage ou d'ingénierie sociale, sur la façon d'éviter ou de répondre au harcèlement ou à l'intimidation en ligne ainsi que des explications concernant la « navigation sécurisée ». Les entreprises doivent dispenser ces conseils dans un langage clair, idéalement accompagné de visuels, 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 tous les utilisateurs.

Sources possibles :
- Centre de sécurité de l'entreprise
- Pages d'aide de l'entreprise ou pages 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 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).

action de modération de contenu : pratique consistant à filtrer le contenu généré par des utilisateurs et publié sur des sites Internet, des médias sociaux et d'autres supports en ligne, afin de déterminer sa pertinence pour un site, une localité ou une juridiction donnée. Le processus peut aboutir au retrait ou à la restriction du contenu par un modérateur, agissant en tant qu'agent de la plateforme ou du site en question. De plus en plus, les entreprises s'appuient sur des systèmes algorithmiques en plus des modérateurs humains pour modérer le contenu et les informations sur leurs plateformes.
Source : *« Content moderation »,* Encyclopedia of Big Data, en anglais, *https://doi.org/10.1007/978-3-319-32001-4_44-1*.

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 un résultat basé 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 (en anglais) : *https://datasociety.net/wp-content/uploads/2018/04/Data_Society_Algorithmic_Accountability_Primer_FINAL-4.pdf*.

annonceur : personne ou entité qui crée ou paye pour la diffusion d'un contenu publicitaire. Il détermine généralement les paramètres de ciblage pour chaque publicité.

app store : plateforme sur laquelle une entreprise donne accès à ses propres applications ainsi qu'à 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 portatif / 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.

appel : dans le cadre de l'Index RDR, un « appel » est un processus par lequel les utilisateurs demandent un changement formel suite à une décision de modération de contenu ou de restriction de compte prise par une entreprise.

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

archive publique : ressource accessible au grand 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.

archives publiques tierces : en principe, les entreprises publient des informations sur les demandes qu'elles reçoivent afin que le public comprenne mieux comment le contenu est restreint sur la plateforme. Les entreprises peuvent fournir des informations sur les demandes qu'elles reçoivent à des archives tierces, comme Lumen (anciennement appelé Chilling Effects). Lumen est un projet de recherche indépendant qui gère une base de données publique de demandes de retrait de contenus en ligne. Ce type de dépôt aide les chercheurs et le public à comprendre les types de contenu dont le retrait est demandé, ainsi qu'à mieux comprendre et distinguer les demandes légitimes et illégitimes. Voir : *https://cyber.harvard.edu/research/lumen*.

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 destinée à ses utilisateurs au sujet d'un élément en rapport avec l'entreprise ou un service.

bot : compte en ligne automatisé dont la totalité ou la quasi-totalité des actions ou des messages ne sont pas le fait d'une personne.

botnet : réseau coordonné de bots agissant de concert, généralement parce qu'ils sont sous le contrôle d'une même personne ou d'une même entité.

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.

catégorie de public (pour la publicité) : groupe identifié d'utilisateurs pour diffuser des publicités ciblées. Les utilisateurs de ce groupe partagent certaines caractéristiques et/ou intérêts, déterminés sur la base d'informations utilisateurs qu'une entreprise a collectées ou déduites.

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 : procédé permettant de cacher 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://fr.wikipedia.org/wiki/Chiffrement (français), https://www.explainthatstuff.com/encryption.html (anglais)

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. Les 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 une personne malveillante obtient une clé de chiffrement, elle n'est toujours 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).

contenu publicitaire : tout contenu payé par quelqu'un à une entreprise pour qu'elle l'affiche à ses utilisateurs.

cookie(s) : « Les cookies (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 (en français) : https://ssd.eff.org/fr/glossary/t%C3%A9moins https://ssd.eff.org/en/glossary/cookies

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 non judiciaire : demande provenant d'entités gouvernementales qui ne sont 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 non judiciaires d'un gouvernement.

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 distribués sur le magasin en ligne 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.

discrimination : Dans le cadre de l'Index RDR, la discrimination est définie comme le fait de distinguer et de traiter différemment (le plus souvent plus mal) une personne, une entreprise, des produits par rapport au reste de la collectivité ou par rapport à une autre personne. Source : dictionnaire Larousse.

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.

documents structurés (de politiques et conditions) : Conditions d'utilisation et politiques de confidentialité organisées en sections avec hyperliens, permettant aux utilisateurs de naviguer directement vers la section qu'ils souhaitent consulter.

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 souvent plutôt de données « 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 fondamental. 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 fusionner plusieurs sources de données pour révéler des renseignements sur les utilisateurs. Ainsi, des acteurs avec outils sophistiqués peuvent utiliser des données qui semblent anonymes pour dessiner une image plus détaillée 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 traditionnels de base de données, 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*

écosystème d'assistants numériques personnels : Un écosystème d'assistants numériques personnels (PDA, pour Personnel Digital Assistant) consiste en une interface alimentée par une intelligence artificielle installée sur des appareils numériques. Elle peut interagir avec les utilisateurs par texte ou voix pour accéder à des informations sur Internet et effectuer certaines tâches en utilisant des données personnelles partagées par les utilisateurs. Les utilisateurs peuvent interagir avec ces écosystèmes PDA grâce à des skills, mises à disposition par des développeurs/fournisseurs tiers ou par le PDA lui-même.

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 : interactions entre l'entreprise et les parties prenantes. Les entreprises ou les parties prenantes peuvent initier ces interactions, qui peuvent prendre différentes formes (réunions, autres formes de communication, etc.)

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://media.business-humanrights.org/media/documents/files/media/documents/ruggie/ruggie-guiding-principles-21-mar-2011.pdf

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

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 compréhensible.

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, l'échange 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 cet 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. Source :

https://apps.fcc.gov/edocs_public/attachmatch/FCC-15-24A1.pdf.

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.

inférence des données : Les entreprises sont en mesure de déduire des informations et de faire des prévisions sur les comportements, les préférences et la vie privée de leurs utilisateurs en utilisant des techniques d'analyse de données massives et des technologies de prise de décision algorithmique. Ces méthodes peuvent être utilisées pour faire des déductions (aussi appelées inférences) sur les préférences ou les attributs des utilisateurs (la race, le sexe, l'orientation sexuelle par exemple), et les opinions (opinions politiques par exemple), ou pour prédire des comportements (pour présenter des publicités par exemple). Sans une transparence et un contrôle suffisants accordées à l'utilisateur sur l'inférence des données, les inférences portant atteinte à la vie privée et non vérifiables ne peuvent être prévues, comprises ou réfutées par les utilisateurs. Voir : Wachter, Sandra et Mittelstadt, Brent. "*A Right to Reasonable Inferences" : Re-Thinking Data Protection Law in the Age of Big Data and AI*", Columbia Business Law Review, 2019(2), https://ssrn.com/abstract=3248829.

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. Plus précisément, 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 et uniquement lorsqu'elles sont agrégées comme base pour générer des mesures globales (par exemple, le nombre d'utilisateurs mensuels actifs). La déclaration « Notre service compte un million d'utilisateurs actifs par mois » contient donc des données anonymes, car elle ne donne pas suffisamment d'informations pour identifier ces utilisateurs.

informations utilisateurs collectées : informations sur les utilisateurs qu'une entreprise observe directement ou acquiert auprès d'un tiers.

initiative multipartite : une organisation multipartite crédible comprend et est dirigée par des membres d'au moins trois autres groupes de parties prenantes en plus du secteur concerné : 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 à, exécutent ou imitent des fonctions qui sont généralement considérées comme nécessitant une intelligence. Nous pouvons citer en exemples 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 d'une politique de confidentialité).

limitation (de bande passante) : aussi appelée « throttling », forme brutale de régulation du trafic par 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.

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 s'astreindre à limiter leur utilisation de ces renseignements pour d'autres fins, 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.

mesure de l'engagement : chiffres décrivant la popularité d'un contenu ou d'un compte sur une plateforme, par exemple le nombre d'abonnés, de connexions, de contacts, d'amis, de commentaires, de mentions « J'aime », de retweets, etc.

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 et 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 non techniques : les entreprises peuvent acquérir des informations sur les utilisateurs par des moyens non techniques, tels que des achats, des accords de partage de données ou toute autre relation contractuelle avec un tiers. Ces données acquises peuvent faire partie d'un « dossier numérique » que les entreprises peuvent détenir sur leurs utilisateurs. Il sert ensuite de base à des informations inférées et partagées sur les utilisateurs

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 utilisateur « aime » ou interagit avec ce contenu.

« ne pas suivre » : connu également 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 « 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). » Voir : 18 U.S. Code § 2703. Required disclosure of customer communications or records, Cornell Law School Legal Information Institute (en anglais) et le Manuel de droit européen en matière de protection des données, Cour européenne des droits de l'homme

notifier directement/notification directe : par notification directe, nous entendons que lorsqu'une entreprise modifie ou actualise ses politiques relatives à un service particulier, nous attendons de celle-ci qu'elle informe directement les utilisateurs via le dit service. Pour les services impliquant des comptes utilisateurs, la notification directe peut se traduire par 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'une notification bien en vue sur la page principale d'accès au service.

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 société 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 du droit à 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.

organiser, recommander et/ou classer : pratique consistant à utiliser des algorithmes, l'apprentissage automatique et d'autres systèmes décisionnels automatisés pour gérer, façonner et régir le flux de contenus et d'informations sur une plateforme, généralement de manière personnalisée pour chacun des utilisateurs.

paramètres de ciblage : conditions, généralement fixées par l'annonceur, déterminant quels utilisateurs recevront le contenu publicitaire en question. Il peut s'agir de données démographiques, de la localisation, du comportement, des centres d'intérêts, des connexions ou d'autres informations utilisateurs

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 au quotidien, 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 par BSR, septembre 2014*

pièce d'identité officielle : document officiel avec ou sans photo délivré par un gouvernement et pouvant être utilisé pour prouver l'identité d'une personne. Il peut s'agir d'une pièce d'identité délivrée par le gouvernement ou de toute autre forme de document permettant d'identifier la personne par son lieu de résidence, sa famille ou sa communauté. Cela inclut

également les numéros de téléphone qui, dans de nombreuses juridictions, sont liés à l'identité hors ligne d'une personne.

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. [1] Pour simplifier, disons qu'il s'agit de la structure sur laquelle les programmes informatiques peuvent fonctionner.

plateformes numériques : Dans le cadre de l'Index RDR, les plateformes numériques désignent une catégorie de l'Index RDR comprenant les entreprises de l'écosystème Internet et mobile, les entreprises exploitant des services de commerce électronique et les écosystèmes d'assistants numériques personnels.

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

politique en matière de bots : documents décrivant les règles d'une entreprise régissant l'utilisation de robots pour générer du contenu, diffuser du contenu ou effectuer d'autres actions. Elle peut faire partie des conditions d'utilisation de l'entreprise ou d'un autre document.

politique de développement des systèmes algorithmiques : documents décrivant les pratiques d'une entreprise en matière de développement et de tests algorithmiques, d'apprentissage automatique et de prise de décision automatisée.

politique relative à la publicité ciblée : documents décrivant les règles d'une entreprise régissant les paramètres de ciblage publicitaire autorisés sur la plateforme.
Politiques relatives à l'utilisation de systèmes algorithmiques - Documents décrivant les pratiques d'une entreprise concernant l'utilisation d'algorithmes, l'apprentissage automatique et la prise de décision automatisée.

politique relative au contenu publicitaire : documents qui décrivent les règles d'une entreprise régissant le contenu publicitaire autorisé sur la plateforme.

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.

procédure privée : demandes présentées dans le cadre d'une procédure privée plutôt que d'une procédure judiciaire ou gouvernementale. Les demandes privées visant à restreindre le contenu ou les comptes peuvent provenir d'un organisme d'autorégulation tel que l'Internet Watch Foundation, ou d'un système de notification et de retrait, tel que le Digital Millennium Copyright Act américain. Pour plus d'informations sur le système de notification et de retrait, ainsi que sur le DMCA en particulier, voir les pages 40 à 52 sur 211 de Fostering Freedom Online : The Role of Internet Intermediaries, en anglais, UNESCO.

Les demandes privées de données d'utilisateurs sont souvent informelles et n'impliquent aucune procédure juridique formelle. Selon la Wikimedia Foundation, qui produit des rapports de transparence qui révèlent des données sur le nombre de ces types de demandes qu'elle reçoit, les demandes privées d'informations sur les utilisateurs comprennent les cas où une

autre entreprise leur envoie une lettre ou un courriel demandant des « informations non publiques » sur l'un de ses utilisateurs. Il peut s'agir de l'adresse IP et du courrier électronique d'un utilisateur.

processus non officiel : processus ou canal par lequel le gouvernement émet des injonctions ou des demandes de restrictions de contenu ou de compte au lieu de processus officiels, tels qu'ordonnés par la loi ou la réglementation. Par exemple, un agent gouvernemental local peut émettre un ordre ou protester sur un certain contenu via un canal informel.

programme « zero-rating » : le « *zero-rating* » désigne la pratique consistant à fournir certains services ou l'accès à des plateformes en ligne sans faire payer les utilisateurs pour les données utilisées. Le *zero-rating* est considéré comme un type de priorisation du réseau portant atteinte au principe de neutralité de l'Internet.

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 : message pour lequel une entreprise a payé une société pour qu'elle l'affiche auprès d'un sous-ensemble de ses utilisateurs, comprenant à la fois un contenu publicitaire et des paramètres de ciblage.

publicité ciblée : également appelée « publicité ciblée par centre 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 des pratiques intensives 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 sur 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. Voir aussi, en français : https://www.ohchr.org/documents/publications/guidingprinciplesbusinesshr_fr.pdf)

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 passante).

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

réseau publicitaire : entreprise ou service mettant en relation des annonceurs avec des sites Internet souhaitant héberger des publicités. La fonction clé d'un réseau publicitaire est l'agrégation de l'offre d'espaces publicitaires proposée par des éditeurs et sa mise en relation avec la demande des annonceurs.

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.

restriction de contenu : mesure prise par une entreprise rendant invisible ou moins visible sur sa plateforme ou son service une instance de contenu publié par un utilisateur. Il peut s'agir d'une suppression intégrale de contenu ou prendre une forme moins absolue, par exemple en le cachant à certains utilisateurs (par exemple, les habitants d'un certain pays ou les personnes d'un certain âge), en limitant la capacité des utilisateurs à interagir avec ce contenu (par exemple, en rendant impossible de réagir via la fonctionnalité « J'aime »), en y ajoutant un contre-discours (par exemple, des informations correctives sur les messages anti-vaccins) ou en réduisant l'amplification fournie par les systèmes de curation de la plateforme.

risques de cybersécurité : 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.

signalement : Processus consistant à alerter une entreprise qu'un élément de contenu ou un compte peut être en infraction avec les règles de l'entreprise, ou signal transmettant cette information à l'entreprise. Ce processus peut se dérouler soit au sein de la plateforme, soit par le biais d'un processus externe. Les signaleurs comprennent les utilisateurs, les systèmes algorithmiques, le personnel de l'entreprise, les gouvernements et d'autres entités privées.

signalement automatisé : signalement provenant d'un système algorithmique. Voir aussi : signalement par un individu.

signalement par un individu : signalement provenant d'un être humain (utilisateur, employé ou prestataire d'une entreprise, employé ou agent du gouvernement, ou employé ou représentant d'une entité privée). Voir aussi : signalement automatisé.

signaleur : personne ou entité alertant une entreprise qu'un contenu ou un compte peut enfreindre le règlement de l'entreprise. Ce processus peut se dérouler soit au sein de la plateforme, soit par le biais d'un processus externe. Les signaleurs comprennent les utilisateurs, les systèmes algorithmiques, le personnel de l'entreprise, les gouvernements et d'autres entités privées.

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 définisse l'option de retrait. De plus, certaines entreprises peuvent exiger qu'un utilisa-

teur installe un module d'extension de navigateur pour empêcher le suivi. Ces deux scénarios illustrent 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.

skill : les skills sont des capacités d'assistant numérique personnel à commande vocale permettant aux utilisateurs d'effectuer certaines tâches ou de s'engager dans des contenus en ligne à l'aide d'appareils équipés d'un assistant numérique personnel. Les skills de l'écosystème des assistants numériques personnels sont similaires aux applications de l'écosystème mobile : les utilisateurs peuvent activer ou désactiver des skills intégrées ou installer des skills développées par des tiers par l'intermédiaire de magasins similaires aux magasins d'applications.

skill store : plateforme par laquelle une entreprise met à disposition ses propres skills (compétences) ainsi que celles créées par des développeurs tiers, disponibles au téléchargement. Un skill store (ou marché de compétences) est un type de plateforme de distribution numérique de logiciels informatiques.

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 algorithmique : système qui utilise des algorithmes, l'apprentissage automatique et/ou des technologies connexes pour automatiser, optimiser et/ou personnaliser les processus de prise de décision.

système algorithmique de curation, de recommandation et/ou de classement de contenu : système utilisant des algorithmes, de l'apprentissage automatique et d'autres technologies de prise de décision automatisée pour gérer, façonner et régir le flux de contenu et d'informations sur une plateforme, généralement de façon personnalisée pour chacun de ses utilisateurs.

système d'exploitation : logiciel exécutant 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.

technologies publicitaires : Systèmes de prise de décision algorithmiques déterminant quels utilisateurs recevront un contenu publicitaire spécifique. Cette détermination peut prendre en compte les paramètres de ciblage fixés par l'annonceur, ou bien être entièrement automatisée.

tierce partie, 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.

utilisateur affecté : utilisateur ayant publié un contenu restreint par une action de modération ou utilisateur associé à un compte restreint par une action de modération, et s'il y a lieu, le ou les utilisateurs ayant effectué le signalement conduisant à l'examen d'un contenu ou d'un compte pour une action de modération.

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-récidive. 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 cadre de référence « protéger, respecter et réparer » des Nations Unies, *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.