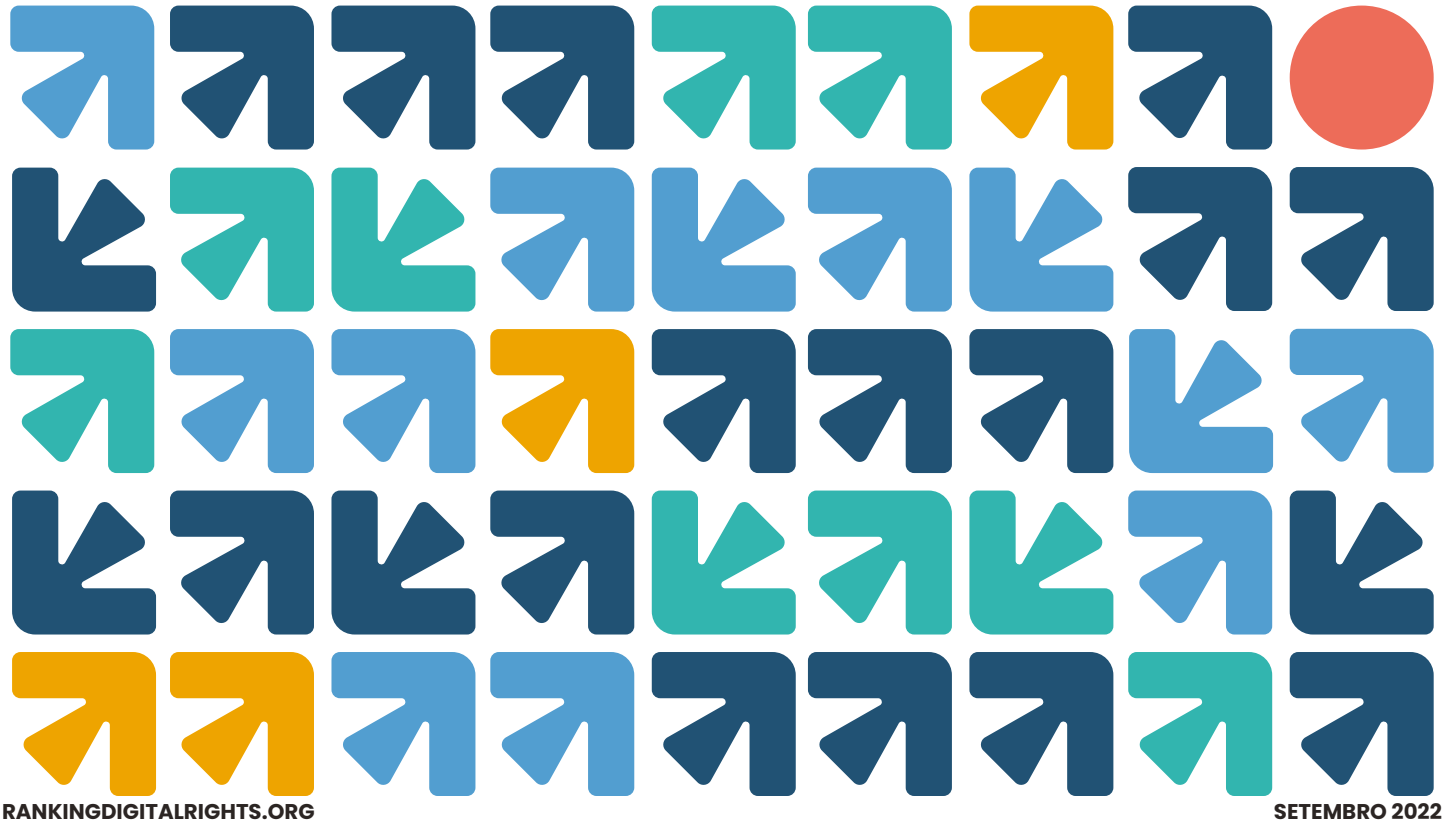
Ranking Digital Rights

2020 Ranking Digital Rights Índice de Responsabilidade Corporativa

Indicadores de pesquisa



Agradecimentos

Os seguintes integrantes da equipe da Ranking Digital Rights participaram da pesquisa e sondagem com as partes interessadas para o desenvolvimento da metodologia do Índice de Responsabilidade Corporativa da RDR:

- Amy Brouillette, Diretora de Pesquisa
- Veszna Wessenauer, Gestora de Pesquisa
- Nathalie Maréchal, Analista Sênior de Políticas
- Afef Abrougui, Analista de Pesquisa
- Zak Rogoff, Analista de Pesquisa
- Jan Rydzak, Líder de Relacionamento Corporativo e Analista de Pesquisa
- Jie Zhang, Analista de Pesquisa

Para uma lista completa da equipe da RDR:

https://rankingdigitalrights.org/who/
A RDR gostaria de agradecer aos mais de 100 atores envolvidos que forneceram feedback crucial durante o desenvolvimento da metodologia. Também gostaríamos de agradecer às ex-integrantes da área de pesquisa da RDR, Laura Reed e Andrea Hackl, por contribuições decisivas durante a fase inicial de expansão da metodologia, que começou em 2019.

Sobre a Ranking Digital Rights

A Ranking Digital Rights é uma iniciativa sem fins lucrativos hospedada no Open Technology Institute da New America, que trabalha com uma rede internacional de parceiros para estabelecer parâmetros globais de respeito à privacidade e à liberdade de expressão entre empresas do setor de tecnologia da informação e comunicação (TIC).

Para mais informações sobre a RDR e seu Índice de Responsabilidade Corporativa, por favor visite www.rankingdigitalrights.org

Para mais informações sobre a New America, por favor visite http://www.newamerica.org

Para mais informações sobre o Open Technology Institute, por favor visite http://www.newamerica.org/oti/

Para uma lista completa de financiadores e parceiros: http://rankingdigitalrights.org/who/partners

Conteúdo

1. Sobre a Ranking Digital Rights

A Ranking Digital Rights (RDR) trabalha para promover a liberdade de expressão e a privacidade na internet, criando parâmetros globais e incentivos para que empresas respeitem e protejam os direitos de seus usuários. Fazemos isso produzindo o Índice de Responsabilidade Corporativa da Ranking Digital Rights (Índice da RDR), o qual avalia as plataformas digitais e empresas de telecomunicação mais poderosas do mundo quanto a compromissos e políticas importantes, baseados em padrões internacionais de direitos humanos. Trabalhamos com empresas, bem como defensores, pesquisadores, investidores e formuladores de políticas públicas para implantar e promover parâmetros globais de responsabilidade corporativa.

O Índice de Responsabilidade Corporativa oferece um caminho para empresas construírem e operarem plataformas e serviços de internet que respeitem os direitos humanos. O Índice de 2019 classificou 24 empresas em 35 indicadores[1], por meio de um rigoroso processo de pesquisa em sete etapas e uma metodologia aberta que examinou os mecanismos de governança adotados pelas empresas para identificar e evitar ameaças em potencial aos direitos humanos de seus usuários, bem como as políticas corporativas que afetam a liberdade de expressão e a privacidade dos usuários.

2. Sobre a metodologia do Índice da RDR

Os parâmetros que o Índice da RDR utiliza para avaliar empresas foram concebidos com base em mais de uma década de trabalho de comunidades de direitos humanos, privacidade e segurança. Esses parâmetros incluem os U.N. Guiding Principles on Business and Human Rights ("Princípios Orientadores da ONU sobre Empresas e Direitos Humanos"), documento elaborado pela Organização das Nações Unidas que afirma que, assim como os governos, as empresas também têm o dever de proteger os direitos humanos. O Índice da RDR baseia-se também nos princípios da Global Network Initiative e suas diretrizes de implementação, as quais tratam das responsabilidades específicas das empresas de TIC em relação à liberdade de expressão e privacidade diante de solicitações de governos para restringir conteúdo ou obter dados de usuários. O Índice também se ampara em um conjunto emergente de parâmetros e normas globais quanto à proteção de dados, segurança e acesso à informação.

A metodologia do Índice da RDR foi desenvolvida ao longo de anos de pesquisa, testes e consultas. Desde a sua concepção, o projeto se engajou profundamente com pesquisadores de todo o mundo. Para o desenvolvimento inicial da metodologia, do estudo piloto e do Índice inaugural, a RDR também se aliou à Sustainalytics, um provedor pioneiro de pesquisa ambiental, social e de governança (Environmental, Social and Governance, ou "ESG") para investidores.

Edições anteriores do Índice da RDR:

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

- Em 2015, lançamos o Índice inaugural, que classificou 16 empresas de internet e telecomunicações a partir de 31 indicadores.

- O Índice da RDR de 2017 expandiu o ranking para 22 empresas, incluindo todas as empresas classificadas em 2015 e seis empresas adicionais. Junto com as empresas de internet e telecomunicações, o Índice incorporou novos tipos de serviços, incluindo aqueles que produzem software e dispositivos do que chamamos de "ecossistemas de dispositivos móveis". Consequentemente, reformulamos ainda mais a metodologia de 2017 com base em revisão detalhada dos dados brutos do Índice de 2015 e em consultas com as partes interessadas da sociedade civil, academia, investidores e empresas.

- O Índice de 2018 usou a mesma metodologia e avaliou as mesmas 22 empresas do Índice de 2017. Isso nos permitiu realizar análises comparativas sobre a performance de cada empresa e identificar tendências gerais.

- A metodologia do Índice de 2019 introduziu mudanças em dois indicadores na categoria Governança[2]. Essas reformulações tiveram como objetivo introduzir parâmetros de linha de base para identificar e mitigar riscos de violações aos direitos humanos associados ao uso de algoritmos e às políticas e práticas de publicidade direcionada das empresas. Também revisamos um indicador (Indicador G6) com o objetivo de fortalecer e explicitar nossa avaliação dos procedimentos de reclamação e de reparação das empresas[3]. Além disso, o Índice de 2019 foi ampliado para incluir duas novas empresas[4] – Deutsche Telekom e Telenor – e cinco serviços de nuvem.

3. Sobre a revisão metodológica do Índice da RDR de 2020

Desde o seu lançamento em 2015, o Índice da RDR tem contribuído para melhorar a divulgação das políticas e práticas das empresas em diversas áreas, incluindo transparência, remoção de conteúdo, restrição de contas, desligamento de rede e tratamento e segurança das informações dos usuários. No entanto, devido aos desdobramentos geopolíticos e tecnológicos que contêm implicações flagrantes para os direitos humanos, ocorridos nos últimos anos desde que a metodologia do Índice da RDR foi criada, ficou evidente que a metodologia precisaria ser revisada para que as empresas sejam efetivamente responsabilizadas pela variedade de ameaças online potenciais aos direitos humanos.

---

[2] "2019 Corporate Accountability Index Research Indicators," (em tradução livre, "Indicadores de pesquisa de responsabilidade corporativa, 2019), *Ranking Digital Rights*, setembro de 2019, https://rankingdigitalrights.org/index2019/assets/static/download/RDRindex2019indicators.pdf

[3] "Proposed revisions to the 2019 Corporate Accountability Index methodology (consultation draft)," (em tradução livre, "Proposta de revisão à metodologia do Índice de Responsabilidade Corporativa de 2019, minuta para consulta)", *Ranking Digital Rights,* julho de 2018, https://rankingdigitalrights.org/wp-content/uploads/2018/06/2019-Index-Methodology_-Consultation-Draft.pdf

[4] Ver a lista de empresas de 2019: https://rankingdigitalrights.org/2019-companies/.

Em janeiro de 2019, a RDR iniciou um processo de expansão e revisão da metodologia para incluir novos temas e novos tipos de empresas[5]. Esse trabalho focou em três temas principais:

- **Aprimoramento da metodologia do Índice da RDR:** Reformulamos a metodologia do Índice de 2019 para identificar temas vitais de revisão e aprimoramento.

- **Incorporação de novos indicadores de publicidade direcionada e algoritmos:** Desde o início de 2019, a RDR tem desenvolvido novos indicadores que estabelecem parâmetros globais de responsabilidade e transparência para que empresas demonstrem respeito pelos direitos humanos online ao desenvolver e implementar essas novas tecnologias. Em outubro de 2019, a RDR publicou minutas de indicadores em publicidade direcionada e algoritmos baseadas em quase um ano de pesquisa interna e incorporando feedback de mais de 90 especialistas. Esses indicadores foram testados pela equipe de pesquisa da RDR. Os resultados foram publicados em março de 2020.

- **Incorporação de novas empresas:** No início de 2019, iniciamos um processo de pesquisa e consulta pública sobre maneiras de expandir o Índice para incluir Amazon e Alibaba. Esse processo deu as bases para incorporar dois novos tipos de serviço – plataformas de e-commerce e "ecossistemas de assistentes pessoais digitais" – na metodologia do Índice da RDR de 2020.

Em abril de 2020, a RDR publicou um rascunho da versão final da metodologia do Índice de 2020, o qual integrou o trabalho feito nessas três áreas[6]. Na sequência, abrimos uma rodada de consultas públicas para solicitar feedback das partes interessadas, que informou as decisões finais sobre a metodologia.

> Para ler um resumo das principais mudanças na metodologia do Índice de 2020:
>
> https://rankingdigitalrights.org/wp-content/uploads/2020/06/2020-methodology-revision-final-summary.pdf

> Para saber mais sobre o processo de desenvolvimento da nossa metodologia:
> https://rankingdigitalrights.org/methodology-development/

[5] "RDR 2019 Index Launch Slated for May; Big Plans Ahead," (em tradução livre, "Índice da RDR de 2019 será lançado em maio: grandes planos à frente"), *Ranking Digital Rights,* fevereiro de 2019, https://rankingdigitalrights.org/2019/02/13/rdr-2019-index-launch-plans/

[6] "2020 Ranking Digital Rights Corporate Accountability Index Draft Indicators," (em tradução livre, Minuta de indicadores do Índice de Responsabilidade Corporativa da Ranking Digital Rights"), *Ranking Digital Rights,* abril de 2020, https://rankingdigitalrights.org/wp-content/uploads/2020/04/2020-draft-methodology-redline-version.pdf

4. Empresas incluídas no Índice da RDR de 2020

O Índice de 2020 vai avaliar 26 empresas, listadas a seguir. Pesquisadores vão examinar políticas e práticas da empresa matriz, além das políticas e práticas divulgadas de alguns de seus serviços e/ou empresas subsidiárias locais (dependendo da estrutura de cada empresa).

Empresas de plataformas digitais: O Índice de 2020 vai avaliar 14 empresas de plataformas digitais. Essas incluem todas as 12 empresas de plataformas digitais avaliadas anteriormente e duas novas empresas (Amazon e Alibaba). Como dito anteriormente, devido à expansão do Índice de 2020 para incluir novos serviços oferecidos pela Amazon e pela Alibaba – especificamente, plataformas de e-commerce e "ecossistemas de assistentes pessoais digitais" –, renomeamos a categoria "internet e ecossistema de dispositivos móveis" como "plataformas digitais", cujo escopo inclui uma gama de produtos e serviços oferecidos por empresas de internet, assim como ecossistemas de dispositivos móveis, plataformas de e-commerce, e ecossistemas de assistentes pessoais digitais.

Para cada uma dessas empresas, avaliamos políticas globais do grupo como também políticas para o mercado interno das empresas. (Por exemplo: avaliamos a política de privacidade do Facebook que é aplicável aos Estados Unidos).

Para cada empresa, avaliamos um máximo de cinco serviços, aqui listados:

- **Alibaba (China)** — Taobao.com (plataforma de e-commerce); AliGenie (ecossistema de assistente digital pessoal)
- **Amazon (EUA)** — Amazon.com (plataforma de e-commerce); Amazon Alexa (ecossistema de assistente digital pessoal), Amazon Drive
- **Apple (EUA)** — ecossistema de dispositivo móvel iOS, iMessage, iCloud
- **Baidu (China)** — Baidu Search, Baidu Cloud, Baidu PostBar
- **Facebook (EUA)** — Facebook, Instagram, WhatsApp, Messenger
- **Google (EUA)** — Search, Gmail, YouTube, ecossistema de dispositivo móvel Android, Google Drive
- **Kakao (Coreia do Sul)** — Kakao Search, Kakao Mail, KakaoTalk
- **Mail.Ru (Rússia)** — Vkontakte, Mail.ru e-mail, Mail.ru Agent messaging, Mail.Ru Cloud
- **Microsoft (EUA)** — Bing, Outlook.com, Skype, OneDrive
- **Oath (EUA)** — Yahoo Mail, Tumblr
- **Samsung (Coreia do Sul)** — Implementação do Android, Samsung Cloud
- **Tencent (China)** — QZone, QQ, WeChat, Tencent Cloud
- **Twitter (EUA)** — Twitter
- **Yandex (Rússia)** — Yandex Mail, Yandex Search, Yandex Disk (armazenamento em nuvem)

Empresas de telecomunicações: O Índice de 2020 vai classificar todas as 12 empresas de telecomunicações que classificamos anteriormente. Não foram adicionadas novas empresas de telecomunicações ao Índice de 2020.

Para cada uma dessas empresas, avaliamos tanto as políticas globais do grupo para indicadores relevantes, como da subsidiária que opera o mercado interno para os serviços móveis (pré-pago e pós-pago) e, quando oferecido, banda larga de linha fixa, da seguinte forma:

- **América Móvil (México):** Telcel (móvel pré e pós-pago)
- **AT&T (EUA):** AT&T (móvel pré e pós-pago, banda-larga)
- **Axiata (Malásia):** Celcom (móvel pré e pós-pago, banda larga)
- **Bharti Airtel (Índia):** Airtel India (móvel pré e pós-pago, banda larga)
- **Deutsche Telekom AG (Alemanha):** Deutsche Telekom (móvel pré e pós-pago, banda larga)
- **Etisalat (Emirados Àrabes Unidos):** Etisalat UAE (móvel pré e pós-pago, banda larga)
- **MTN (África do Sul):** MTN South Africa (móvel pré e pós-pago, banda larga)
- **Ooredoo (Catar):** Ooredoo Qatar (móvel pré e pós-pago, banda larga)
- **Orange (França):** Orange France (móvel pré e pós-pago, banda larga)
- **Telefónica (Espanha):** Movistar (móvel pré e pós-pago, banda larga)
- **Telenor ASA (Noruega):** Telenor (móvel pré e pós-pago, banda larga)
- **Vodafone (Reino Unido):** Vodafone UK (móvel pré e pós-pago, banda larga)

5. Processo de pesquisa

O Índice da RDR é produzido usando um rigoroso processo de sete etapas para coleta de dados, verificação cruzada e revisão. A pesquisa é realizada por uma rede de mais de 30 pesquisadores de diversas partes do mundo. As etapas para o Índice de 2020 são descritas a seguir:

- **Etapa 1:** Coleta preliminar de dados. Nesta etapa, os pesquisadores principais são responsáveis por verificar os resultados do Índice anterior (2019) da RDR. Se a política da empresa tiver mudado, ou para novos indicadores e elementos, os pesquisadores principais são responsáveis por avaliar esses processos. Os pesquisadores da Etapa 1 também vão realizar uma avaliação sobre como a política atual se compara à do Índice anterior (2019).

- **Etapa 2:** Revisão adicional. Nesta etapa, revisores adicionais verificam as avaliações dos pesquisadores principais da Etapa 1, o que inclui concordância ou discordância com a análise ano-a-ano.

- **Etapa 3: Revisão e reconciliação.** A equipe da RDR discutirá os resultados das Etapas 1 e 2 e resolver quaisquer diferenças que surgirem.

- **Etapa 4: Feedback da empresa.** Nesta etapa, as empresas terão a oportunidade de apreciar a avaliação preliminar e fornecer feedback para a equipe da RDR. A equipe analisa as considerações das empresas para determinar se uma mudança na avaliação se faz necessária.

- **Etapa 5: Processando o feedback da empresa.** A RDR analisa o feedback das empresas e faz ajustes às avaliações, conforme a necessidade.

- **Etapa 6: Revisão horizontal.** A equipe da RDR conduz uma revisão horizontal, usando o feedback das empresas, coletado na Etapa 4, e verifica os indicadores para garantir que foram aplicados consistentemente a cada empresa.

- **Etapa 7: Pontuação final.** As equipes da RDR atribuem pontuações finais. As avaliações incluem se as empresas mudaram sua política ou forma de divulgação desde a avaliação anterior.

6. Avaliação e pontuação

O ciclo do Índice de 2020 avalia políticas de empresas que estiveram em vigência de 25 de janeiro de 2019 a 14 de setembro de 2020. As empresas recebem uma pontuação cumulativa de sua performance em cada uma das categorias do Índice, e os resultados mostram o desempenho das empresas em cada categoria e indicador.

Cada indicador contém uma lista de elementos, e as empresas recebem pontos (total, parcial ou nenhum) para cada um deles. A avaliação inclui uma análise da divulgação para cada elemento de cada indicador, baseado em uma das possíveis respostas:

- **"Sim"** / Divulgação total. A divulgação da empresa corresponde aos requerimentos do elemento.

- **"Parcial."** A divulgação da empresa correspondeu a alguns, mas não a todos os aspectos do elemento, ou a divulgação não é abrangente o suficiente para satisfazer a totalidade daquilo que o elemento pede.

- **"Divulgação não encontrada."** Pesquisadores não foram capazes de encontrar as informações fornecidas pela empresa em seu website que respondesse à pergunta do elemento.

- **“Não.”** A divulgação existe, mas não diz especificamente aos usuários aquilo que o elemento está pedindo. Isso é distinto da opção de “divulgação não encontrada”, ainda que ambos resultem em zero pontos.

- **“N/A.”** Não aplicável. Este elemento não se aplica à empresa ou ao serviço. Elementos marcados como N/A não vão ser considerados no processo de pontuação da empresa.

Pontos

- Sim/divulgação total = 100
- Parcial = 50
- Não = 0
- Divulgação não encontrada = 0
- N/A excluída da pontuação e médias

Governança

Indicadores nesta categoria buscam evidências de que a empresa dispõe de processos de governança que assegurem o respeito aos direitos humanos de livre expressão e de privacidade. Ambos os direitos são parte da Declaração Universal dos Direitos Humanos[7], e estão consagrados no Pacto Internacional sobre Direitos Civis e Políticos[8]. Eles são aplicáveis online e offline[9]. Para que a empresa obtenha um bom desempenho nessa categoria, a divulgação deve ao menos seguir, e idealmente ultrapassar, os Princípios Orientadores da ONU sobre Empresas e Direitos Humanos[10] e outros parâmetros de direitos humanos focados em liberdade de expressão e privacidade, como aqueles adotados pela Global Network Initiative[11].

G1. Compromisso político

A empresa deve publicar formalmente um **compromisso político** de respeito aos direitos humanos dos usuários à liberdade de expressão, informação e privacidade.

Elementos:

1. A empresa faz um **compromisso político** com os direitos humanos, incluindo liberdade de expressão e informação, de forma **explícita** e articulada?

2. A empresa faz um **compromisso político** com os direitos humanos, incluindo o direito à privacidade, de forma **explícita** e articulada?

3. A empresa divulga um **compromisso político** com os direitos humanos quando se trata do desenvolvimento e uso de sistemas de algoritmos, de forma **explícita** e articulada?

Orientação: Este indicador busca evidências de que a empresa fez compromissos explícitos com a liberdade de expressão e informação, e com a privacidade. Esses parâmetros são descritos no Princípio Operacional 16 dos Princípios Orientadores da ONU sobre Empresas e Direitos Humanos, o qual diz que empresas devem adotar políticas formais e publicamente afirmar seu compromisso com parâmetros e princípios de direitos humanos internacionais[12].

---

[7] Declaração Universal dos Direitos Humanos, https://www.ohchr.org/en/human-rights/universal-declaration/translations/portuguese?LangID=por

[8] "Pacto Internacional sobre Direitos Civis e Políticos," *UN Human Rights Office of the High Commissioner*, https://www.ohchr.org/en/professionalinterest/pages/ccpr.aspx.

[9] Conselho de Direitos Humanos da ONU, *Resolução adotada pelo Conselho de Direitos Humanos em 27 de junho de 2019 – Promoção e proteção de todos os direitos humanos, civis, políticos, econômicos, sociais e culturais, incluindo o direito ao desenvolvimento*, disponível em: https://daccess-ods.un.org/TMP/2969264.09006119.html

[10] "Guiding Principles on Business and Human Rights," *UN Human Rights Office of the High Commissioner*, https://www.ohchr.org/Documents/Publications/GuidingPrinciplesBusinessHR_EN.pdf.

[11] "The GNI Principles," *Global Network Initiative*, https://globalnetworkinitiative.org/gni-principles/.

[12] "Guiding Principles on Business and Human Rights," *UN Human Rights Office of the High Commissioner*, https://www.ohchr.org/Documents/Publications/GuidingPrinciplesBusinessHR_EN.pdf.

Empresas também deveriam publicar um compromisso formal de respeito aos direitos humanos na medida em que desenvolvem sistemas de tomada de decisão via algoritmos, em conformidade com as recomendações do Conselho Europeu em seu Recommendation on the human rights impacts of algorithmic systems (2020) (em tradução livre, "Recomendação sobre os impactos de sistemas de algoritmos aos direitos humanos"). A empresa deve divulgar explicitamente esses compromissos, em documentos formais ou outros comunicados que reflitam a política oficial da empresa.

Possíveis fontes:

- Política de direitos humanos da empresa
- Declarações, relatórios e outros comunicados que reflitam a política oficial da empresa
- Relatório anual da empresa ou relatório de sustentabilidade
- Política de "princípios de IA" da empresa

G2. Governança e supervisão

A **liderança sênior** da empresa deveria exercer **supervisão** sobre suas políticas e práticas na medida em que elas afetem a liberdade de expressão e informação, e a privacidade.

Elementos:

1. A empresa **divulga publicamente** que o **conselho diretor** exerce **supervisão** formal sobre as práticas da empresa que afetam a liberdade de expressão e informação?

2. A empresa **divulga publicamente** que o **conselho diretor** exerce **supervisão** formal sobre as práticas da empresa que afetam a privacidade?

3. A empresa **divulga publicamente** que um comitê, equipe, programa ou funcionário encarregado do **nível executivo** **supervisiona** como as práticas da empresa afetam a liberdade de expressão e informação?

4. A empresa **divulga publicamente** que um comitê, equipe, programa ou funcionário encarregado do **nível executivo** **supervisiona** como as práticas da empresa afetam a privacidade?

5. A empresa **divulga publicamente** que um comitê, equipe, programa ou funcionário encarregado de **nível administrativo** **supervisiona** como as práticas da empresa afetam a liberdade de expressão e informação?

6. A empresa **divulga publicamente** que um comitê, equipe, programa ou funcionário encarregado de **nível administrativo** **supervisiona** como as práticas da empresa afetam a privacidade?

Orientação: Este indicador busca evidências de que a empresa dispõe de forte supervisão sobre questões de liberdade de expressão e informação e de privacidade em todos os níveis de suas operações. Empresas devem divulgar que a liderança sênior—do conselho à administração—supervisiona e responde pelas políticas e práticas que afetam esses direitos humanos.

Para receber pontuação total nesse indicador, as empresas devem divulgar explicitamente que em todos os níveis de governança (conselho, executivo, administrativo), há supervisão tanto de questões relacionadas à liberdade de expressão e informação, quanto aquelas relacionadas à privacidade. No nível do conselho, essa supervisão deve incluir um conselho diretor ou outra explicação pública de como o conselho exerce supervisão sobre esses assuntos. Abaixo do nível do conselho, a supervisão pode consistir em uma unidade, programa ou indivíduo da empresa, que reporta diretamente ao nível executivo ou administrativo. O conselho, programa, equipe, funcionário encarregado etc. deveria especificamente citar liberdade de expressão e privacidade na descrição de suas responsabilidades.

Fontes em potencial

- Lista do conselho diretor
- Documentos de administração da empresa
- Relatório de sustentabilidade da empresa
- Quadro organizacional da empresa
- Política de direitos humanos da empresa
- Documentos da Global Network Initiative (se a empresa for integrante)

G3. Implementação interna

A empresa deveria dispor de mecanismos para implementar seus compromissos com a liberdade de expressão e informação e privacidade dentro da própria empresa.

Elementos:

1. A empresa **divulga claramente** que fornece treinamento para seus funcionários em questões de liberdade de expressão e informação?

2. A empresa **divulga claramente** que fornece treinamento para seus funcionários em questões relacionadas à privacidade?

3. A empresa **divulga claramente** que mantém um **programa de whistleblower** por meio do qual funcionários podem denunciar preocupações pela maneira como a empresa lida com a liberdade de expressão e o direito da informação dos usuários?

4. A empresa **divulga claramente** que mantém um **programa de whistleblower** por meio do qual funcionários podem denunciar preocupações pela maneira como a empresa

lida com o direito à privacidade dos usuários?

Orientação: O indicador G2 avalia se a liderança sênior de uma empresa se compromete a supervisionar questões de liberdade de expressão e privacidade. O indicador G3, por sua vez, avalia se a empresa divulga se e como esses compromissos estão institucionalizados dentro da empresa. Especificamente, este indicador busca a divulgação de se e como a empresa auxilia seus funcionários a entender a importância da liberdade de expressão e privacidade. Quando funcionários escrevem códigos de computador para um novo produto, avaliam solicitações de dados dos usuários ou respondem a perguntas de usuários sobre como usar determinado serviço, eles agem de forma que pode afetar diretamente a liberdade de expressão e privacidade dos usuários. Esperamos que as empresas divulguem se elas fornecem aos funcionários treinamento sobre o papel que desempenham em respeitar direitos humanos e que forneça a eles um meio para manifestar preocupações com relação aos direitos humanos.

Uma empresa só poderá receber pontuação total neste indicador se explicitamente divulgar informações sobre treinamento de funcionários em liberdade de expressão e informação e privacidade, e sobre a existência de um programa de whistleblower para essas questões. A divulgação deve especificar que o treinamento dos funcionários e o programa de whistleblower abrangem liberdade de expressão e privacidade. Mesmo que o programa de whistleblower da empresa não mencionar especificamente reclamações de liberdade de expressão e privacidade, a empresa poderá receber pontuação neste indicador se tiver feito compromissos com esses princípios em outras instâncias e de uma forma que deixe claro que a empresa consideraria essas reclamações através de seu programa de whistleblower.

Fontes em potencial

- Código de conduta da empresa
- Manual do funcionário
- Quadro organizacional da empresa
- Relatório de sustentabilidade/Responsabilidade Social Corporativa da empresa
- Posts do blog da empresa

G4: Devida diligência em direitos humanos

G4(a). Avaliação de impacto: Governos e regulamentos

Empresas deveriam realizar devida diligência de forma regular, abrangente e confiável, por meio de **avaliações de impacto em direitos humanos** robustas, com o objetivo de identificar como regulamentos e políticas governamentais afetam a liberdade de expressão e informação e a privacidade, e para mitigar quaisquer riscos postos por esses impactos nas jurisdições onde operam.

Elementos:

1. A empresa **avalia** como as leis afetam a liberdade de expressão e informação nas jurisdições onde opera?

2. A empresa **avalia** como as leis afetam a privacidade nas jurisdições onde opera?

3. A empresa **avalia** os riscos à liberdade de expressão e informação associados a produtos e serviços existentes nas jurisdições onde opera?

4. A empresa **avalia** riscos à privacidade associados a produtos e serviços existentes nas jurisdições onde opera?

5. A empresa **avalia** riscos à liberdade de expressão e informação associados a uma nova atividade, incluindo o lançamento e/ou aquisição de novos produtos, serviços ou empresas, ou entrada em um novo mercado ou jurisdição?

6. A empresa **avalia** riscos à privacidade associados a uma nova atividade, incluindo o lançamento e/ou aquisição de novos produtos, serviços ou empresas, ou entrada em um novo mercado ou jurisdição?

7. A empresa conduz avaliações adicionais quando a **avaliação de risco** da empresa identifica problemas?

8. Os **executivos sêniores** ou membros do **conselho diretor** da empresa revisam e consideram os resultados das **avaliações** de devida diligência em suas tomadas de decisão?

9. A empresa conduz **avaliações** em um cronograma regular?

10. As **avaliações** da empresa são asseguradas por um **ente externo**?

11. O **ente externo** que assegura as **avaliações** é acreditado por uma organização de direitos humanos com credibilidade e renome?

Orientação: Esse indicador avalia se as empresas realizam avaliações regulares, robustas e responsáveis de riscos aos direitos humanos em regulamentos e políticas governamentais nas jurisdições onde operam. Essas avaliações deveriam ser parte das atividades formais e sistemáticas de devida diligência da empresa, com o objetivo de assegurar que suas decisões e práticas não causem, contribuam ou amplifiquem violações de direitos humanos. Avaliações permitem que empresas identifiquem possíveis riscos à liberdade de expressão e ao direito à privacidade dos usuários e tomem medidas para mitigar possíveis violações, caso identificadas.

Ressalta-se que esse indicador não pressupõe que as empresas publiquem resultados detalhados de suas avaliações de impacto nos direitos humanos, uma vez que essas avaliações podem incluir informações sensíveis. Em vez disso, espera-se que as empresas divulguem que conduzem avaliação de impacto em direitos humanos e forneçam informações sobre o que seus processos de avaliação de impacto em direitos humanos abrangem.

Possíveis fontes:

- Relatórios de Responsabilidade Social Corporativa/sustentabilidade
- Política de direitos humanos da empresa
- Avaliações da Global Network Initiative

G4(b). Avaliação de impacto: Processos para a aplicação da política

A empresa deveria realizar devida diligência de forma regular**,** abrangente e confiável, por meio de **avaliações de impacto em direitos humanos**, por exemplo, para identificar como seus processos de aplicação de políticas afetam os direitos fundamentais dos usuários à liberdade de expressão e informação, à privacidade e à não discriminação, e mitigar qualquer risco associado a tais impactos.

Elementos:

1. A empresa **avalia** os riscos à liberdade de expressão e informação colocados pela aplicação de seus termos de serviço?

2. A empresa conduz **avaliação de risco** da aplicação de suas políticas de privacidade?

3. A empresa **avalia** riscos de discriminação associados com seus processos de aplicação de seus **termos de serviço**?

4. A empresa **avalia** riscos de **discriminação** associados com os processos de aplicação de suas **políticas de privacidade**?

5. A empresa faz avaliações adicionais quando a **avaliação de risco** identifica problemas?

6. Os **executivos sêniores** e/ou membros do **conselho diretor** da empresa avaliam e levam em conta os resultados de **avaliações** e devida diligência em suas tomadas de decisão?

7. A empresa conduz **avaliações** conforme um cronograma regular?

8. As **avaliações** da empresa são certificadas por um **ente externo**?

9. O **ente externo** que certifica a **avaliação** é acreditado por uma organização de direitos humanos confiável e renomada?

Orientação: Este indicador examina se a empresa divulga que realiza avaliações de risco de direitos humanos robustas, regulares e responsáveis, sobre o impacto de suas próprias políticas nos direitos fundamentais dos usuários à liberdade de expressão, privacidade e não discriminação. Essas avaliações devem fazer parte das atividades formais e sistemáticas de devida diligência da empresa, de forma a garantir que suas decisões e práticas não causem, contribuam ou amplifiquem violações de direitos humanos. Avaliações permitem que as empresas identifiquem possíveis riscos postos por suas próprias políticas à liberdade de expressão e informação, privacidade e direito à não discriminação dos usuários, e tomar medidas que mitiguem possíveis violações, caso identificadas.

Ressalta-se que este indicador não pressupõe que as empresas publiquem resultados detalhados de suas avaliações de impacto nos direitos humanos, uma vez que essas avaliações podem incluir informações sensíveis. Em vez disso, espera-se que as empresas divulguem que conduzem avaliação de impacto em direitos humanos e forneçam informações sobre o que seus processos de avaliação de impacto em direitos humanos abrangem.

Possíveis fontes:

- Relatórios de Responsabilidade Social Corporativa/sustentabilidade da empresa
- Política de direitos humanos da empresa
- Relatórios da Global Network Initiative

G4(c). Avaliação de impacto: Publicidade direcionada

A empresa deveria realizar devida diligência de forma regular**,** abrangente e confiável, por meio de **avaliações de impacto em direitos humanos**, por exemplo, para identificar como sua política e suas práticas de **publicidade direcionada**, em todos os seus aspectos, afetam os direitos fundamentais dos usuários à liberdade de expressão e informação, à privacidade e à não discriminação, e mitigar qualquer risco associado a tais impactos.

Elementos:

1. A empresa **avalia** riscos à liberdade de expressão e informação associados a suas políticas e práticas de **publicidade direcionada**?

2. A empresa conduz **avaliação** de risco à privacidade associado a suas políticas e práticas de **publicidade direcionada**?

3. A empresa **avalia** riscos de discriminação associados a suas políticas e práticas de

publicidade direcionada?

4. A empresa faz avaliações adicionais quando a **avaliação de risco** identifica problemas?

5. Os **executivos sêniores** e/ou membros do **conselho diretor** da empresa avaliam e levam em conta os resultados de **avaliações** e devida diligência em suas decisões?

6. A empresa conduz **avaliações** conforme um cronograma regular?

7. As **avaliações** da empresa são certificadas por um **ente externo**?

8. O **ente externo** que certifica a **avaliação** é acreditado por uma organização de direitos humanos confiável e renomada?

Orientação: Publicidade direcionada pode ter efeitos adversos nos direitos humanos, especificamente nos direitos dos usuários à liberdade de expressão, de informação e à não discriminação[13]. Discriminação ocorre quando as plataformas permitem que terceiros mostrem anúncios diferentes para usuários diferentes, de acordo com informações divulgadas e inferidas, incluindo filiação a categorias protegidas (raça, etnia, idade, identidade e expressão de gênero, orientação sexual, saúde, deficiência física etc.). Discriminação não precisa ser ilegal ou imediatamente nociva para resultar em efeitos prejudiciais em grande escala, como no nível populacional ou ao longo da vida de um indivíduo. Considerando o fato de que publicidade direcionada é menos transparente que outras formas de publicidade e que há grandes incentivos financeiros das empresas para implementar tecnologia rapidamente, as potenciais violações de direitos devem ser consideradas em avaliações de risco.

Este indicador examina se as empresas divulgam que realizam avaliações de direitos humanos robustas, regulares e responsáveis sobre o impacto da publicidade direcionada nos direitos fundamentais dos usuários à liberdade de expressão, privacidade e não discriminação. Essas avaliações deveriam fazer parte das atividades formais e sistemáticas de devida diligência da empresa, cujo objetivo é garantir que as decisões e práticas da empresa não causem, contribuam ou amplifiquem violações de direitos humanos. Avaliações permitem que as empresas identifiquem possíveis riscos da publicidade direcionada à liberdade de expressão e informação, privacidade e direito de não discriminação dos usuários, e tomem medidas capazes de mitigar possíveis violações, caso identificadas.

Ressalta-se que este indicador não pressupõe que as empresas publiquem resultados detalhados de suas avaliações de impacto em direitos humanos, uma vez que as avaliações podem incluir informações sensíveis. Em vez disso, espera-se que as empresas divulguem que

[13] "Human Rights Risk Scenarios: Targeted advertising," (em tradução livre, "Situações de Riscos aos Direitos Humanos: Publicidade direcionada"), *Ranking Digital Rights*, fevereiro de 2019, https://rankingdigitalrights.org/wp-content/uploads/2019/02/Human-Rights-Risk-Scenarios-targeted-advertising.pdf.

conduzem avaliação de impacto em direitos humanos e forneçam informações sobre o que seus processos de avaliação de impacto em direitos humanos abrangem.

Possíveis fontes:

- Relatórios de Responsabilidade Social Corporativa/sustentabilidade da empresa
- Política de direitos humanos da empresa
- Relatórios da Global Network Initiative

G4(d). Avaliação de impacto: Sistemas de algoritmos

A empresa deveria realizar devida diligência de forma regular**,** abrangente e confiável, por meio de **avaliações de impacto em direitos humanos**, por exemplo, para identificar como sua política e suas práticas de desenvolvimento e uso de **sistemas de algoritmos**, em todos os seus aspectos, afetam os direitos fundamentais dos usuários à liberdade de expressão e informação, à privacidade e à **não discriminação**, e mitigar qualquer risco associado a tais impactos.

Elementos:

1. A empresa **avalia** riscos à liberdade de expressão e informação associadas a suas políticas e práticas de desenvolvimento e uso de **sistemas de algoritmos**?

2. A empresa conduz **avaliação** de risco à privacidade associado a suas políticas e práticas de desenvolvimento e uso de **sistemas de algoritmos**?

3. A empresa avalia riscos de **discriminação** associados a suas políticas e práticas de desenvolvimento e uso de **sistemas de algoritmos**?

4. A empresa faz avaliações adicionais quando a **avaliação de risco** identifica problemas?

5. Os **executivos sêniores** e/ou membros do **conselho diretor** da empresa revisam e levam em conta os resultados de **avaliações** de devida diligência em suas tomadas de decisão?

6. A empresa conduz **avaliações** conforme um cronograma regular?

7. As **avaliações** da empresa são certificadas por um **ente externo**?

8. O **ente externo** que certifica a **avaliação** é acreditado por uma organização de direitos humanos confiável e renomada?

Orientação: Há muitas formas pelas quais sistemas de algoritmos podem apresentar ameaças aos direitos humanos[14]. O desenvolvimento desses sistemas pode depender de informações do usuário, frequentemente sem conhecimento ou consentimento explícito e informado do titular dos dados, constituindo uma violação de privacidade. Esses sistemas também podem causar ou contribuir com ameaças à expressão e informação. Além disso, o objetivo de muitos sistemas de tomada de decisão via algoritmos é automatizar a personalização da experiência do usuário com base em informações coletadas e inferidas do usuário, o que pode causar ou contribuir com a discriminação. Empresas deveriam, portanto, conduzir avaliações de impacto em direitos humanos do desenvolvimento e uso de algoritmos, como recomendado pelo Conselho Europeu, na Recomendação sobre os impactos de sistemas de algoritmos aos direitos humanos (2020).

Este indicador examina se as empresas divulgam que realizam avaliações de direitos humanos robustas, regulares e responsáveis sobre o impacto do desenvolvimento e uso de sistemas de algoritmos nos direitos fundamentais dos usuários à liberdade de expressão, privacidade e não discriminação. Essas avaliações deveriam fazer parte das atividades formais e sistemáticas de devida diligência da empresa, cujo objetivo é garantir que as decisões e práticas da empresa não causem, contribuam ou amplifiquem violações de direitos humanos. Avaliações permitem que as empresas identifiquem possíveis riscos do desenvolvimento e uso de sistemas de algoritmos à liberdade de expressão e informação, privacidade e direito de não discriminação dos usuários, e tomem medidas capazes de mitigar possíveis violações, caso identificadas.

Ressalta-se que este indicador não pressupõe que as empresas publiquem resultados detalhados de suas avaliações de impacto em direitos humanos, uma vez que as avaliações podem incluir informações sensíveis. Em vez disso, espera-se que as empresas divulguem que conduzem avaliação de impacto em direitos humanos e forneçam informações sobre o que seus processos de avaliação de impacto em direitos humanos abrangem.

Possíveis fontes:

- Relatórios de Responsabilidade Social Corporativa/sustentabilidade da empresa
- Política de direitos humanos da empresa
- Relatórios da Global Network Initiative

G4(e). Avaliação de impacto: Zero-rating

Caso faça uso de **zero-rating**, a empresa deveria realizar devida diligência de forma regular**,** abrangente e confiável, por meio de **avaliações de impacto em direitos humanos**, por exemplo, para identificar como sua política e suas práticas de zero-rating, em todos os seus aspectos, afetam os direitos fundamentais dos usuários à liberdade de expressão e informação,

[14] "Human Rights Risk Scenarios: Algorithms, machine learning and automated decision-making,'' (em tradução livre, "Situações de risco aos direitos humanos: Algoritmos, aprendizado de máquina e tomada de decisão automatizada"), *Ranking Digital Rights*, julho de 2019, https://rankingdigitalrights.org/wp-content/uploads/2019/07/Human-Rights-Risk-Scenarios_-algorithms-machine-learning-automated-decision-making.pdf.

à privacidade e à não discriminação, e mitigar qualquer risco associado a tais impactos.

Elementos:

1. A empresa avalia riscos à liberdade de expressão e informação associadas a suas políticas e práticas de **zero-rating**?

2. A empresa conduz avaliação de risco à privacidade associado a suas políticas e práticas de **zero-rating**?

3. A empresa avalia riscos de discriminação associados a suas políticas e práticas de **zero-rating**?

4. A empresa faz avaliações adicionais quando a **avaliação de risco** identifica problemas?

5. Os **executivos sêniores** e/ou membros do **conselho diretor** da empresa revisam e levam em conta os resultados de **avaliações** de devida diligência em suas decisões?

6. A empresa conduz **avaliações** conforme um cronograma regular?

7. As **avaliações** da empresa são certificadas por um **ente externo**?

8. O **ente externo** que certifica a **avaliação** é acreditado por uma organização de direitos humanos confiável e renomada?

Orientação: "Zero-rating" se refere a programas – que podem ser oferecidos tanto por empresas de telecomunicações quanto por plataformas em parceria com empresas de telecomunicações – que fornecem acesso a certos serviços online ou plataformas sem cobrança no plano de dados de uma pessoa. Muitos provedores de telecomunicação, incluindo empresas classificadas pela RDR, oferecem tais programas, seja por si próprios ou em parceria com plataformas de redes sociais, como o programa "Free Basics" do Facebook. Esses tipos de programas são uma forma de priorização de rede que vai de encontro ao princípio da neutralidade de rede -- e pode desencadear uma série de outras violações de direitos humanos, incluindo danos ao direito à liberdade de expressão e informação. Além disso, o Global Voices Advox identificou o programa Free Basics, do Facebook, como um "mecanismo de coleta de dados lucrativos dos usuários" (Global Voices, 2017), levantando sérias preocupações quanto à privacidade no programa. Programas de zero-rating também podem ser discriminatórios na medida em que priorizam certos tipos de dados em detrimento de outros, seja baseado no protocolo em questão (HTTP, HTTPS, VoIP etc.) ou no conteúdo (ex.: priorizando uma rede social em detrimento de outra). Essa discriminação (contra certos tipos de dados) pode por sua vez levar a violações de direitos humanos que afetam indivíduos de acordo com suas características pessoais, incluindo gênero, raça ou etnia, idioma, e muitos outros atributos.

Este indicador examina se as empresas divulgam que elas realizam avaliações de direitos humanos robustas, regulares e responsáveis sobre o impacto do uso de zero-rating nos direitos fundamentais dos usuários à liberdade de expressão, privacidade, e não discriminação. As empresas que oferecem esse tipo de programa deveriam conduzir avaliações de como esses programas podem impactar os direitos dos usuários à expressão e informação, à privacidade e à não discriminação. Essas avaliações deveriam fazer parte das atividades formais e sistemáticas de devida diligência da empresa cujo objetivo é garantir que as decisões e práticas da empresa não causem, contribuam ou amplifiquem violações de direitos humanos. Avaliações permitem que as empresas identifiquem possíveis riscos do uso de zero-rating e tomem medidas para mitigar possíveis violações, caso identificadas.

Ressalta-se que este indicador não pressupõe que as empresas publiquem resultados detalhados de suas avaliações de impacto em direitos humanos, uma vez que as avaliações podem incluir informações sensíveis. Em vez disso, espera-se que as empresas divulguem que elas conduzem avaliações de risco em direitos humanos e forneçam informações sobre o que seus processos de avaliação de risco em direitos humanos incluem.

Possíveis fontes:

- Relatórios de Responsabilidade Social Corporativa/sustentabilidade da empresa
- Política de direitos humanos da empresa
- Relatórios da Global Network Initiative

G5. Engajamento e responsabilidade das partes interessadas

A empresa deve se **engajar** com uma variedade de **partes interessadas** (stakeholders) sobre o impacto da empresa na liberdade de expressão e informação e na privacidade, e sobre os potenciais riscos relacionados a violações de direitos humanos, como a **discriminação**.

Elementos:

1. A empresa é membro de uma ou mais **iniciativas multissetoriais** que aborde as diferentes formas com que os direitos fundamentais de liberdade de expressão e informação, de privacidade e de não discriminação do usuário podem ser afetados pelas operações da empresa?

2. Caso não seja membro de uma ou mais **iniciativas multissetoriais** do tipo, a empresa é membro de alguma organização que se engaje sistemática e regularmente com as partes interessadas que não façam parte do setor corporativo ou do governo sobre liberdade de expressão e questões de privacidade?

3. Caso não seja membro de nenhuma dessas organizações, a empresa divulga que realiza ou participa de reuniões com as partes interessadas representantes ou defensoras, ou

com as próprias pessoas cujos direitos à liberdade de expressão e informação e privacidade são impactados diretamente pelos negócios da empresa?

Orientação: O indicador busca evidências de que a empresa se engaja e responde a diferentes partes interessadas — particularmente aquelas que têm seus direitos humanos ameaçados por suas atividades online. Esperamos que o engajamento com as partes interessadas seja um componente central do desenvolvimento da política e do processo de avaliação da empresa. O engajamento com as partes interessadas deve acontecer em todas as instâncias relacionadas à liberdade de expressão e de informação, privacidade e outros direitos relacionados dos usuários, incluindo o processo da empresa para desenvolver termos de serviço e políticas de privacidade e identidade, como também políticas de uso de algoritmos e políticas de publicidade direcionada, assim como as práticas de aplicação dessas políticas. Engajamento com as partes interessadas e mecanismos de responsabilidade deveriam abranger todas as maneiras pelas quais os direitos dos usuários podem ser violados: solicitações do governo, ações de terceiros através dos produtos e serviços da empresa, ou pelas próprias empresas. Empresas que recebem pontuação completa neste indicador não apenas se engajam com as partes interessadas, como também se comprometem com processos de responsabilização, como avaliações independentes supervisionadas por uma organização cujas decisões finais não sejam controladas apenas pela empresa.

Engajamento com as partes interessadas, especialmente aquelas que operam em ambientes de alto risco, pode ser sensível. A empresa pode não se sentir confortável em divulgar publicamente detalhes específicos sobre quais partes ela consulta, onde e quando eles se encontram, e o que discutem. Incentivamos empresas a fornecer detalhes sobre engajamento com as partes interessadas que não for sensível, e buscamos, no mínimo, a divulgação pública de que a empresa se engaja com as partes interessadas que são ou representam usuários cujos direitos à liberdade de expressão e privacidade estão em risco. Uma maneira pela qual o público sabe que a empresa participa desse tipo de engajamento e que o engajamento produz resultados concretos é pelo seu envolvimento em uma iniciativa multissetorial cujo propósito não é apenas criar um espaço seguro para engajamento, e sim permitir que empresas assumam compromissos, demonstrem apoio em encontros entre as partes e que as empresas sejam responsabilizadas. Quando se trata de processos de responsabilização e engajamento, mecanismos de responsabilização com credibilidade e completos exigem governança multissetorial, cuja autoridade para a tomada de decisão não é controlada apenas pela empresa, mas, sim, dividida com representantes de outros setores.

Se uma empresa recebe pontuação total no Elemento 1, ela automaticamente recebe pontuação total no Elemento 2 e no Elemento 3. Note-se que como o escopo do trabalho da Global Network Initiative foca em solicitações do governo, e pelo menos metade da metodologia da RDR aborda ameaças a direitos humanos que não vêm de governos, para o Índice de 2020, ser membro da GNI (sem evidência de engajamento e responsabilização em outros riscos a direitos humanos além daqueles postos por governos) apenas resultará em pontuação parcial para o Elemento 1 deste indicador.

Possíveis fontes:

- Relatório de Responsabilidade Social Corporativa/sustentabilidade da empresa
- Relatório anual da empresa
- Blog da empresa
- FAQ ou Central de ajuda da empresa

G6: Reparações e recursos

G6(a). Reparações

A empresa deve dispor de mecanismos claros e padronizados de **reclamação** e **reparação** que atendam as preocupações dos usuários quanto à liberdade de expressão e privacidade.

Elementos:

1. A empresa **divulga claramente** que dispõe de **mecanismos de reclamação** que permitem que os usuários enviem reclamações caso sintam que seus direitos à liberdade de expressão e informação foram adversamente afetados pelas políticas e práticas da empresa?

2. A empresa **divulga claramente** que dispõe de **mecanismos de reclamação** que permite que os usuários enviem reclamações caso sintam que sua privacidade foi adversamente afetada pelas políticas e práticas da empresa?

3. A empresa **divulga claramente** que dispõe de procedimentos para fornecer **reparação** para **reclamações** relacionadas à liberdade de expressão e informação?

4. A empresa **divulga claramente** que dispõe de procedimentos para fornecer **reparação** para **reclamações** relacionadas à privacidade?

5. A empresa **divulga claramente** os cronogramas dos seus procedimentos de **reclamação** e **reparação**?

6. A empresa **divulga claramente** o número de reclamações recebidas que são relacionadas à liberdade de expressão?

7. A empresa **divulga claramente** o número de reclamações recebidas que são relacionadas à privacidade?

8. A empresa **divulga claramente** evidências de que fornece **reparação** para **reclamações** relacionadas à liberdade de expressão?

9. A empresa **divulga claramente** evidências de que fornece **reparação** para **reclamações** relacionadas à privacidade?

Orientação: Direitos humanos só podem ser protegidos e respeitados se as pessoas obtêm reparação quando elas acreditam que seus direitos foram violados. Este indicador examina se as empresas dispõem desses mecanismos de reparação e se elas divulgaram publicamente processos para responder a reclamações de indivíduos que acreditam que a empresa violou ou diretamente facilitou violações à sua liberdade de expressão ou privacidade.

Esperamos que as empresas divulguem claramente um mecanismo de reclamação que permita que usuários enviem reclamações se perceberem que sua liberdade de expressão ou privacidade foram infringidas pelas políticas e práticas da empresa. Para receber pontuação total no Elemento 1, o mecanismo de reclamação da empresa não precisa afirmar explicitamente que ele se aplica a reclamações relacionadas à liberdade de expressão e privacidade. No entanto, deve ficar claro que o mecanismo serve para receber qualquer tipo de reclamação relacionado à violação de direitos humanos. Também esperamos que o mecanismo de reclamação da empresa esteja facilmente acessível aos usuários. Além disso, a empresa deve explicar seu processo para fornecer reparação para esses tipos de reclamação e divulgar evidências de que faz isso. As empresas deveriam descrever cronogramas claros para atender cada estágio do processo de reclamação e reparação. Esses parâmetros estão descritos no Princípio 31 da Princípios Orientadores da ONU sobre Empresas e Direitos Humanos, o qual estabelece que empresas devem publicar mecanismos de reparação claros, acessíveis e previsíveis[15].

Possíveis fontes:

- Termos de serviço ou acordos de uso equivalentes
- Políticas de conteúdo da empresa
- Políticas de privacidade, diretrizes de privacidade, ou site de recursos de privacidade da empresa
- Relatório de Responsabilidade Social Corporativa/sustentabilidade
- Central de ajuda ou manual do usuário da empresa
- Relatório de transparência da empresa (para o número de reclamações recebidas)
- Política de publicidade da empresa

G6(b). Processo de recurso a decisões da moderação de conteúdo

A empresa deveria oferecer mecanismos claros de **recurso** e processos para recurso a **decisões da moderação de conteúdo**.

Elementos:

[15] "Guiding Principles on Business and Human Rights," *UN Human Rights Office of the High Commissioner*, 2011, https://www.ohchr.org/Documents/Publications/GuidingPrinciplesBusinessHR_EN.pdf.

1. A empresa **divulga claramente** que fornece a **usuários afetados** a possibilidade de **recorrer às decisões da moderação de conteúdo**?

2. A empresa **divulga claramente** que **notifica** usuários **afetados** por uma determinada **decisão da moderação de conteúdo**?

3. A empresa **divulga claramente** um cronograma para **notificar usuários afetados** quando toma uma **decisão de moderação de conteúdo**?

4. A empresa **divulga claramente** quando **recursos** não são permitidos?

5. A empresa **divulga claramente** seus processos para analisar **recursos**?

6. A empresa **divulga claramente** um cronograma para analisar **recursos**?

7. A empresa **divulga claramente** que recursos são analisados por pelo menos um humano que não esteve envolvido com a decisão original de **moderação de conteúdo**?

8. A empresa **divulga claramente** qual papel a automação exerce na análise de **recursos**?

9. A empresa **divulga claramente** que os **usuários afetados** têm a oportunidade de apresentar informações adicionais que serão consideradas na análise?

10. A empresa **divulga claramente** que fornece aos **usuários afetados** uma declaração descrevendo a razão da sua decisão?

11. A empresa **divulga claramente** evidências de que está analisando **recursos** da moderação de conteúdo?

Orientação: Mesmo que os termos de serviço de uma plataforma sejam bastante cuidadosos, erros são inevitáveis quando se trata de algo tão árduo e subjetivo quanto moderação de conteúdo, ainda mais quando essa moderação é ampliada rapidamente através do uso de automação. De modo a respeitar os direitos dos usuários à liberdade de expressão e informação, as empresas deveriam fornecer um sistema de recursos robusto e transparente que permita que os usuários recorram de decisões feitas pela empresa que diretamente influenciem a habilidade dos usuários de exercer esses direitos. As empresas deveriam divulgar seus processos para recorrer de decisões da moderação de conteúdo, incluindo permitir que usuários afetados possam recorrer da decisão imediatamente. Um processo de apelação robusto deve incluir supervisão por um analista humano e dar aos usuários afetados a oportunidade de apresentar informações adicionais. Empresas deveriam oferecer um cronograma claro para análise de recursos e claramente divulgar as circunstâncias em que recursos não são possíveis.

Para receber pontuação total neste indicador, empresas deveriam informar como usuários podem submeter um recurso e descrever o que acontece quando esse recurso é submetido. Isso inclui notificar usuários de suas opções de recurso tão logo a empresa tome uma decisão inicial sobre conteúdo, informando sobre o papel tanto da automação quanto do moderador humano independente no processo, divulgando a razão de uma decisão sobre o recurso e os cronogramas envolvidos, e especificando as circunstâncias em que um recurso não está disponível. Empresas também deveriam claramente demonstrar que respondem aos recursos ao publicar dados sobre pedidos recebidos e o resultado dessas decisões.

Possíveis fontes:

- Termos de serviço da empresa ou acordos de uso
- Política de privacidade da empresa
- Relatório de sustentabilidade da empresa

Liberdade de expressão e informação

Indicadores nesta categoria buscam evidências de que a empresa demonstra respeito pelos direitos à liberdade de expressão e informação, conforme articulados na Declaração Universal dos Direitos Humanos[16], no Pacto Internacional sobre Direitos Civis e Políticos[17] e em outros instrumentos internacionais de direitos humanos. As políticas da empresa e suas práticas demonstram o que ela faz para não contribuir com ações que possam interferir com esse direito, exceto nos casos em que essas ações são legais, proporcionais e têm um propósito justificável. Empresas que obtêm um bom desempenho neste indicador demonstram um forte compromisso público com transparência não apenas quando se trata de solicitações governamentais e de outros, mas também como elas determinam, comunicam e aplicam regras privadas e práticas comerciais que afetam o direito fundamental à liberdade de expressão e informação dos usuários.

L1: Acesso a políticas

L1(a). Acesso aos termos de serviço

A empresa deveria oferecer **termos de serviço** **fáceis de localizar** e **fáceis de entender**.

Elementos:

1. Os **termos de serviço** da empresa são **fáceis de localizar**?

2. Os **termos de serviço** da empresa estão disponíveis na principal língua falada pelos usuários da jurisdição nacional da empresa?

3. Os **termos de serviço** são apresentados de **maneira compreensível**?

Orientação: Os termos de serviço da empresa descrevem a relação entre o usuário e a empresa. Esses termos definem as regras sobre conteúdo e atividades proibidas, e a empresa também pode tomar medidas contra usuários que violem as regras descritas nesses termos. Por causa disso, esperamos que as empresas garantam que esses termos sejam de fácil acesso e compreensão.

Este indicador avalia se os termos de serviço da empresa são fáceis de localizar pelos usuários. Um documento fácil de encontrar está na homepage da empresa ou serviço, a um ou dois cliques de distância da homepage, ou em um lugar lógico onde usuários podem esperar encontrá-los. O uso de posicionamento ou de cores que fazem o texto ou link menos

[16] "Declaração Universal dos Direitos Humanos," https://www.un.org/en/universal-declaration-human-rights/.

[17] "Pacto Internacional sobre Direitos Civis e Políticos," *UN Human Rights Office of the High Commissioner*, https://www.ohchr.org/en/professionalinterest/pages/ccpr.aspx,

perceptível ou difícil de localizar numa página da web significa que o documento não está facilmente acessível. Os termos de serviço de um aplicativo nunca devem estar a mais de dois cliques de distância dentro do app (ex.: ao incluir uma opção "Privacidade/Proteção de dados" no menu do aplicativo). Os termos também devem estar na língua principal do mercado de operação. Além disso, esperamos que a empresa tome medidas para ajudar os usuários a entender as informações apresentadas em seus documentos. Isso inclui, mas não se limita a fornecer resumos, dicas ou orientações que expliquem o que os termos significam, utilizando subtítulos, tamanho de fonte legível e outros recursos gráficos que ajudem os usuários a entender o documento, ou escrever os termos usando linguagem acessível.

Possíveis fontes:

- Termos de serviço da empresa, termos de uso, termos e condições etc.
- Política de uso aceitável da empresa, diretrizes de comunidade, regras etc.

L1(b). Acesso às políticas de conteúdo publicitário

A empresa deveria oferecer **políticas de conteúdo publicitário** **fáceis de localizar** e **fáceis de entender**.

Elementos:

1. As **políticas de conteúdo publicitário** da empresa são **fáceis de localizar**?

2. As **políticas de conteúdo publicitário** da empresa estão disponíveis na principal língua dos usuários da jurisdição nacional da empresa?

3. As **políticas de conteúdo publicitário** da empresa são apresentadas de **maneira compreensível**?

4. (Para **ecossistemas de dispositivos móveis**): A empresa **divulga claramente** que exige que os aplicativos disponíveis em sua **loja de aplicativos** forneçam uma **política de conteúdo publicitário**?

5. (Para **ecossistemas de assistente pessoal digital**): A empresa **divulga claramente** que exige que **habilidades disponíveis** em sua loja de habilidades forneçam uma **política de conteúdo publicitário**?

Orientação: Empresas que permitem publicidade em seus serviços e produtos devem divulgar claramente as regras sobre quais tipos de conteúdo publicitário são proibidos – por exemplo, anúncios que discriminem contra indivíduos ou grupos baseados em características pessoais como idade, religião, gênero e etnia. Empresas deveriam ser transparentes sobre essas regras para que tanto usuários quanto anunciantes entendam o que é ou não permitido nos anúncios, e assim possam responder pelo conteúdo dos anúncios que aparecem em seus serviços e

plataformas.

Portanto, empresas deveriam tornar essas regras fáceis de localizar (E1), fáceis de entender (E3) e disponíveis nas línguas principais da jurisdição nacional da empresa (E2). Empresas que operam ecossistemas de dispositivos móveis (Apple iOS, Google Android, e a implementação do Android pela Samsung) e assistentes digitais pessoais (Alexa da Amazon, AliGenie do Alibaba) devem permitir que usuários escolham quais aplicativos ou habilidades baixar com base em sua participação (ou não) em redes de publicidade. Portanto, o Elemento 4 e o Elemento 5 perguntam se a empresa divulga que exige que aplicativos ou habilidades disponíveis em sua loja de habilidades forneçam aos usuários uma política de conteúdo publicitário.

Possíveis fontes:

- Política de publicidade da empresa
- Central de ajuda de negócios da empresa
- Termos de uso da empresa

L1(c). Acesso às políticas de publicidade direcionada

A empresa deveria oferecer **políticas de publicidade direcionada** **fáceis de localizar** e **fáceis de entender**.

Elementos:

1. A **política de publicidade direcionada** da empresa é **fácil de localizar**?

2. A **política de publicidade direcionada** da empresa está disponível no idioma principal dos usuários da jurisdição nacional da empresa?

3. A **política de publicidade direcionada** da empresa é apresentada de **maneira compreensível**?

4. (Para **ecossistemas de dispositivos móveis**): A empresa **divulga claramente** que exige que aplicativos disponibilizados em sua **loja de aplicativos** forneçam aos usuários uma **política de publicidade direcionada**?

5. (Para **ecossistemas de assistentes digitais pessoais**): A empresa divulga claramente que exige que **habilidades** disponibilizadas em sua **loja de habilidades** forneçam aos usuários uma **política de publicidade direcionada**?

Orientação: Além de fornecer políticas de conteúdo publicitário acessíveis (Indicador L1b), empresas também devem divulgar suas políticas de publicidade direcionada. A capacidade de anunciantes ou terceiros de direcionar conteúdo personalizado aos usuários – baseados em

seus comportamentos de navegação, informações de localização e outros dados e características inferidos sobre eles[18] – pode moldar (ou distorcer, em alguns casos) significativamente o ecossistema online de um usuário. O direcionamento, que pode incluir tanto conteúdo pago quanto não pago, pode ampliar inequidades sociais offline e pode ser explicitamente discriminatório. Também pode resultar em "bolhas", bem como amplificar conteúdo problemático, incluindo conteúdo criado para induzir ao erro ou espalhar mentiras[19].

Portanto, empresas que permitem que anunciantes e terceiros direcionem publicidade a seus usuários com anúncios personalizados devem publicar políticas de direcionamento que os usuários possam localizar e entender facilmente, e que elas estejam disponíveis nas principais línguas do mercado consumidor. Usuários deveriam ter acesso e entender essas regras para que possam tomar decisões informadas sobre o conteúdo publicitário que estão recebendo. Para ecossistemas de dispositivos móveis e assistentes digitais pessoais, empresas devem divulgar que exigem que aplicativos e habilidades disponibilizados em suas lojas virtuais forneçam aos usuários uma política de publicidade direcionada acessível.

Possíveis fontes:

- Política de anúncios da empresa
- Central de ajuda de negócios da empresa
- Termos de uso da empresa

L1(d). Acesso às políticas de uso de sistemas de algoritmos

A empresa deveria oferecer aos usuários políticas relacionadas ao uso de **algoritmos** que sejam **fáceis de localizar** e **entender**.

Elementos:

1. A **política de uso de sistemas de algoritmos** da empresa é **fácil de localizar**?

2. A **política de uso de sistemas de algoritmos** está disponível no idioma principal dos usuários da jurisdição nacional da empresa?

3. A **política de uso de sistemas de algoritmos** está apresentada de **maneira compreensível**?

[18] Para mais informações sobre política de inferência de dados, ver Seção 6.2 do "2020 Pilot Study and Lessons Learned," (em tradução livre, "Estudo piloto e lições aprendidas, 2020"), *Ranking Digital Rights*, 16 de março de 2020, 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," (em tradução livre, "Minuta de indicadores: Parâmetros de transparência e responsabilidade para publicidade direcionada e tomada de decisão por algoritmos"), *Ranking Digital Rights*, outubro de 2019, https://rankingdigitalrights.org/wp-content/uploads/2019/10/RDR-Index-Draft-Indicators_-Targeted-advertising-algorithms.pdf.

Orientação: O uso de sistemas de algoritmos pode causar efeitos adversos em direitos humanos fundamentais – e especificamente no direito à liberdade de expressão e informação como também no direito de não discriminação[20]. Além de se comprometer claramente a respeitar e proteger direitos humanos ao desenvolver e implementar essas tecnologias (ver Indicador G1, Elemento 3), empresas também deveriam publicar políticas que descrevam claramente os termos que orientam o uso de sistemas de algoritmos em seus serviços e plataformas. Semelhante aos termos de serviço ou acordos de uso que descrevam os termos sob os quais um conteúdo ou atividades são proibidos, empresas que usam sistemas de algoritmos com o potencial de causar violações de direitos humanos deveriam publicar uma política clara e acessível expondo a natureza e funções desses sistemas. Como recomendado pelo Conselho Europeu na *Recomendação sobre os impactos de sistemas de algoritmos aos direitos humanos* (2020), essa política deveria ser fácil de encontrar, ser apresentada em linguagem simples e conter opções para que os usuários administrem as configurações.

Note-se que, neste indicador, estamos buscando uma política que explique os termos sob quais a empresa implementa sistemas de algoritmos em suas plataformas e serviços. Também esperamos que as empresas divulguem os termos que descrevem como desenvolvem e testam sistemas de algoritmos, conforme tratado no indicador P1b.

Possíveis fontes:

- Política de uso de sistemas de algoritmos
- Orientações para desenvolvimento de sistemas de algoritmos
- Política de privacidade ou política de dados
- Central de ajuda

L2: Notificação de mudanças de política

L2(a). Mudança nos termos de serviço

A empresa deveria **divulgar claramente** que **notificará diretamente** seus usuários quando houver mudança nos termos de serviço, antes que as mudanças entrem em vigor.

Elementos:

1. A empresa **divulga claramente** que **notifica diretamente** usuários sobre todas as mudanças em seus **termos de serviço**?

2. A empresa **divulga claramente** como vai **notificar diretamente** os usuários sobre as mudanças?

[20] "Human Rights Risk Scenarios: Algorithms, machine learning, and automated decision-making," *Ranking Digital Rights*, julho de 2019, https://rankingdigitalrights.org/wp-content/uploads/2019/07/Human-Rights-Risk-Scenarios_-algorithms-machine-learning-automated-decision-making.pdf.

3. A empresa **divulga claramente** o cronograma pelo qual vai **notificar diretamente** os **usuários** sobre as mudanças, antes que entrem em vigor?

4. A empresa mantém um **arquivo público** ou um **registro de alterações**?

Orientação: É comum que empresas mudem seus termos de serviço na medida em que seu negócio evolui. No entanto, essas atualizações, as quais podem se aplicar a regras sobre conteúdos e atividades proibidas, podem impactar significativamente na liberdade de expressão e informação dos usuários. Portanto, esperamos que as empresas se comprometam a notificar seus usuários quando modificarem seus termos e forneçam informações que os ajudem a entender o que as mudanças significam.

Este indicador avalia se as empresas divulgam claramente o método e o cronograma para notificar usuários sobre mudanças nos seus termos de serviço. Esperamos que as empresas se comprometam a notificar os usuários diretamente sobre essas mudanças antes que entrem em vigor. O método pelo qual os usuários serão diretamente notificados pode variar de acordo com o tipo de serviço; esperamos que as empresas notifiquem usuários diretamente de modo que o acesso pelo usuário seja garantido. Para serviços que contenham contas de usuário, notificação direta pode consistir em envio de e-mail ou SMS. Para serviços que não exigem conta de usuário, a notificação direta pode consistir em publicar um aviso com destaque no lugar onde os usuários acessam o serviço. Este indicador também busca evidências de que a empresa fornece registros públicos de termos anteriores para que as pessoas possam entender como os termos da empresa evoluíram ao longo do tempo.

Fontes potenciais:

- Termos de serviço da empresa

L2(b). Mudança nas políticas de conteúdo publicitário

A empresa deveria **divulgar claramente** que **notifica diretamente usuários** quando muda sua **política de conteúdo publicitário** antes que essas alterações entrem em vigor.

Elementos:

1. A empresa **divulga claramente** que **notifica diretamente usuários** sobre mudanças em sua política de conteúdo publicitário?

2. A empresa **divulga claramente** como vai **notificar diretamente** os **usuários** sobre as mudanças?

3. A empresa **divulga claramente** o cronograma pelo qual vai **notificar diretamente** os **usuários** sobre as mudanças antes que entrem em vigor?

4. A empresa mantém um **arquivo público** ou um **registro de alterações**?

5. (Para **ecossistemas de dispositivos móveis**): A empresa **divulga claramente** que exige que aplicativos disponibilizados em sua **loja de aplicativos** **notifiquem** **usuários** quando modificarem sua **política de conteúdo publicitário**?

6. (Para **ecossistemas de assistentes digitais pessoais**): A empresa **divulga claramente** que exige que **habilidades** disponibilizadas em sua **loja de habilidades** **notifiquem** **usuários** quando modificarem sua política de conteúdo publicitário?

Orientação: É comum que empresas mudem suas políticas de conteúdo publicitário na medida em que seu negócio evolui. No entanto, essas mudanças, as quais podem se aplicar a regras sobre conteúdos e atividades proibidas, podem impactar significativamente na liberdade de expressão e informação dos usuários, assim como seu direito à não discriminação. Portanto, esperamos que empresas se comprometam a notificar seus usuários quando modificarem seus termos e que forneçam informações que os ajudem a entender o que essas mudanças significam.

Este indicador avalia se as empresas divulgam claramente o método e o cronograma pelo qual notificam usuários sobre mudanças antes que elas entrem em vigor. O método pelo qual os usuários serão diretamente notificados pode variar de acordo com o tipo de serviço; esperamos que empresas notifiquem usuários diretamente de uma maneira garantida de acesso. Para serviços que contenham contas de usuário, notificação direta pode consistir em envio de e-mail ou SMS. Para serviços que não exigem conta de usuário, a notificação direta pode consistir em publicar um aviso com destaque no lugar onde os usuários acessam o serviço. Este indicador também busca evidências de que a empresa fornece registros públicos de termos anteriores para que as pessoas possam entender como os termos da empresa evoluíram ao longo do tempo.

Possíveis fontes:

- Políticas de publicidade, orientações, termos de uso etc.
- Central de ajuda de publicidade ou business da empresa

L2(c). Mudança nas políticas de publicidade direcionada

A empresa deveria **divulgar claramente** que **notifica diretamente** **usuários** quando muda sua **política de direcionamento de anúncios** antes que essas mudanças entrem em vigor.

Elementos:

1. A empresa **divulga claramente** que **notifica diretamente** **usuários** sobre mudanças em sua **política de publicidade direcionada**?

2. A empresa **divulga claramente** como vai **notificar diretamente** os **usuários** sobre as mudanças?

3. A empresa **divulga claramente** o cronograma pelo qual vai **notificar diretamente** os **usuários** sobre as mudanças antes que entrem em vigor?

4. A empresa mantém um **arquivo público** ou um **registro de alterações**?

5. (Para **ecossistemas de dispositivos móveis**): A empresa **divulga claramente** que exige que aplicativos disponibilizados em sua **loja de aplicativos** **notifiquem diretamente usuários** quando modificarem sua **política de publicidade direcionada**?

6. (Para **ecossistemas de assistentes digitais pessoais**): A empresa **divulga claramente** que exige que os **usuários** sejam **diretamente notificados** quando **habilidades** disponibilizadas em sua **loja de habilidades** tenham mudanças na **política de publicidade direcionada**?

Orientação: É comum que empresas mudem suas políticas de publicidade direcionada na medida em que seu negócio evolui. No entanto, essas mudanças, as quais podem se aplicar a regras sobre conteúdos e atividades proibidas, podem impactar significativamente na liberdade de expressão e informação dos usuários, bem como ao seu direito à não discriminação. Portanto, esperamos que as empresas se comprometam a notificar seus usuários quando modificarem esses termos e a fornecer informações que os ajudem a entender o que as mudanças significam.

Este indicador avalia se as empresas divulgam claramente o método e o cronograma para notificar usuários sobre mudanças antes que entrem em vigor. O método pelo qual os usuários serão diretamente notificados pode variar de acordo com o tipo de serviço; esperamos que empresas notifiquem usuários diretamente de uma maneira garantida de acesso. Para serviços que contenham contas de usuário, notificação direta pode consistir em envio de e-mail ou SMS. Para serviços que não exigem conta de usuário, a notificação direta pode consistir em publicar um aviso com destaque no lugar onde os usuários acessam o serviço. Este indicador também busca evidências de que a empresa fornece registros públicos de termos anteriores para que as pessoas possam entender como os termos da empresa evoluíram ao longo do tempo.

Possíveis fontes:
- Políticas de publicidade, orientações, termos de uso etc.
- Central de ajuda de publicidade ou business da empresa

L2(d). Mudança nas políticas de uso de sistemas de algoritmos

A empresa deveria **divulgar claramente** que **notifica diretamente** os **usuários** quando muda

sua **política de uso de sistemas de algoritmos** antes que essas mudanças entrem em vigor.

Elementos:

1. A empresa **divulga claramente** que **notifica diretamente** os **usuários** sobre mudanças em sua **política de uso de sistemas de algoritmos**?

2. A empresa **divulga claramente** como vai **notificar diretamente** os usuários sobre as mudanças?

3. A empresa **divulga claramente** o cronograma pelo qual vai **diretamente notificar usuários** sobre as mudanças antes que elas entrem em vigor?

4. A empresa mantém um **arquivo público** ou um **registro de alterações**?

Orientação: Quando uma empresa muda suas políticas de uso de algoritmos, essas mudanças podem afetar o direito dos usuários à liberdade de expressão e informação e seu direito à não discriminação. Empresas, portanto, devem se comprometer a notificar usuários quando modificarem essas políticas e a fornecer aos usuários informações que os ajudem a entender o que essas mudanças significam. Este parâmetro está de acordo com a *Recomendação sobre os impactos de sistemas de algoritmos aos direitos humanos* (2020) do Conselho Europeu.

Este indicador avalia se as empresas divulgam claramente o método e o cronograma para notificar usuários sobre mudanças antes que elas entrem em vigor. O método pelo qual os usuários serão diretamente notificados pode variar de acordo com o tipo de serviço; esperamos que empresas notifiquem usuários diretamente de uma maneira garantida de acesso. Para serviços que contenham contas de usuário, notificação direta pode consistir em envio de e-mail ou SMS. Para serviços que não exigem conta de usuário, a notificação direta pode consistir em publicar um aviso com destaque no lugar onde os usuários acessam o serviço. Este indicador também busca evidências de que a empresa fornece registros públicos de termos anteriores para que as pessoas possam entender como os termos da empresa evoluíram ao longo do tempo.

Possíveis fontes:

- Políticas de uso de sistemas de algoritmos
- Orientações para o desenvolvimento de sistemas de algoritmos
- Política de privacidade ou política de dados
- Central de ajuda

L3: Processo de aplicação de políticas

L3(a). Processo de aplicação dos termos de serviço

A empresa deve **divulgar claramente** as circunstâncias nas quais ela pode restringir **conteúdo** ou **contas de usuários**.

Elementos:

1. A empresa **divulga claramente** que tipos de **conteúdo** ou atividades não são permitidos?

2. A empresa **divulga claramente** as razões pelas quais ela pode **restringir a conta de um usuário**?

3. A empresa **divulga claramente** informações sobre os processos que utiliza para identificar **conteúdo** ou **contas** que violam as regras da empresa?

4. A empresa **divulga claramente** como utiliza **sistemas de algoritmos** para **identificar** conteúdo que viola as regras da empresa?

5. A empresa **divulga claramente** se alguma autoridade governamental recebe atenção prioritária quando se trata de **identificação** de **conteúdo** para ser restringido por violar as políticas da empresa?

6. A empresa **divulga claramente** se alguma autoridade privada recebe atenção prioritária quando se trata de **identificação** de **conteúdo** a ser restringido por violar as regras da empresa?

7. A empresa **divulga claramente** o processo para aplicar suas regras uma vez que violações são detectadas?

Orientação: É justo esperar que empresas estabeleçam regras proibindo um conteúdo ou atividades – como discurso tóxico ou comportamento malicioso. No entanto, quando empresas desenvolvem ou aplicam regras sobre o que as pessoas podem ou não podem dizer na internet – ou se elas podem ou não acessar um serviço como um todo –, devem fazê-lo de forma transparente e responsável.

Portanto, esperamos que empresas divulguem claramente quais são essas regras e como elas se aplicam. Isso inclui informações sobre como empresas tomam conhecimento sobre material ou atividades que violam seus termos. Por exemplo, empresas podem depender de terceirizados para revisar conteúdo e/ou atividades dos usuários. Podem também depender de mecanismos de alerta vindo da comunidade, os quais permitem que usuários sinalizem conteúdo ou atividade de outros usuários para análise da empresa. Elas também podem implementar sistemas de algoritmos para detectar e identificar violações, e em casos assim as empresas devem explicar como esses sistemas são usados e em quais tipos de conteúdo. Esperamos que as empresas divulguem claramente se mantêm uma política prioridade a pedidos de autoridades governamentais, membros de organizações privadas ou outras

entidades que identificam sua filiação quando denunciam conteúdo ou usuários por alegadamente violar as regras da empresa. Para ecossistemas de dispositivos móveis, esperamos que empresas divulguem que tipo de aplicativos seriam restringidos. Para assistentes pessoais digitais, esperamos que empresas divulguem quais habilidades e resultados de busca elas restringiriam. Nessa divulgação, a empresa também deve dar exemplos para ajudar os usuários a entender o que essas regras significam.

Possíveis fontes:

- Termos de serviço da empresa, acordos de usuário
- Política de uso aceitável, diretrizes de comunidade, diretrizes de conteúdo, política de comportamento abusivo ou documento similar que explique as regras que os usuários devem seguir
- Centro de apoio da empresa, central de ajuda, FAQ

L3(b). Regras de conteúdo publicitário e sua aplicação

A empresa deveria **divulgar claramente** suas políticas sobre os tipos de conteúdo publicitário proibidos.

Elementos:

1. A empresa **divulga claramente** que tipos de **conteúdo publicitário** não são permitidos?

2. A empresa **divulga claramente** se exige que todo **conteúdo publicitário** seja rotulado como tal?

3. A empresa **divulga claramente** os processos e tecnologias que usa para identificar **conteúdo publicitário** ou **contas** que violam as regras da empresa?

Orientação: Empresas deveriam divulgar claramente políticas sobre os tipos de conteúdo publicitário proibidos em uma plataforma ou serviço, e os processos para aplicar essas regras. Especificamente, este indicador pergunta se empresas divulgam claramente que tipo de conteúdo publicitário é proibido, se a empresa divulga a exigência de rotular todo conteúdo publicitário como tal, e se divulga seus processos para aplicar essas regras.

Fontes possíveis:

- Portal do anunciante da empresa, política de publicidade, política de publicidade política
- Termos de serviço da empresa, contrato do usuário
- Política de uso aceitável da empresa, diretrizes de comunidade, diretrizes de conteúdo
- Centro de suporte, central de ajuda, FAQ

L3(c). Regras de publicidade direcionada e sua aplicação

A empresa deveria **divulgar claramente** suas políticas sobre que tipos de **publicidade direcionada** são proibidos.

Elementos:

1. A empresa **divulga claramente** se permite que **terceiros** direcionem **conteúdo publicitário** a seus **usuários**?

2. A empresa **divulga claramente** que tipos de **parâmetros de direcionamento** não são permitidos?

3. A empresa **divulga claramente** que não permite que **anunciantes** direcionem conteúdo a indivíduos específicos?

4. A empresa **divulga claramente** quais **categorias de público-alvo para anúncios** geradas por **algoritmos** são avaliadas por humanos antes de serem usadas?

5. A empresa **divulga claramente** informações sobre os processos e tecnologias usadas para identificar **conteúdo publicitário** ou **contas** que violam as regras da empresa?

Orientação: A habilidade de anunciantes e terceiros de direcionar conteúdo personalizado a usuários – baseado em comportamento de navegação, informações de localização e outros dados e características inferidas sobre eles[21] -- pode moldar significativamente o ecossistema online de um usuário. Direcionamento, que pode incluir tanto conteúdo pago e não pago, pode amplificar inequidades sociais offline e ser explicitamente discriminatório. Também pode resultar nas chamadas "bolhas" e espalhar conteúdo problemático, incluindo conteúdo feito com a intenção de enganar ou de espalhar mentiras[22].

Portanto, empresas que permitem que anunciantes e terceiros direcionem anúncios ou conteúdo personalizados deveriam ter políticas claras descrevendo suas regras de conteúdo publicitário. Empresas deveriam divulgar claramente se permitem que terceiros direcionem anúncios personalizados ou outros tipos de conteúdo patrocinado, e quais parâmetros de direcionamento – como usar certos tipos de categorias de público-alvo, entre os quais idade, localização e outras características do usuário – não são permitidos. Empresas também deveriam divulgar seus processos para identificar violações às regras de direcionamento.

[21] Para mais informações sobre políticas de inferência de dados, veja a Seção 6.2 deste relatório. "2020 Pilot Study and Lessons Learned," *Ranking Digital Rights*, 16 de março, 2020, 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*, outubro de 2019, https://rankingdigitalrights.org/wp-content/uploads/2019/10/RDR-Index-Draft-Indicators_-Targeted-advertising-algorithms.pdf.

Possíveis fontes:

- Portal do anunciante da empresa, política de publicidade, política de publicidade política
- Política de uso aceitável da empresa
- Suporte, central de ajuda, FAQ

L4: Dados sobre aplicação de políticas

L4(a). Dados sobre restrições de conteúdo para aplicação de termos de serviço

A empresa deveria **divulgar claramente** e publicar regularmente dados sobre o volume e a natureza das medidas tomadas para **restringir conteúdo** que viole as regras da empresa.

Elementos:

1. A empresa publica dados sobre o número total de itens de **conteúdo restringido** por violar as regras da empresa?

2. A empresa publica dados sobre o número de itens de **conteúdo restringido** com base na regra violada?

3. A empresa publica dados sobre o número de itens de **conteúdo** restringiu com base no formato do conteúdo (ex.: texto, imagem, vídeo, transmissão ao vivo)?

4. A empresa publica dados sobre o número de itens de **conteúdo** que **restringiu** com base no método utilizado para identificar a violação?

5. A empresa publica esses dados pelo menos quatro vezes por ano?

6. Esses dados podem ser exportados como um arquivo de **dados estruturados**?

Orientação: Empresas podem e deveriam estabelecer regras precisas sobre quais tipos de conteúdo não são permitidos em suas plataformas ou serviços. Este indicador espera que empresas divulguem publicamente dados sobre as medidas que tomam para restringir ou até mesmo censurar conteúdo devido a violações às regras da empresa. A publicação desses dados é um primeiro passo essencial para responsabilizar empresas sobre a aplicação de suas próprias regras e pelas medidas que tomam para moderar conteúdo em suas plataformas e serviços.

Empresas deveriam publicar dados sobre o número agregado de itens de conteúdo que restringem, removem ou – no caso de empresas de telecomunicações – conteúdo que bloqueiam ou filtram como resultado de violações de seus termos de serviço. Também

deveriam categorizar esses dados por violação e pelo método – se foi por um programa de identificação pela comunidade ou por automação – através do qual a violação foi detectada. Empresas deveriam publicar esses dados pelo menos quatro vezes por ano, como estabelecido pelos Princípios de Santa Clara, e como um arquivo de dados estruturados.

Possíveis fontes:

- Relatório de transparência da empresa
- Relatório de aplicação de diretrizes de comunidade etc.

L4(b). Dados sobre restrições de contas para aplicação de termos de serviço

A empresa deveria **divulgar claramente** e publicar regularmente dados sobre o volume e a natureza das medidas tomadas para **restringir contas** que violam as regras da empresa.

Elementos:

1. A empresa publica dados sobre o número total de **contas restringidas** por violar as próprias regras da empresa?

2. A empresa publica dados sobre o número de **contas restringidas** com base na regra violada?

3. A empresa publica dados sobre o número de **contas restringidas** com base no método utilizado para identificar a violação?

4. A empresa publica esses dados pelo menos quatro vezes por ano?

5. Os dados podem ser exportados como um arquivo de **dados estruturados**?

Orientação: Empresas podem e devem estabelecer regras claras sobre que tipos de conteúdo não são permitidos em suas plataformas ou serviços. Este indicador espera que empresas divulguem publicamente dados sobre as ações que tomam para aplicar essas regras. A publicação desses dados é um primeiro passo essencial para responsabilizar empresas pela aplicação de suas próprias regras e pelas medidas que tomam para moderar conteúdo em suas plataformas e serviços.

Empresas deveriam publicar dados sobre o número de contas restringidas por motivo de violações a seus termos de serviço. Deveriam também categorizar esses dados por violação e pelo método de identificação – se foi por um programa de identificação pela comunidade ou por automação – através do qual a violação foi detectada. Empresas deveriam publicar esses dados pelo menos quatro vezes por ano, como estabelecido pelos Princípios de Santa Clara, e como um arquivo de dados estruturados.

Possíveis fontes:

- Relatório de transparência da empresa

L4(c). Dados sobre aplicação de políticas de conteúdo publicitário e publicidade direcionada

A empresa deveria **divulgar claramente** e publicar dados regularmente sobre o volume e a natureza das medidas tomadas para **restringir conteúdo publicitário** que viole as **políticas de conteúdo publicitário** e as **políticas de publicidade direcionada**.

Elementos:

1. A empresa publica o número total de **anúncios** que **restringiu** com fins de aplicação das **políticas de conteúdo publicitário**?

2. A empresa publica o número de **anúncios** que **restringiu** com base na regra de **conteúdo publicitário** que foi violada?

3. A empresa publica o número total de **anúncios** que **restringiu** com fins de aplicação das **políticas de publicidade direcionada**?

4. A empresa publica o número de **anúncios** que **restringiu** com base na regra de **publicidade direcionada** que foi violada?

5. A empresa publica esses dados pelo menos uma vez por ano?

6. Esses dados podem ser exportados como um **arquivo de dados estruturados**?

Orientação: Os indicadores L3c e L3d perguntam se as empresas divulgam regras claras sobre que tipos de conteúdo publicitário e publicidade direcionada são proibidos, e se as empresas descrevem seus processos de aplicação dessas regras. Este indicador, L4c, pergunta se as empresas publicam evidências de que elas estão aplicando essas regras. As empresas deveriam publicar dados sobre o número total de anúncios removidos por motivo de violações a políticas de conteúdo publicitário. Empresas também deveriam categorizar esses dados por regra violada, como também fornecer evidências de que estão aplicando suas políticas de conteúdo publicitário ao publicar dados sobre o número de anúncios removidos por violação de regras de direcionamento (e categorizá-los por regra violada). Empresas também deveriam publicar esses dados pelo menos uma vez por ano e em um arquivo de dados estruturados.

Fontes possíveis:

- Relatório de transparência da empresa

L5: Processo de resposta a solicitações de terceiros para restrição de conteúdo ou contas

L5(a). Processo de resposta a solicitações governamentais para restrição de conteúdo ou contas

A empresa deveria **divulgar claramente** seu processo para responder a **solicitações governamentais** (incluindo ordens judiciais) para remover, filtrar ou restringir **conteúdo** ou **contas**.

Elementos:

1. A empresa **divulga claramente** seus processos para responder a **solicitações governamentais não judiciais**?

2. A empresa **divulga claramente** seu processo para responder a **ordens judiciais**?

3. A empresa **divulga claramente** seu processo para responder a **solicitações governamentais** de jurisdições estrangeiras?

4. A empresa **divulga** a base legal segundo a qual ela pode vir a acatar **solicitações governamentais**?

5. A empresa **divulga claramente** que faz a devida diligência sobre **solicitações governamentais** antes de decidir como responder?

6. A empresa se compromete a enfrentar **solicitações governamentais** inapropriadas ou amplas demais?

7. A empresa fornece diretrizes claras ou exemplos de implementação de seus processos para responder a **solicitações governamentais**?

Orientação: Empresas frequentemente recebem solicitações de governos para remover, filtrar ou restringir acesso a conteúdo ou contas. Essas solicitações podem vir de agências do governo, da polícia ou de tribunais (tanto domésticos quanto estrangeiros). Esperamos que empresas divulguem claramente seus processos para responder a esse tipo de solicitação. Empresas deveriam divulgar as razões legais segundo as quais cumpririam uma solicitação governamental, assim como divulgar um compromisso em enfrentar solicitações amplas demais.

Note-se que nossa definição de "solicitação governamental" inclui aquelas que vêm de processos "não judiciais", como ordens da polícia, como também solicitações civis de atores privados que têm origem em tribunais civis. Solicitações de exclusão feitas via processos

organizados, como o U.S. Digital Millenium Copyright Act (DMCA) ou o Direito ao Esquecimento da União Europeia, são definidos como "processos privados" e avaliados no indicador L5b a seguir.

Fontes possíveis:

- Relatório de transparência da empresa
- Diretrizes de cumprimento de lei da empresa
- Relatórios anuais da empresa

L5(b). Processo de resposta a solicitações privadas para restrição de conteúdo ou contas

A empresa deveria **divulgar claramente** seu processo de resposta a **solicitações privadas** para remover, filtrar ou restringir **conteúdo** ou **contas**.

Elementos:

1. A empresa **divulga claramente** seu processo de resposta a **solicitações privadas** para remover, filtrar ou restringir **conteúdo** ou **contas**?

2. As explicações da empresa **divulgam claramente** a base segundo a qual ela pode vir a acatar **solicitações** feitas via **processos privados**?

3. A empresa **divulga claramente** que faz a devida diligência sobre **solicitações** feitas via **processos privados** antes de decidir como responder?

4. A empresa se compromete a enfrentar **solicitações** inapropriadas ou amplas demais feitas via **processos privados**?

5. A empresa fornece diretrizes claras ou exemplos de implementação de seu processo de resposta a **solicitações** feitas via **processos privados**?

Orientação: Além de solicitações feitas por governos e outros tipos de autoridades, empresas podem receber solicitações para excluir ou restringir acesso a conteúdo e contas através de processos privados. Essas solicitações podem ser feitas por meio de processos formais estabelecidos em lei (ex.: solicitações feitas sob o U.S. Digital Millenium Copyright Act, o Direito ao Esquecimento da União Europeia etc.) ou via arranjos autorregulatórios (ex.: acordos da empresa para bloquear certos tipos de materiais ou imagens, como aqueles via o EU's Code of Conduct on Disinformation, em tradução livre, "Código de Conduta sobre Desinformação da União Europeia"). Note-se que este indicador não considera solicitações privadas vindas através de qualquer tipo de ordem judicial, as quais são consideradas sob solicitações "governamentais" (Indicador L5a).

Este indicador avalia se a empresa divulga claramente como responde a solicitações para

remover, filtrar ou restringir conteúdo ou contas vindos deste tipo de processo privado (Elemento 1). A empresa deveria divulgar a fundamentação que leva ao acato desse tipo de solicitação (Elemento 2) e divulgar se conduz devida diligência sobre essas solicitações antes de decidir como responder (Elemento 3). Também esperamos que empresas se comprometam a enfrentar solicitações para remover conteúdo ou contas que sejam amplas demais e que venham via processos privados (Elemento 4), e publicar exemplos claros que ilustrem como a empresa lida com esse tipo de solicitação (Elemento 5).

Fontes potenciais:

- Relatório de transparência da empresa
- Centro de ajuda ou suporte
- Blog posts da empresa
- Política da empresa sobre direitos autorais e propriedade intelectual

L6. Dados sobre solicitações governamentais para restrição de conteúdo ou contas

A empresa deveria publicar regularmente dados sobre **solicitações governamentais** (incluindo ordens judiciais) para remover, filtrar ou restringir **conteúdo** ou **contas**.

Elementos:

1. A empresa categoriza as **solicitações** que recebe por país?
2. A empresa lista o número de **contas** afetadas?
3. A empresa lista o número de itens de **conteúdo** ou URLs afetados?
4. A empresa lista os tipos de assuntos associados com as **solicitações** que recebe?
5. A empresa lista o número de **solicitações** que vêm de diferentes autoridades legais?
6. A empresa lista o número de **solicitações** para restringir **conteúdo** ou **contas** que vêm de oficiais de governo em **processos não oficiais**, caso tome conhecimento delas?
7. A empresa lista o número de **solicitações** que acata?
8. A empresa publica as **solicitações** originais ou divulga que fornece cópias a um **arquivo público de terceiros**?
9. A empresa relata esses dados pelo menos uma vez por ano?
10. Os dados podem ser exportados como um arquivo de **dados estruturados**?

Orientação: Empresas frequentemente recebem solicitações do governo para remover, filtrar ou restringir conteúdo ou contas. Esperamos que empresas publiquem regularmente dados sobre o número e tipo de solicitações governamentais que recebem, e o número de solicitações que acatam. Empresas podem receber essas solicitações através de processos oficiais, como uma ordem judicial, ou canais informais, como um sistema de identificação que permite que indivíduos privados denunciem conteúdo que viola os termos de serviço. Empresas deveriam ser transparentes sobre a natureza dessas solicitações. Se uma empresa sabe que uma solicitação vem de uma entidade governamental ou de um tribunal, a empresa deve divulgá-la como parte de um relatório de demandas governamentais. Divulgar esses dados ajuda o público a entender melhor a relação entre empresas e governos quando se trata de policiar conteúdo online, e ajuda o público e o governo a responsabilizar empresas por suas obrigações de respeitar e proteger o direito à liberdade de expressão.

Em alguns casos, a lei pode impedir uma empresa de divulgar as informações pedidas pelos elementos desse indicador. Por exemplo, esperamos que empresas publiquem números exatos em vez de faixas de números. Reconhecemos que leis às vezes impedem as empresas de o fazerem, e pesquisadores vão documentar esses casos. Ainda assim, uma empresa irá perder pontos se ela não atingir os parâmetros especificados em todos os elementos acima. Isso representa uma situação em que uma lei leva empresas a ficar aquém das boas práticas, e nós incentivamos que empresas pleiteiem por leis que as permitam respeitar completamente os direitos de liberdade de expressão e privacidade dos usuários.

Possíveis fontes:

- Relatório de transparência da empresa

L7. Dados sobre solicitações privadas para restrição de conteúdo ou contas

A empresa deveria publicar regularmente dados sobre solicitações para remover, filtrar ou restringir acesso a **conteúdo** ou **contas** que venham através de **processos privados**.

Elementos:

1. A empresa categoriza o número de solicitações para restringir **conteúdo** ou **contas** que recebe através de **processos privados**?

2. A empresa lista o número de **contas** afetadas?

3. A empresa lista o número de itens de **conteúdo** ou URLs afetados?

4. A empresa lista as razões para exclusões associadas com as solicitações que recebe?

5. A empresa **divulga claramente** os **processos privados** que fizeram solicitações?

6. A empresa lista o número de solicitações que acatou?

7. A empresa publica as solicitações originais ou divulga que fornece cópias para um **arquivo público de terceiros**?

8. A empresa relata esses dados pelo menos uma vez por ano?

9. Os dados podem ser exportados como um arquivo de **dados estruturados**?

10. A empresa **divulga claramente** que seu relatório abrange todo tipo de solicitação que recebe via **processos privados**?

Orientação: Empresas frequentemente recebem solicitações para remover, filtrar ou restringir conteúdo ou contas através de processos privados, como solicitações feitas sob o U.S. Digital Millenium Copyright Act, o Direito ao Esquecimento da União Europeia ou por meio de um processo autorregulatório (ex.: acordos da empresa para bloquear certos tipos de imagens). Esperamos que as empresas publiquem regularmente dados sobre o número e o tipo de solicitações recebidas através desses processos privados, e o número de solicitações que acatam.

Fontes potenciais:

- Relatório de transparência da empresa

L8. Notificação de usuários sobre restrição de contas e conteúdo

A empresa deveria **divulgar claramente** que **notifica usuários** quando restringe **conteúdo** ou **contas**.

Elementos:

1. Caso hospede **conteúdo** gerado pelo usuário, a empresa **divulga claramente** que notifica os **usuários** que geraram o **conteúdo** quando este for restringido?

2. A empresa **divulga claramente** que notifica usuários que tentam acessar **conteúdo** que foi restringido?

3. Na notificação, a empresa **divulga claramente** uma razão (legal ou não) pela qual o **conteúdo** foi **restringido**?

4. A empresa **divulga claramente** que notifica usuários quando ela restringe suas **contas**?

Orientação: O Indicador L3 analisa a divulgação da empresa de restrições sobre o que usuários

podem postar ou fazer em um serviço. Este indicador, L8, foca na divulgação de notificação a usuários quando a empresa toma esse tipo de medida (seja devido à aplicação de seus próprios termos de serviço ou devido a uma solicitação vinda de terceiros). A decisão da empresa de restringir ou remover acesso a conteúdo ou contas pode impactar significativamente no direito à liberdade de expressão e acesso à informação dos usuários. Portanto, esperamos que a empresa divulgue que notifica usuários quando ela exclui conteúdo, restringe a conta de um usuário, ou restringe de alguma forma a habilidade do usuário de acessar um serviço. Se a empresa exclui um conteúdo postado por um usuário, esperamos que a empresa informe ao usuário sobre sua decisão. Se um usuário diferente tenta acessar um conteúdo que a empresa restringiu, esperamos que a empresa notifique esse usuário sobre a restrição do conteúdo. Também esperamos que as empresas especifiquem razões para suas decisões. Essa divulgação deve fazer parte da explicação das empresas sobre suas práticas de restrição de conteúdo e acesso.

Possíveis fontes:

- Termos de serviço da empresa, política de uso aceitável
- Diretrizes de comunidade da empresa
- Página de suporte da empresa, central de ajuda, FAQ
- Diretrizes para desenvolvedores da empresa
- Política de direitos humanos da empresa

L9. Gerenciamento de rede (empresas de telecomunicações)

A empresa deveria **divulgar claramente** que não **prioriza**, bloqueia ou atrasa certos tipos de tráfego, **aplicativos**, **protocolos** ou **conteúdo** por nenhuma razão além de garantir qualidade do serviço e confiabilidade da rede.

Elementos:

1. A empresa **divulga claramente** seu compromisso político de não priorizar, bloquear ou atrasar certos de tipos de tráfego, **aplicações**, **protocolos** ou **conteúdo** por razões além de garantir qualidade do serviço e confiabilidade da rede?

2. A empresa adere a práticas que priorizam tráfego de rede por razões que vão além de garantir qualidade do serviço e confiabilidade da rede, como oferecimento de **programas de zero-rating**?

3. Se a empresa adere a práticas de **priorização** de rede por razões além de garantir a qualidade do serviço e confiabilidade da rede, ela **divulga claramente** as razões pelas quais o faz?

Orientação: Esse indicador avalia se as empresas de telecomunicações claramente divulgam que elas aderem a práticas que afetam o fluxo de conteúdo em suas redes, como

estrangulamento ou moldagem de tráfego. Esperamos que essas empresas se comprometam publicamente a evitar priorização ou degradação de conteúdo. Em alguns casos, a empresa adere a práticas de moldagem de tráfego legítimas com o objetivo de garantir o tráfego em suas redes. Esperamos que a empresa divulgue isso publicamente e explique suas razões para tal. Empresas podem praticar priorização paga ou zero-rating, as quais não se enquadram como práticas de gerenciamento de tráfego legítimas. Uma empresa pode ter uma declaração em seu site se comprometendo com a neutralidade da rede, por exemplo, mas também oferecer zero-rating.

Possíveis fontes:

- Políticas de gerenciamento de rede ou gerenciamento de tráfego da empresa
- Relatórios anuais da empresa

L10. Bloqueio ("shutdown") de rede (empresas de telecomunicações)

A empresa deveria **divulgar claramente** as circunstâncias nas quais pode **bloquear ou restringir acesso à rede** ou a **protocolos**, serviços ou aplicações específicas na rede

Elementos:

1. A empresa **divulga claramente** as razões pelas quais pode bloquear um serviço para uma área ou grupo específico de usuários?

2. A empresa **divulga claramente** por que ela pode restringir acesso a **aplicativos** ou **protocolos** específicos (ex.: VoIP, mensagem) em uma área ou um grupo específico de usuários?

3. A empresa **divulga claramente** seus processos de resposta a **solicitações governamentais** para **bloquear uma rede ou restringir acesso a um serviço**?

4. A empresa **divulga claramente** um compromisso em enfrentar **solicitações governamentais** para **bloquear uma rede ou restringir acesso a um serviço**?

5. A empresa **divulga claramente** que notifica usuários diretamente quando **bloqueia uma rede ou restringe acesso a um serviço**?

6. A empresa **divulga claramente** o número de **solicitações de bloqueio de rede** que recebe?

7. A empresa **divulga claramente** a autoridade legal específica que faz as **solicitações**?

8. A empresa **divulga claramente** o número de **solicitações governamentais** que acatou?

Orientação: Bloqueios de rede são uma ameaça crescente aos direitos humanos. O Conselho de Direitos Humanos da ONU condenou bloqueios de rede como uma violação à lei internacional de direitos humanos e pediu a governos que cessem a prática[23]. Ainda assim, governos estão, cada vez mais, ordenando empresas de telecomunicações a bloquear suas redes[24], pressionando, assim, as empresas para tomar medidas que violem sua responsabilidade de respeitar os direitos humanos. Esperamos que as empresas divulguem claramente as circunstâncias nas quais elas venham a tomar essas medidas, que relatem as solicitações recebidas para tomar essas medidas e que divulguem compromissos de enfrentar ou mitigar os efeitos das ordens governamentais.

Possíveis fontes:

- Termos de serviço da empresa
- Relatório de transparência da empresa
- Diretrizes para cumprimento de lei da empresa
- Política de direitos humanos da empresa

L11. Política de identidade

A empresa não deveria **exigir** aos usuários que verifiquem sua identidade com documentos emitidos pelo governo ou outras formas de identificação que possam ser associadas à sua identidade offline.

1. A empresa **exige** que o usuário verifique sua identidade com uma forma de **identificação emitida pelo governo** ou outras formas de identificação que podem associá-lo à sua identidade offline?

Orientação: A habilidade de se comunicar anonimamente é essencial para a liberdade de expressão online ou offline. O uso de um nome real online ou a exigência de que usuários forneçam à empresa informações que os identifiquem fornecem um elo entre atividades online e uma pessoa offline específica. Isso apresenta riscos aos direitos humanos para aqueles que, por exemplo, emitem opiniões que não se alinham com as visões do governo ou praticam um tipo de ativismo que o governo não permite. A prática também põe em risco pessoas que são perseguidas por suas crenças religiosas ou sua orientação sexual.

Portanto, esperamos que empresas divulguem se elas podem vir a pedir aos usuários para verificar sua identidade com documentos emitidos pelo governo ou outras formas de identificação que podem ser associadas à sua identidade offline. Outras formas de identificação

[23] "The promotion, protection, and enjoyment of human rights on the Internet,'' (em tradução livre, "A promoção, proteção e usufruto dos direitos humanos na internet"), *United Nations Human Rights Council* (32nd Session), 27 de junho de 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/, acessado pela última vez em 2 de abril de 2020.

podem incluir cartões de crédito e números de telefone registrados. Reconhecemos que usuários talvez tenham que fornecer informações que podem ser associadas às suas identidades offline para acessar serviços e produtos pagos. No entanto, usuários devem poder acessar recursos que não exigem pagamento sem precisar fornecer informação que pode ser associada à sua identidade offline. Em alguns casos, números de telefone podem ser associados à identidade offline de um usuário, por exemplo, em contextos legais em que usuários pré-pagos devem registrar-se com seu documento de identidade. Quando o fornecimento de um número de telefone é necessário para a provisão do serviço (por exemplo, no caso de aplicativos de mensagens instantâneas), empresas devem receber a pontuação completa do indicador, a não ser que elas também exijam que usuários usem seus nomes reais ou enviem documentos que associem seus nomes a suas identidades offline. Serviços que exigem que usuários forneçam um número de telefone para quaisquer fins além da provisão do próprio serviço não vão receber nenhum ponto: por exemplo, alguns serviços podem exigir números de telefone para propósitos de autenticação de dois fatores, mas isso deve ser opcional; a empresa deve oferecer aos usuários outros tipos de autenticação de dois fatores.

Este indicador é aplicável para empresas de plataformas digitais e serviços de telefonia pré-paga (para empresas de telecomunicações).

Possíveis fontes:

- Termos de serviço da empresa ou documento equivalente
- Central de ajuda da empresa
- Página de cadastro da empresa

L12. Sistemas de curadoria, recomendações e/ou classificação por algoritmos

Empresas deveriam **divulgar claramente** como o **conteúdo** online dos usuários é **curado, classificado ou recomendado**.

Elementos:

1. A empresa **divulga claramente** se usa **sistemas de algoritmos** para **curar, recomendar e/ou classificar** o **conteúdo** que os **usuários** acessam pela plataforma?

2. A empresa **divulga claramente** como seus **sistemas de algoritmos** são implementados para **curar, recomendar e/ou classificar conteúdo**, incluindo as variáveis que influenciam esses sistemas?

3. A empresa **divulga claramente** quais opções os usuários têm para controlar as variáveis que os **sistemas de algoritmos** levam em conta para **curar, recomendar ou classificar conteúdo**?

4. A empresa **divulga claramente** se **sistemas de algoritmos** são usados para **curar, recomendar e/ou classificar conteúdo** automaticamente, sem que o usuário precise aderir a eles?

5. A empresa **divulga claramente** que usuários podem optar por automatizar **sistemas de curadoria, recomendação ou classificação** de **conteúdo**?

Orientação: Sistemas de curadoria, recomendação e classificação desempenham um papel crucial em moldar os tipos de conteúdo e informação usuários veem e acessam online. Além disso, sistemas otimizados para engajamento do usuário podem ter o efeito de priorizar conteúdo controverso e inflamatório, incluindo conteúdo que não está protegido pela lei internacional de direitos humanos. Com o tempo, dependência em sistemas de curadoria e recomendação via algoritmos que são otimizados para engajamento pode alterar o ecossistema de notícias e informação de comunidades e países inteiros. Esses sistemas podem ser manipulados para espalhar desinformação ou de alguma forma distorcer ecossistemas de informação, o que por sua vez pode inflamar violações de direitos humanos.

Empresas deveriam, portanto, ser transparentes quanto ao seu uso de sistemas de curadoria, recomendação e classificação automatizados, incluindo as variáveis que podem influenciar esses sistemas. Empresas deveriam publicar informação sobre se elas usam sistemas de algoritmos para curar, recomendar ou classificar conteúdo. Deveriam divulgar como funcionam, que opções de controle os usuários têm sobre como sua informação é usada por esses sistemas, se esses sistemas são acionados automaticamente sem a necessidade de o usuário aderir aos eles, ou se os usuários podem optar por aderir a um conteúdo automaticamente curado pelo sistema de algoritmo.

Possíveis fontes:

- Política de direitos humanos da empresa
- Política de inteligência artificial da empresa, incluindo princípios, linguagem e diretrizes de uso de IA
- Páginas de ajuda descrevendo como configurações do feed, home page, resultados de busca, recomendações, interesses do usuário ou tópicos são afetados por algoritmos

L13. Agentes de software automatizados (“bots”)

Empresas deveriam **divulgar claramente** as políticas que governam o uso de agentes de software automatizados (“bots”) em suas plataformas, produtos e serviços, e como elas executam essas políticas.

Elementos:

1. A empresa **divulga claramente** as regras que governam o uso de **bots** em sua plataforma?

2. A empresa **divulga** que exige que **usuários** rotulem claramente todo **conteúdo** e todas as **contas** que são produzidas, disseminadas, ou operadas com assistência de um bot?

3. A empresa **divulga claramente** seus processos para executar sua **política de bots**?

4. A empresa **divulga claramente** dados sobre o volume e a natureza do **conteúdo** e **contas** restringidas por violar sua política de bots?

Orientação: Plataformas de redes sociais frequentemente permitem que usuários criem agentes de software, ou "bots", que automatizam diversas ações que uma conta de usuário pode executar, como postar ou promover conteúdo (retuitar, por exemplo). Há muitos usos inofensivos ou até positivos de bots – por exemplo, artistas usam bots no Twitter com objetivo de paródia[25]. Há também usos mais problemáticos que muitas empresas proíbem ou desencorajam, como quando partidos políticos ou seus subsidiários usam redes de bots ("botnets") para promover certas mensagens ou para artificialmente inflar o alcance de certo candidato, manipulando a discussão pública e os resultados. Em algumas redes sociais, bots ou redes de bots coordenados ("botnets") podem ser usadas para assediar usuários ("brigading"), amplificar artificialmente um conteúdo (retuítes em massa etc.) ou de alguma forma distorcer a discussão pública na plataforma. Alguns especialistas têm pedido às empresas que exijam de seus usuários que utilizam bots que os rotulem explicitamente como bots para ajudar a deter essas distorções[26].

Empresas que permitem bots, portanto, deveriam ter políticas claras governando o uso de bots em suas plataformas. Deveriam divulgar se exigem que conteúdo e contas produzidas, disseminadas ou operadas com a assistência de um bot sejam rotulados como tal. Elas também devem esclarecer seu processo para aplicar suas políticas de bot, incluindo publicação de dados sobre o volume e a natureza do conteúdo e contas que são restringidas por violar essas regras.

Possíveis fontes:

- Políticas da plataforma para desenvolvedores
- Automação ou regras de bot
- Relatórios de transparência

[25] *Thinkpiece Bot*, Twitter, https://twitter.com/thinkpiecebot, acessado pela última vez em 2 de abril de 2020.

[26] Engler, A. (2020, January 22). The case for AI transparency requirements (em tradução livre, "Uma defesa de requisitos de transparência para IA"). Brookings Institution. https://www.brookings.edu/research/the-case-for-ai-transparency-requirements/, acessado pela última vez em 2 de abril de 2020.

Privacidade

Indicadores nesta categoria buscam evidências de que, em suas políticas e práticas divulgadas, a empresa demonstra maneiras concretas de respeito ao direito dos usuários à privacidade, conforme articulado na Declaração Universal dos Direitos Humanos[27], no Pacto Internacional sobre Direitos Civis e Políticos[28] e em outros instrumentos internacionais de direitos humanos. As políticas e práticas divulgadas da empresa demonstram como ela age para evitar contribuir com ações que podem interferir com a privacidade dos usuários, exceto nos casos em que essas ações são legais, proporcionais e para um propósito justificável. Elas também devem demonstrar um compromisso robusto com a proteção e a defesa da segurança digital dos usuários. Empresas que obtêm um bom desempenho nestes indicadores demonstram um compromisso robusto com transparência não apenas com relação a como respondem a solicitações de governos e outros, mas também em como determinam, comunicam e executam regras privadas e práticas comerciais que afetam a privacidade dos usuários.

P1: Acesso às políticas que afetam a privacidade dos usuários

P1(a). Acesso às políticas de privacidade

A empresa deveria oferecer **políticas de privacidade** **fáceis de localizar** e **fáceis de entender**.

Elementos:

1. As **políticas de privacidade** da empresa são **fáceis de localizar**?

2. As **políticas de privacidade** estão disponíveis no principal idioma falado pelos usuários da jurisdição nacional da empresa?

3. As políticas estão apresentadas de **maneira compreensível**?

4. (Para **ecossistemas de dispositivos móveis**): A empresa divulga que exige que **aplicativos** disponibilizados em sua **loja de aplicativos** forneçam aos **usuários** uma **política de privacidade**?

5. (Para **ecossistemas de assistentes digitais pessoais**): A empresa divulga que exige que **habilidades** disponibilizadas em sua **loja de habilidades** forneçam aos **usuários** uma **política de privacidade**?

---

[27] "Declaração Universal dos Direitos Humanos," *Nações Unidas*, https://www.un.org/en/universal-declaration-human-rights/, acessado pela última vez em 2 de abril de 2020.
[28] "Pacto Internacional sobre Direitos Civis e Políticos," *UN Human Rights Office of the High Commissioner*, https://www.ohchr.org/en/professionalinterest/pages/ccpr.aspx.

Orientação: Políticas de privacidade tratam de como as empresas coletam, administram, usam e asseguram informações sobre usuários como também informações fornecidas por usuários. Desta forma, empresas devem garantir que usuários possam localizar essas políticas facilmente, além de fazer um esforço para ajudar os usuários a entender o que elas significam. Este indicador espera que empresas publiquem políticas de privacidade que sejam fáceis de encontrar, e que estejam disponíveis nos principais idiomas falados no mercado interno da empresa, e que sejam fáceis de entender. Se a empresa oferece múltiplos produtos e serviços, deve estar claro a quais produtos e serviços as políticas de privacidade se aplicam.
Um documento "fácil de localizar" deve estar facilmente acessível na homepage da empresa ou website do serviço. Deve estar localizado a alguns cliques de distância da homepage ou acessível de alguma forma em local lógico onde os usuários esperariam encontrá-la. Os termos também devem estar disponíveis na(s) principal(is) línguas do mercado interno. Além disso, esperamos que uma empresa tome medidas para ajudar usuários a entender a informação apresentada em suas políticas. Isso pode incluir, mas não se limita a fornecer resumos, dicas ou diretrizes que expliquem o que os termos significam, utilizando títulos de seção, tamanho de fonte legível e outros recursos gráficos que ajudem os usuários a entender o documento, ou escrever os termos em linguagem acessível.

Possíveis fontes:

- Política de privacidade da empresa
- Política de uso de dados da empresa

P1(b). Acesso às políticas de desenvolvimento de algoritmos

A empresa deveria oferecer **políticas de desenvolvimento de sistemas de algoritmos** **fáceis de localizar** e **fáceis de entender**.

Elementos:

1. A **política de desenvolvimento de sistemas de algoritmos** da empresa é **fácil de localizar**?

2. A **política de desenvolvimento de sistemas de algoritmos** está disponível no idioma principal dos usuários?

3. A **política de desenvolvimento de sistemas de algoritmos** está apresentada de **maneira compreensível**?

Orientação: O desenvolvimento e o teste de sistemas de algoritmos podem trazer riscos significativos à privacidade, particularmente quando empresas usam as informações coletadas sobre usuários para desenvolver, treinar e testar esses sistemas sem o consentimento

informado do titular dos dados[29]. Empresas deveriam divulgar claramente as políticas que descrevem o desenvolvimento e o teste de sistemas de algoritmos de uma forma que usuários possam acessar, ler e entender, para que assim possam tomar decisões informadas sobre usar ou não os produtos e serviços de uma empresa.

Possíveis fontes:

- Políticas de uso de sistemas de algoritmos
- Diretrizes para o desenvolvimento de sistemas de algoritmos
- Política de privacidade ou política de dados

P2: Notificações de mudanças

P2(a). Mudanças nas políticas de publicidade

A empresa deveria **divulgar claramente** que **notifica diretamente** os usuários quando muda sua **política de privacidade** antes que essas mudanças entrem em vigor.

Elementos:

1. A empresa **divulga claramente** que **notifica diretamente** usuários sobre mudanças em sua **política de privacidade**?

2. A empresa **divulga claramente** como vai **notificar diretamente** os **usuários** sobre as mudanças?

3. A empresa **divulga claramente** o cronograma pelo qual vai **diretamente notificar usuários** sobre as mudanças, antes que elas entrem em vigor?

4. A empresa mantém um **arquivo público** ou um **registro de alterações**?

5. (Para **ecossistemas de dispositivos móveis**): A empresa **divulga claramente** que exige que aplicativos disponibilizados em sua **loja de aplicativos** notifiquem **usuários** quando modificarem sua **política de privacidade**?

6. (Para **ecossistemas de assistentes digitais pessoais**): A empresa **divulga claramente**

[29] Zuboff, S. (2019). The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power. (em tradução livre, "A era do capitalismo de vigilância: A luta por um futuro humano na nova fronteira do poder"). New York, NY, USA: PublicAffairs; Nathalie Maréchal. Targeted Advertising Is Ruining the Internet and Breaking the World, (em tradução livre, "Publicidade direcionada está arruinando a internet e fragmentando o mundo"), 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*, julho de 2019, https://rankingdigitalrights.org/wp-content/uploads/2019/07/Human-Rights-Risk-Scenarios_-algorithms-machine-learning-automated-decision-making.pdf.

que exige que **habilidades** disponibilizadas em sua **loja de habilidades** notifiquem **usuários** quando modificarem sua **política de privacidade**?

Orientação: Empresas frequentemente modificam suas políticas de privacidade conforme seus negócios evoluem. Entretanto, essas mudanças podem afetar o direito à privacidade dos usuários ao modificar quais informações dos usuários as empresas podem coletar, compartilhar e armazenar. Portanto, esperamos que empresas se comprometam a notificar usuários quando modificarem essas políticas e a fornecer aos usuários informações que os ajudem a entender o que essas mudanças significam.

Este indicador busca uma divulgação clara do método e do cronograma para notificar usuários sobre mudanças na política de privacidade. Esperamos que empresas notifiquem usuários diretamente antes que as mudanças entrem em vigor. O método de notificação direta pode variar de acordo com o tipo de serviço. Para serviços que exigem contas de usuário, notificação direta pode consistir em envio de e-mail ou SMS. Para serviços que não exigem conta de usuário, a notificação direta pode consistir em publicar um aviso com destaque no espaço onde os usuários acessam o serviço. Este indicador também procura evidências de que a empresa fornece registros públicos de termos anteriores para que as pessoas possam entender como os termos da empresa evoluíram ao longo do tempo.

Possíveis fontes:

- Company privacy policy
- Company data use policy

P2(b). Mudanças nas políticas de desenvolvimento de sistemas de algoritmos

A empresa deveria **divulgar claramente** que **notifica diretamente usuários** quando muda sua **política de uso de sistemas de algoritmos**, antes que essas mudanças entrem em vigor.

Elementos:

1. A empresa **divulga claramente** que **notifica diretamente usuários** sobre mudanças em sua **política de uso de sistemas de algoritmos**?

2. A empresa **divulga claramente** como vai **notificar diretamente** os **usuários** sobre as mudanças?

3. A empresa **divulga claramente** o cronograma pelo qual vai **notificar diretamente usuários** sobre as mudanças, antes que elas entrem em vigor?

4. A empresa mantém um **arquivo público** ou um **registro de alterações**?

Orientação: Empresas podem mudar suas políticas de desenvolvimento de sistemas de algoritmos conforme seus negócios evoluem. No entanto, essas mudanças podem ter um impacto significativo no direito à privacidade dos usuários. Esperamos, portanto, que empresas se comprometam a notificar usuários quando modificarem essas políticas e a fornecer aos usuários informações que os ajudem a entender o que essas mudanças significam, como recomendado pelo Conselho Europeu em *Recomendação sobre os impactos de sistemas de algoritmos aos direitos humanos* (2020).

Este indicador busca divulgação clara do método e do cronograma para notificar usuários sobre mudanças na política de privacidade. Esperamos que empresas notifiquem usuários diretamente antes das mudanças entrarem em vigor. O método de notificação direta pode variar de acordo com o tipo de serviço. Para serviços que exigem contas de usuário, notificação direta pode consistir em envio de e-mail ou SMS. Para serviços que não exigem conta de usuário, a notificação direta pode consistir em publicar um aviso com destaque no lugar onde os usuários acessam o serviço. Este indicador também procura evidências de que a empresa fornece registros públicos de termos anteriores para que as pessoas possam entender como os termos da empresa evoluíram ao longo do tempo.

Possíveis fontes:

- Política de uso de algoritmos da empresa
- Política de privacidade ou política de dados

P3: Coleta e inferência de informações do usuário

P3(a). Coleta de informações do usuário

A empresa deveria **divulgar claramente** quais **informações do usuário** coleta e como.

Elementos:

1. A empresa **divulga claramente** que tipo de **informações do usuário** coleta?

2. Para cada tipo de **informação do usuário** que a empresa **coleta**, **divulga claramente** como coleta cada uma delas?

3. A empresa **divulga claramente** que **limita a coleta** de **informações do usuário** para o que é diretamente relevante e necessário para realizar o objetivo do serviço?

4. (Para **ecossistemas de dispositivos móveis**): A empresa **divulga claramente** que avalia se as **políticas de privacidade** de **aplicativos** de terceiros disponibilizados em sua **loja de aplicativos** divulgam quais **informações do usuário coletam**?

5. (Para **ecossistemas de dispositivos móveis**): A empresa **divulga claramente** que avalia

se **aplicativos** de terceiros disponibilizados em sua **loja de aplicativos** **limitam a coleta** de **informações do usuário** para aquilo que é diretamente relevante e necessário para realizar o objetivo do serviço?

6. (Para **ecossistemas de assistentes digitais pessoais**): A empresa **divulga claramente** que avalia se as **políticas de privacidade** de **habilidades** de terceiros, disponibilizadas em sua **loja de habilidades**, divulgam quais **informações do usuário** **coletam**?

7. (Para **ecossistemas de assistentes digitais pessoais**): A empresa **divulga claramente** que avalia se **habilidades** de terceiros, disponibilizadas em sua **loja de habilidades**, **limitam** a **coleta** de **informações do usuário** para aquilo que é diretamente relevante e necessário para realizar o objetivo do serviço?

Orientação: Empresas coletam uma grande variedade de informações pessoais de usuários – de detalhes pessoais e perfis de conta a atividades e localização. Esperamos que empresas divulguem claramente quais informações do usuário coletam e como o fazem. Também esperamos que empresas se comprometam ao princípio da minimização de dados e demonstrem como esse princípio orienta suas práticas com relação às informações do usuário. Se as empresas coletam muitos tipos de informação, esperamos que forneçam detalhes sobre como administram cada tipo de informação. Para ecossistemas de dispositivos móveis e de assistentes digitais pessoais (PDA), esperamos que a empresa divulgue claramente se as políticas de privacidade dos aplicativos ou habilidades disponibilizados em sua loja virtual especificam quais informações do usuário os aplicativos ou as habilidades coletam, e se essas políticas estão de acordo com princípios de minimização de dados.

Possíveis fontes:
- Política de privacidade da empresa
- Site da empresa ou seção sobre proteção de dados ou coleta de dados

P3(b). Inferência de informações do usuário

A empresa deveria **divulgar claramente** quais **informações do usuário** infere e como.

Elementos:

1. A empresa **divulga claramente** que tipos de **informação do usuário** **infere** com base nas **informações do usuário coletadas**?

2. Para cada tipo de **informação do usuário** que **infere**, a empresa **divulga claramente** como **infere** cada uma delas?

3. A empresa **divulga claramente** que limita **inferência** de **informações do usuário** para o que é diretamente relevante e necessário para realizar o objetivo do serviço?

Orientação: Além de coletar informações sobre seus usuários, empresas também realizam análises de dados para fazer inferência, ou previsões, sobre os usuários com base nas informações coletadas. Esses métodos podem ser usados para fazer inferências sobre preferências ou características do usuário (como raça, gênero, orientação sexual), e opiniões (inclusive opiniões políticas), ou prever comportamentos de consumo. Sem suficiente transparência ou controle do usuário sobre a inferência de dados, inferências invasivas e não verificáveis não podem ser previstas, compreendidas ou mesmo refutadas pelos usuários[30].

Além de divulgar as informações que coletam, empresas deveriam divulgar que informações inferem e como inferem. Também deveriam se comprometer a apenas inferir informações que sejam relevantes e necessárias para fornecer o serviço. Por exemplo, empresas não devem tentar inferir a religião, orientação sexual ou o estado de saúde dos usuários (por exemplo, enquadrá-los numa categoria de público-alvo com base nessa característica), a não ser que essa informação seja diretamente necessária para realizar o objetivo do serviço.

Possíveis fontes:

- Política de privacidade da empresa, política de cookies
- Site da empresa ou seção sobre proteção e coleta de dados

P4. Compartilhamento de informações do usuário

A empresa deveria **divulgar claramente** quais **informações do usuário** **compartilha** e com quem.

Elementos:

1. Para cada tipo de **informação do usuário** que coleta, a empresa **divulga claramente** se **compartilha** aquela informação?

2. Para cada tipo de **informação do usuário** que **compartilha**, a empresa **claramente divulga** os tipos de **terceiros** com quem ela **partilha** aquela informação?

3. A empresa **divulga claramente** que pode **compartilhar informações do usuário** com governo(s) ou autoridades judiciais?

4. Para cada tipo de **informação do usuário** que compartilha, a empresa **claramente divulga** os nomes dos **terceiros** com quem ela partilha aquela informação?

[30] Para mais informações, veja: Wachter, Sandra and Mittelstadt, Brent, A Right to Reasonable Inferences: Re-Thinking Data Protection Law in the Age of Big Data and AI (October 5, 2018). Columbia Business Law Review, 2019(2), https://ssrn.com/abstract=3248829

5. (Para **ecossistemas de dispositivos móveis**): A empresa **divulga claramente** que avalia se as **políticas de privacidade** de **aplicativos** de **terceiros** disponibilizados em sua **loja de aplicativos** divulgam quais informações dos usuários compartilham?

6. (Para **ecossistemas de dispositivos móveis**): A empresa **divulga claramente** que avalia se as **políticas de privacidade** de **aplicativos** de **terceiros** disponibilizados em sua **loja de aplicativos** divulgam os tipos de **terceiros** com quem **partilham** **informações do usuário**?

7. (Para **ecossistemas de assistentes digitais pessoais**): A empresa **divulga claramente** que avalia se as **políticas de privacidade** de **habilidades** de **terceiros** disponibilizadas em sua loja de habilidades divulgam quais **informações dos usuários** **compartilham**?

8. (Para **ecossistemas de assistentes digitais pessoais**): A empresa **divulga claramente** que avalia se as **políticas de privacidade** de **habilidades** de **terceiros** disponibilizadas em sua **loja de habilidades** divulgam os tipos de **terceiros** com quem **partilham informações do usuário**?

Orientação: Empresas coletam uma grande variedade de informações pessoais de usuários – de detalhes pessoais e perfis de conta a atividades e localização. Empresas também frequentemente partilham essas informações com terceiros, incluindo anunciantes, governos e autoridades judiciais. Esperamos que empresas divulguem claramente quais informações do usuário (da maneira que a RDR define) compartilham e com quem. Empresas deveriam especificar se compartilham informações dos usuários com governos e com entidades comerciais. Para ecossistemas de dispositivos móveis, esperamos que a empresa divulgue claramente se as políticas de privacidade dos aplicativos disponibilizados em sua loja de aplicativos especificam quais informações do usuário eles partilham com terceiros. Empresas que operam ecossistemas de assistentes digitais pessoais (PDA), devem exigir que habilidades de terceiros disponibilizadas em sua loja de habilidades divulguem claramente que tipos de informações são compartilhadas e os tipos de terceiros com quem partilham.

Possíveis fontes:
- Política de privacidade da empresa
- Políticas da empresa relativas a compartilhamento de dados, interações com terceiros

P5. Objetivo da coleta, inferência e compartilhamento de informações do usuário

A empresa deveria **divulgar claramente** o motivo pelo qual **coleta**, **infere** e **compartilha** informações do usuário.

Elementos:

1. Para cada tipo de **informação do usuário** que **coleta**, a empresa **divulga claramente** o

objetivo da **coleta**?

2. Para cada tipo de **informação do usuário** que **infere**, a empresa **claramente divulga** o objetivo da **inferência**?

3. A empresa **claramente divulga** se combina **informações do usuário** de vários serviços da empresa e, caso faça, por qual motivo o faz?

4. Para cada tipo de **informação do usuário** que compartilha, a empresa **claramente divulga** o motivo para fazê-lo?

5. A empresa **claramente divulga** que limita o uso de **informações do usuário** apenas para o motivo pelo qual foram **coletadas** ou **inferidas**?

Orientação: Esperamos que empresas divulguem claramente o motivo para coletar, compartilhar ou inferir cada tipo de informação de usuário que coletam, compartilham e inferem. Além disso, muitas empresas possuem ou operam uma variedade de produtos ou serviços, e esperamos que divulguem claramente como as informações dos usuários podem ser compartilhadas ou combinadas entre esses serviços. Empresas deveriam se comprometer publicamente ao princípio de limitação do uso – o que significa declarar publicamente em suas políticas que elas apenas usam dados pelos motivos especificados –, de acordo com as regras de privacidade da OCDE, o Regulamento Geral de Proteção de Dados da União Europeia (GDPR) e outros regimes jurídicos, para as informações do usuário que coletam e que inferem.

Possíveis fontes:

- Política de privacidade da empresa

P6. Retenção de informações do usuário

A empresa deveria **divulgar claramente** por quanto tempo **retém** **informações do usuário**.

Elementos:

1. Para cada tipo de **informação do usuário** que coleta, a empresa **claramente divulga** por quanto tempo **retém** essa informação?

2. A empresa **divulga claramente** quais informações **desidentificadas** do **usuário** retém?

3. A empresa **claramente divulga** o processo pelo qual **desidentifica** **informações do usuário**?

4. A empresa **claramente divulga** que exclui todas as **informações do usuário** após os usuários cancelarem suas contas?

5. A empresa **divulga claramente** o cronograma conforme o qual vai remover as **informações do usuário** após os usuários cancelarem suas contas?

6. (Para **ecossistemas de dispositivos móveis**): A empresa **divulga claramente** que avalia se as **políticas de privacidade** de **aplicativos de terceiros** disponibilizados em sua **loja de aplicativos** divulgam por quanto tempo retêm **informações do usuário**?

7. (Para **ecossistemas de dispositivos móveis**): A empresa **divulga claramente** que avalia se as **políticas de privacidade** de **aplicativos de terceiros** disponibilizados em sua **loja de aplicativos** declaram que todas as **informações do usuário** são excluídas quando os usuários cancelam suas contas ou excluem o **aplicativo**?

8. (Para **ecossistemas de assistentes digitais pessoais**): A empresa **divulga claramente** que avalia se as **políticas de privacidade** de **habilidades** de **terceiros** disponibilizadas em sua **loja de habilidades** divulgam por quanto tempo retêm **informações do usuário**?

9. (Para **ecossistemas de assistentes digitais pessoais**): A empresa **divulga claramente** que avalia se as **políticas de privacidade** de **habilidades** de **terceiros** disponibilizadas em sua **loja de habilidades** declaram que todas as **informações do usuário** são excluídas quando os usuários cancelam suas contas ou excluem a **habilidade**?

Orientação: Assim como esperamos que empresas divulguem quais informações coletam e compartilham sobre nós, também esperamos que empresas divulguem claramente por quanto tempo as retêm e até que ponto removem identificadores das informações dos usuários que armazenam. Além disso, usuários também deveriam ser capazes de entender o que acontece com suas informações quando cancelam, rescindem suas contas. Em alguns casos, leis ou regulamentos podem exigir que empresas retenham certas informações por um determinado período. Nesses casos, as empresas deveriam divulgar claramente esses regulamentos aos usuários. Empresas que decidem reter informações dos usuários por longos períodos também deveriam tomar medidas para assegurar que os dados não estejam associados a um usuário específico. Ainda que reconheçamos os debates atuais sobre a eficácia de processos de desidentificação, e a crescente sofisticação de práticas de reidentificação, seguimos considerando a desidentificação uma medida positiva que as empresas podem tomar para proteger a privacidade de seus usuários.

Além disso, se as empresas coletam muitos tipos de informações, esperamos que divulguem claramente por quanto tempo retêm cada um. Para ecossistemas de dispositivos móveis e de assistentes digitais pessoais (PDA), esperamos que as empresas divulguem se as políticas de privacidade de aplicativos móveis ou habilidades de PDA disponibilizadas em suas respectivas lojas virtuais declaram por quanto tempo o aplicativo ou habilidade retém informações dos usuários e se todas as informações são excluídas quando o usuário rescinde sua conta ou exclui o aplicativo ou a habilidade.

Possíveis fontes:

- Política de privacidade da empresa
- Website da empresa ou seção sobre proteção de dados ou coleta de dados

P7. Controle do usuário sobre sua própria informação

A empresa deveria **divulgar claramente** para os usuários quais **opções eles têm para controlar** a **coleta**, **inferência**, **retenção** e o uso de suas **informações** pela empresa.

Elementos:

1. Para cada tipo de **informação do usuário** que **coleta**, a empresa **divulga claramente** se os **usuários** podem controlar a **coleta** dessas **informações**?

2. Para cada tipo de **informação do usuário** que **coleta**, a empresa **divulga claramente** se **usuários** podem excluir essas **informações**?

3. Para cada tipo de **informação do usuário** que a empresa **infere** com base em **informações coletadas**, a empresa **claramente divulga** se **usuários** podem decidir se a empresa pode inferir cada uma delas?

4. Para cada tipo de **informação do usuário** que a empresa **infere** com base em **informações coletadas**, a empresa **claramente divulga** se **usuários** têm a opção de excluir essa **informação**?

5. A empresa **claramente divulga** que fornece aos **usuários** **opções para controlar** como suas **informações** são usadas para **publicidade direcionada**?

6. A empresa **divulga claramente** que **publicidade direcionada** está desativado como padrão, sem que os usuários precisem escolhê-lo?

7. A empresa **divulga claramente** que fornece aos **usuários** **opções para controlar** como suas **informações** são usadas para o desenvolvimento de **sistemas de algoritmos**?

8. A empresa **claramente divulga** que utiliza **informações do usuário** para desenvolver **sistemas de algoritmos** como padrão, sem que o usuário precise optar por isso?

9. (Para **ecossistemas de dispositivos móveis** e **assistentes digitais pessoais**): A empresa **divulga claramente** que fornece aos **usuários** opções de controlar as funções de **geolocalização** do dispositivo?

Orientação: Esperamos que empresas divulguem claramente quais opções os usuários têm

para controlar as informações que as empresas coletam, retêm e inferem sobre eles. Permitir que os usuários controlem quais informações sobre eles a empresa coleta, infere e retém significa dar aos usuários a habilidade de excluir tipos específicos de informação sem exigir que a exclusão da conta por completo. Portanto, esperamos que empresas divulguem claramente se os usuários têm a opção de excluir tipos específicos de informação. Além disso, esperamos que a empresa permita aos usuários controlar o uso de suas informações para fins de publicidade direcionada e desenvolvimento de sistemas de algoritmos. Publicidade direcionada exige vasta coleta, retenção e inferência de informações dos usuários, e empresas devem, portanto, divulgar claramente se os usuários têm opções de controlar como suas informações estão sendo usadas para esses fins.

Para ecossistemas de dispositivos móveis e assistentes digitais pessoais (PDA), esperamos que as empresas divulguem claramente quais opções usuários têm para controlar a coleta de informações de localização. A localização de um usuário muda frequentemente, e muitos usuários levam seus dispositivos móveis consigo por toda parte, tornando a coleta desse tipo de informação particularmente sensível. Além disso, as configurações de localização em ecossistemas de dispositivos móveis e de assistentes digitais pessoais pode influenciar como outros produtos e serviços acessam essa informação. No entanto, se o dispositivo em que esses aplicativos ou habilidades de PDA operam coleta informações de geolocalização como padrão (sem que o usuário opte por isso) e não dá aos usuários uma forma de desativá-la, usuários talvez não possam limitar a coleta de suas informações de localização por aplicativos móveis ou habilidades de PDA. Por essas razões, esperamos que as empresas divulguem que os usuários possam controlar como seus dispositivos interagem com informações de localização.

Possíveis fontes:

- Política de privacidade da empresa
- Página de configurações de conta da empresa, painéis de privacidade
- Central de ajuda da empresa

P8. Acesso dos usuários às próprias informações

Empresas deveriam permitir que usuários obtenham todas as **informações do usuário** que são mantidas pela empresa.

Elementos:

1. A empresa **divulga claramente** que os usuários podem obter uma cópia de suas **informações**?

2. A empresa **divulga claramente** quais **informações do usuário** os **usuários** podem obter?

3. A empresa **divulga claramente** que **usuários** podem obter suas **informações do**

usuário em um arquivo de **dados estruturados**?

4. A empresa **divulga claramente** que **usuários** podem obter todas as **informações** públicas e privadas sobre eles mantidas pela empresa?

5. A empresa **divulga claramente** que **usuários** podem acessar a lista de **categorias de público-alvo de publicidade** às quais foram atribuídos pela empresa?

6. A empresa **divulga claramente** que **usuários** podem obter todas as informações que a empresa **inferiu** sobre eles?

7. (Para **ecossistemas de dispositivos móveis**): A empresa **divulga claramente** que avalia se as **políticas de privacidade** de **aplicativos** de **terceiros** disponibilizados em sua loja de aplicativos divulgam que **usuários** podem obter todas as **informações** mantidas sobre eles pelo aplicativo?

8. (Para **ecossistemas de assistentes digitais pessoais**): A empresa **divulga claramente** que avalia se as **políticas de privacidade** de **habilidades** de **terceiros** disponibilizadas em sua **loja de habilidades** divulgam que **usuários** podem obter todas as **informações** mantidas sobre eles pela habilidade?

Orientação: Usuários deveriam ser capazes de obter todas as informações, tanto as públicas quanto as internas, que empresas mantêm sobre eles, incluindo informações que a empresa usou para fazer inferências ou previsões a seu respeito. Esperamos que empresas divulguem claramente que opções os usuários têm para obter essas informações, que dados esse registro contém e em que formatos usuários podem obtê-las. Empresas também devem permitir que usuários acessem a lista de categorias de público-alvo de publicidade atribuídas a eles. Para direcionar anúncios, empresas normalmente atribuem a cada usuário um número indeterminado de categorias de público-alvo. Anunciantes podem, então, selecionar quais categorias gostariam de utilizar. Usuários deveriam poder saber em que categorias de público-alvo foram colocados, com base nas informações que a empresa coletou ou inferiu sobre eles.

Para ecossistemas de dispositivos móveis, esperamos que empresas divulguem aos usuários se os aplicativos disponibilizados em sua loja especificam que os usuários podem obter todas as informações do usuário que os aplicativos mantêm a seu respeito. Esperamos que empresas que operam lojas de habilidade de assistentes digitais pessoais estabeleçam parâmetros mínimos para habilidades de terceiros que são hospedadas em suas plataformas. Esperamos que as próprias empresas divulguem que os usuários podem obter da empresa um registro de suas próprias informações do usuário, assim como as habilidades de PDA em suas lojas deveriam forneçam divulgação similar aos usuários.

Possíveis fontes:

- Política de privacidade da empresa

- Configurações de conta da empresa
- Central de ajuda da empresa
- Blog posts da empresa

P9. Coleta de informações do usuário por terceiros

A empresa deveria **divulgar claramente** suas práticas com relação à coleta de **informações do usuário** por **meios técnicos** via websites ou **aplicativos** de terceiros, como também **informações** coletadas por **meios não técnicos**.

Elementos:

1. (Para **plataformas digitais**) A empresa **divulga claramente** que **informações do usuário** coleta por **meios técnicos** via terceiros?

2. (Para **plataformas digitais**) A empresa **explica claramente** como coleta **informações do usuário** por **meios técnicos** via **terceiros**?

3. (Para **plataformas digitais**) A empresa **claramente divulga** o objetivo para a coleta de **informações do usuário** por **meios técnicos** via **terceiros**?

4. (Para **plataformas digitais**) A empresa **divulga claramente** por quanto tempo ela retém as **informações do usuário** coletadas por **meios técnicos** via **terceiros**?

5. (Para **plataformas digitais**) A empresa **claramente divulga** que respeita sinais gerados pelo usuário para desativar coleta de dados?

6. A empresa **divulga claramente** como coleta **informações do usuário** por **meios não técnicos** via **terceiros**?

7. A empresa **divulga claramente** como coleta **informações do usuário** por **meios não técnicos** via **terceiros**?

8. A empresa **divulga claramente** o objetivo para a coleta de **informações do usuário** por **meios não técnicos** via **terceiros**?

9. A empresa **divulga claramente** por quanto tempo retém as **informações do usuário** coletadas por **meios não técnicos** via **terceiros**?

Orientação: Esperamos que empresas divulguem quais informações sobre os usuários coletam de terceiros, o que pode significar tanto informação coletada de websites terceiros ou de aplicativos por meios técnicos – por exemplo, através de cookies, plug-ins, widgets – ou através de meios não técnicos, como por meio de contratos. Empresas também podem adquirir

informações de usuários através de meios não técnicos, como contratos, e esses dados podem vir a fazer parte de um "dossiê digital" que as empresas mantêm sobre seus usuários, que podem, por sua vez, formar a base para informações inferidas e compartilhadas. Empresas deveriam ser transparentes e responsáveis sobre essas práticas, de modo que usuários possam entender se e como suas atividades estão sendo rastreadas por empresas, mesmo quando não estão no site da empresa ou quando não são usuários de um serviço ou plataforma específica da empresa.

Possíveis fontes:

- Política de privacidade da empresa
- Política de terceiros ou política de cookies da empresa

P10: Processo de resposta a solicitações de informações do usuário

P10(a). Processo de resposta a solicitações governamentais

A empresa deveria **divulgar claramente** seu processo de resposta a **solicitações** de informações **dos usuários** feitas por **governos**.

Elementos:

1. A empresa **divulga claramente** seus processos para responder a **solicitações governamentais não judiciais**?

2. A empresa **divulga claramente** seu processo para responder a **ordens judiciais**?

3. A empresa **divulga claramente** seu processo para responder a **solicitações governamentais** de jurisdições estrangeiras?

4. A empresa **divulga claramente** a base legal segundo a qual pode vir a acatar **solicitações governamentais**?

5. A empresa **divulga claramente** que faz devida diligência de **solicitações governamentais** antes de decidir como responder?

6. A empresa se compromete a enfrentar **solicitações governamentais** inapropriadas ou amplas demais?

7. A empresa fornece diretrizes claras ou exemplos de implementação de seus processos para responder a **solicitações governamentais**?

Orientação: Empresas cada vez mais recebem solicitações de governos para revelar informações de usuários. Essas solicitações podem vir de agências governamentais ou

tribunais (tanto domésticos quanto estrangeiros). Esperamos que as empresas divulguem claramente seus processos de resposta a solicitações de governos, assim como a base legal segundo a qual podem vir a acatá-las. Empresas também deveriam se comprometer publicamente a resistir a solicitações governamentais inapropriadas ou amplas demais.

Em alguns casos, a lei pode impedir uma empresa de divulgar as informações referenciadas nos elementos deste indicador. Os analistas vão documentar situações em que esse é o caso, mas a empresa irá ainda assim perder pontos se não atingir os parâmetros especificados em todos os elementos. Isso representa uma situação em que uma lei leva empresas a ficar aquém das boas práticas, por isso incentivamos que as empresas pleiteiem por leis que as permitam respeitar completamente os direitos de liberdade de expressão e privacidade dos usuários.

Possíveis fontes:

- Relatório de transparência da empresa
- Diretrizes da empresa de acato a lei
- Política de privacidade da empresa
- Relatório de sustentabilidade da empresa
- Blog posts da empresa

P10(b). Processo de resposta a solicitações privadas

A empresa deveria **divulgar claramente** seu processo de resposta a solicitações de **informações dos usuários** feitas via **processos privados**.

Elementos:

1. A empresa **divulga claramente** seus processos para responder a solicitações via **processos privados**?

2. As explicações da empresa **divulgam claramente** a base segundo a qual ela pode vir a acatar solicitações feitas via **processos privados**?

3. A empresa **divulga claramente** que faz devida diligência sobre solicitações feitas via **processos privados** antes de decidir como responder?

4. A empresa se compromete a enfrentar solicitações inapropriadas ou amplas demais feitas via **processos privados**?

5. A empresa fornece diretrizes claras ou exemplos de implementação de seu processo de resposta a solicitações feitas via **processos privados**?

Orientação: Empresas recebem cada vez mais solicitações privadas para revelar informações dos usuários. Essas solicitações são frequentemente informais, feitas por uma entidade não

governamental, que não envolvem ou não vêm através de nenhum processo judicial. De acordo com a Fundação Wikimedia – que publica relatórios de transparência com dados sobre os tipos de solicitações que recebe --, solicitações privadas de informações do usuário incluem casos em que outra empresa envia uma carta ou e-mail pedindo "informações não públicas" de algum usuário. Esse pedido pode incluir o endereço de IP ou o e-mail do usuário.

Este indicador espera que as empresas divulguem seus processos para responder a esse tipo de requisição. Empresas deveriam explicar suas razões para acatar esse tipo de requisição e se comprometer a resistir a solicitações amplas demais.

Possíveis fontes:

- Relatório de transparência da empresa
- Diretrizes de acato a lei da empresa
- Políticas de privacidade da empresa
- Blog posts da empresa

P11: Dados sobre solicitações de informações do usuário

P11(a). Dados sobre solicitações governamentais de informações do usuário

A empresa deveria publicar regularmente dados sobre **solicitações governamentais** de **informações do usuário**.

Elementos:

1. A empresa lista o número de **solicitações governamentais** que recebe por país?

2. A empresa lista o número de **solicitações governamentais** que recebe para informações do usuário armazenadas e para **acesso a comunicações em tempo real**?

3. A empresa lista o número de contas afetadas?

4. A empresa lista se uma requisição solicitou **conteúdo** de comunicações, "**non-content**" ou ambos?

5. A empresa identifica a autoridade judicial específica ou o tipo de procedimento legal através do qual solicitações de autoridades policiais ou de segurança nacional são feitas?

6. A empresa inclui **solicitações governamentais** enviadas por **ordens judiciais**?

7. A empresa lista o número de **solicitações governamentais** que acatou, separadas por

categoria de requisição?

8. A empresa lista que tipos de **solicitações governamentais** está proibida por lei de divulgar?

9. A empresa relata esses dados pelo menos uma vez por ano?

10. Os dados relatados pela empresa podem ser exportados como arquivo de **dados estruturados**?

Orientação: Empresas frequentemente recebem solicitações governamentais para repassar informações do usuário. Essas demandas podem de vir de agências governamentais ou tribunais (tanto domésticos quanto estrangeiros). Esperamos que empresas publiquem regularmente dados sobre o número e tipo de solicitações que recebem, e o número de solicitações que acatam. Empresas deveriam divulgar dados sobre solicitações recebidas por país, incluindo de sua jurisdição nacional e de governos estrangeiros, assim como de agentes policiais ou tribunais. Também esperamos que as empresas indiquem o número de contas afetadas por essas solicitações e separem por categoria as solicitações que acataram. Entendemos que às vezes empresas são proibidas por lei de divulgar solicitações governamentais de informações de usuários. Entretanto, nesses casos, esperamos que empresas relatem quais tipos de demandas governamentais estão proibidas por lei de divulgar. Empresas também deveriam relatar esses dados uma vez por ano e assegurar que possam ser exportados em um arquivo de dados estruturados.

Em alguns casos, a lei pode impedir uma empresa de divulgar as informações pedidas pelos elementos deste indicador. Os analistas vão documentar situações nesse caso, mas a empresa ainda assim perderá pontos se não atingir os parâmetros especificados em todos os elementos. Isso representa uma situação em que uma lei leva empresas a ficar aquém das boas práticas, e por isso incentivamos empresas a pleitear por leis que as permitam respeitar completamente os direitos de liberdade de expressão e privacidade dos usuários.

Possíveis fontes:
- Relatório de transparência da empresa
- Relatório de acato a lei da empresa
- Relatório de sustentabilidade da empresa

P11(b). Dados sobre solicitações privadas de informações do usuário

Empresas deveriam publicar regularmente dados sobre solicitações de **informações do usuário** recebidas via **processos privados**.

Elementos:

1. A empresa lista o número de solicitações de **informações do usuário** que recebe via **processos privados**?

2. A empresa lista o número de solicitações de **informações do usuário** recebidas via **processos privados** que acatou?

3. A empresa relata esses dados pelo menos uma vez por ano?

4. Os dados relatados pela empresa podem ser exportados como arquivo de **dados estruturados**?

Orientação: Empresas recebem cada vez mais solicitações privadas para repassar informações dos usuários. Essas solicitações são frequentemente informais, feitas por uma entidade não governamental que não envolvem ou não vêm através de nenhum processo judicial. De acordo com a Fundação Wikimedia – que publica relatórios de transparência com dados sobre os tipos de solicitações que recebe --, solicitações privadas de informações do usuário incluem casos em que outra empresa envia uma carta ou e-mail pedindo "informações não públicas" de um usuário. Esse pedido pode incluir o endereço de IP ou o e-mail do usuário.

Assim como empresas deveriam publicar dados sobre solicitações governamentais de informações de usuários que recebem, também deveriam publicar dados sobre as solicitações de informações dos usuários que recebem (e aquelas que acatam) via processos privados. Esperamos que empresas publiquem regularmente dados sobre o número e tipo de solicitações que recebem, e o número de solicitações que acatam. Empresas também deveriam relatar esses dados pelo menos uma vez por ano e assegurar que podem ser exportados como arquivo de dados estruturados.

Possíveis fontes:
- Relatório de transparência da empresa
- Relatório de sustentabilidade da empresa
- Relatório de responsabilidade corporativa da empresa

P12. Notificação do usuário sobre solicitações de informações feitas por terceiros

A empresa deveria **notificar** usuários, dentro do que for legalmente possível, quando suas **informações de usuário** forem **solicitadas por governos** e **terceiros**.

Elementos:

1. A empresa **divulga claramente** que notifica usuários quando **entidades governamentais** (**incluindo tribunais e outros órgãos judiciais**) **solicitam** suas **informações de usuário**?

2. A empresa **divulga claramente** que **notifica** usuários quando recebe solicitações de suas **informações** via **processos privados**?

3. A empresa **divulga claramente** as situações em que pode vir a não **notificar** usuários, incluindo uma descrição dos tipos de **solicitações governamentais** que está proibida por lei de revelar aos usuários?

Orientação: Esperamos que as empresas divulguem claramente o compromisso de notificar usuários quando governos e terceiros solicitem dados sobre eles. Entendemos que essas notificações podem não ser possíveis em casos de investigações em curso, entretanto, as empresas deveriam especificar quais tipos de solicitações estão proibidas por lei de divulgar.

Possíveis fontes:

- Relatório de transparência da empresa
- Diretrizes de acato a lei da empresa
- Política de privacidade da empresa
- Política de direitos humanos da empresa

P13. Monitoramento de segurança

A empresa deveria **divulgar claramente** informações sobre seus processos institucionais para garantir a segurança de seus produtos e serviços.

Elementos:

1. A empresa **divulga claramente** que dispõe de sistemas para limitar e monitorar o acesso de funcionários a **informações do usuário**?

2. A empresa **divulga claramente** que tem uma equipe de segurança que realiza auditorias nos produtos e serviços da empresa?

3. A empresa **divulga claramente** que contrata auditorias de segurança externas em seus produtos e serviços?

Orientação: Como as empresas administram e armazenam quantidades imensas de informações sobre seus usuários, elas deveriam dispor de medidas de segurança para garantir que a informação é mantida em segurança. Esperamos que empresas divulguem claramente que dispõem de sistemas para limitar e monitorar o acesso de funcionários às informações dos usuários. Também esperamos que a empresa divulgue claramente que dispõem de equipes de segurança internas e externas para realizar auditorias de segurança em seus produtos e serviços.

Possíveis fontes:

- Política de privacidade da empresa
- Manual de segurança da empresa

P14. Solucionando vulnerabilidades de segurança

A empresa deveria solucionar **vulnerabilidades de segurança** quando elas são descobertas.

Elementos:

1. A empresa **divulga claramente** que dispõe de um mecanismo através do qual **analistas de segurança** podem comunicar vulnerabilidades que descobrirem?

2. A empresa **divulga claramente** o cronograma conforme o qual vai analisar notificações de **vulnerabilidades**?

3. A empresa se compromete a não tomar medidas legais contra **analistas** que comuniquem **vulnerabilidades** dentro dos termos do mecanismo de apresentação de relatório da empresa?

4. (Para ecossistemas de dispositivos móveis e de **assistentes pessoais digitais**): A empresa **divulga claramente** que **atualizações de software**, **patches** de segurança, add-ons ou extensões são baixadas por canal **criptografado**?

5. (Para ecossistemas de dispositivos móveis e empresas de telecomunicações): A empresa **divulga claramente** quais, se houver, alterações fez em um **sistema operacional do dispositivo móvel**?

6. (Para ecossistemas de dispositivos móveis, **ecossistemas de assistentes digitais pessoais** e empresas de telecomunicações): A empresa **divulga claramente** quais, se houver, efeitos tais alterações podem ter na habilidade da empresa de enviar **atualizações de segurança** para seus usuários?

7. (Para ecossistemas de dispositivos móveis e de **assistentes pessoais digitais**): A empresa **divulga claramente** a data até quando continuará a fornecer **atualizações de segurança** para o **dispositivo/sistema operacional (SO)**?

8. (Para ecossistemas de dispositivos móveis e de **assistentes pessoais digitais**): A empresa se compromete a fornecer **atualizações de segurança** para o sistema operacional e outros softwares cruciais por um mínimo de cinco anos a partir do lançamento?

9. (Para ecossistemas de dispositivos móveis**, ecossistemas de assistentes digitais pessoais** e empresas de telecomunicações): Caso utilize um sistema operacional

adaptado de outro sistema existente, a empresa se compromete a fornecer **patches** de segurança em até um mês após uma **vulnerabilidade** de segurança ser anunciada ao público?

10. (Para **ecossistemas de assistentes digitais pessoais**): A empresa **divulga claramente** quais, se houver, **alterações fez em sistema operacional de um assistente digital pessoal**?

11. (Para **ecossistemas de assistentes digitais pessoais**): A empresa **divulga claramente** que efeito, se houver, essas **alterações produzem na habilidade da empresa de enviar atualizações de segurança a seus usuários**?

Orientação: Códigos de computador não são perfeitos. Quando empresas descobrem vulnerabilidades que podem colocar usuários e suas informações em risco, elas deveriam tomar medidas para mitigar essas preocupações. Isso inclui assegurar que as pessoas possam comunicar, para a empresa, quaisquer vulnerabilidades que descubram. Acreditamos ser especialmente importante que empresas forneçam políticas claras a usuários sobre como e quando receberão atualizações de segurança. Além disso, uma vez que provedores de telecomunicações podem alterar sistemas operacionais de dispositivos móveis de código fonte aberto, esperamos que estas empresas divulguem informações sobre o que pode afetar a habilidade de um usuário de acessar atualizações cruciais.

Possíveis fontes:

- Política de privacidade da empresa
- Manual de segurança da empresa
- Fóruns de ajuda da empresa

P15. Vazamento de dados

A empresa deveria divulgar publicamente informações sobre seus processos para solucionar **vazamentos de dados**.

Elementos:

1. A empresa **divulga claramente** que, quando um **vazamento de dados** ocorre, notifica sem atrasos não justificados as autoridades relevantes?

2. A empresa **divulga claramente** seu processo para **notificar** titulares dos dados que possam ter sido afetados por um **vazamento de dados**?

3. A empresa **divulga claramente** quais tipos de medidas toma para solucionar o impacto de um **vazamento de dados** para seus usuários?

Orientação: Empresas deveriam dispor de processos claros e públicos para solucionar vazamentos de dados, incluindo políticas claras para notificar usuários afetados. Considerando que vazamentos de dados podem resultar em ameaças significativas à segurança pessoal e financeira de um indivíduo, além da exposição de informações privadas, empresas deveriam tornar públicos esses processos. Indivíduos podem, então, tomar decisões informadas e considerar os riscos potenciais antes de se registrar para um serviço ou dar à empresa suas informações.

Esperamos que empresas disponham de políticas formais sobre como lidam com vazamentos de dados se e quando ocorrerem, e que tornem pública a informação sobre essas políticas e os compromissos antes de ocorrer um vazamento.

Possíveis fontes:

- Termos de serviço ou política de privacidade da empresa
- Manual de segurança da empresa

P16. Criptografia da comunicação do usuário e de conteúdo privado (plataformas digitais)

A empresa deveria **criptografar** a comunicação e o conteúdo **privado** dos **usuários**, para que eles controlem quem tem acesso.

Elementos:

1. A empresa **divulga claramente** que transmissões de comunicação do usuário são **criptografadas** como padrão, sem que os usuários precisem optar por isso?

2. A empresa **divulga claramente** que transmissões de comunicação do usuário são **criptografadas** utilizando chaves únicas?

3. A empresa **divulga claramente** que usuários podem assegurar seu conteúdo privado através de **criptografia de ponta a ponta** ou **criptografia de disco completo** (quando aplicável)?

4. A empresa **divulga claramente** que **criptografia de ponta a ponta** ou **criptografia de disco completo** está ativada como padrão, sem que o usuário precise optar por isso?

Orientação: Criptografia é uma ferramenta importante para proteger a liberdade de expressão e a privacidade. O Relator Especial da ONU para liberdade de expressão declarou categoricamente que criptografia e anonimato são essenciais para o exercício e a proteção dos

direitos humanos[31]. Esperamos que empresas divulguem claramente se as comunicações do usuário são criptografadas como padrão, se as transmissões são protegidas por "perfect forward secrecy", se usuários têm a opção de ativar criptografia de ponta a ponta, ou se a criptografia está ativada como padrão. Para ecossistemas de dispositivos móveis e de assistentes digitais pessoais, esperamos que empresa divulguem claramente se permitem criptografia de disco completo.

Possíveis fontes:

- Termos de serviço ou política de privacidade da empresa
- Manual de segurança da empresa
- Central de ajuda da empresa
- Relatórios de sustentabilidade da empresa
- Blog oficial da empresa ou comunicados à imprensa

P17. Segurança da conta (plataformas digitais)

A empresa deveria ajudar os usuários a manter suas **contas** seguras.

Elementos:

1. A empresa **divulga claramente** que faz uso de métodos de autenticação avançados para evitar acesso fraudulento?

2. A empresa **divulga claramente** que usuários podem ver sua atividade recente na conta?

3. A empresa **divulga claramente** que **notifica usuários** sobre atividade suspeita de conta e possíveis acessos não autorizados a suas contas?

Orientação: Empresas deveriam ajudar usuários a manter suas contas seguras. Deveriam divulgar claramente que utilizam técnicas de autenticação avançadas para evitar acesso não autorizado a contas e informações dos usuários. Também esperamos que empresas forneçam aos usuários ferramentas para que possam proteger suas contas e saber quando suas contas foram comprometidas.

Possíveis fontes:

- Centro de segurança da empresa
- Páginas de ajuda ou página de ajuda da comunidade
- Página de configurações de conta

[31] "Report on encryption, anonymity, and the human rights framework," (em tradução livre, "Relatório sobre criptografia, anonimidade, e o âmbito dos direitos humanos"), *UN Human Rights Office of the High Commissioner,* https://www.ohchr.org/en/issues/freedomopinion/pages/callforsubmission.aspx, acessado pela última vez em 2 de abril de 2020.

- Blog da empresa

P18. Informar e educar usuários sobre riscos em potencial

A empresa deveria publicar informações para ajudar os usuários a se defender de **riscos à cibersegurança**.

Elementos:

1. A empresa publica materiais práticos que educam os usuários sobre como se proteger de **riscos à cibersegurança** relevantes a seus produtos e serviços?

Orientação: Como empresas mantêm vastas quantidades de dados sobre seus usuários, são frequentemente alvo de atores maliciosos. Esperamos que as empresas ajudem seus usuários a se proteger dessas ameaças. Ações podem incluir publicação de materiais sobre como configurar autenticação avançada de conta ou ajustar configurações de privacidade, como evitar malwares, phishing e ataques de engenharia social, como evitar ou agir em casos de bullying ou assédio online e o que significa "navegação segura". Empresas deveriam apresentar essas orientações em linguagem clara, idealmente combinada com materiais visuais, elaborados para ajudar que os usuários entendam a natureza dos riscos que empresas e usuários enfrentam. Esses materiais podem estar em diversos formatos, incluindo dicas, tutoriais, manuais, FAQs e outros recursos, apresentados de forma que usuários possam entender facilmente.

Possíveis fontes:
- Centro de segurança da empresa
- Páginas de ajuda ou centro de suporte da comunidade
- Blog da empresa

Glossário

Nota: *Este não é um glossário geral. As definições e explicações abaixo foram escritas especificamente para orientar pesquisadores a respeito dos indicadores deste projeto para a avaliação de empresas de TIC.*

Acesso a comunicações em tempo real – Vigilância de uma conversa ou outra comunicação eletrônica em "tempo real", enquanto a conversa está acontecendo, ou intercepção de dados no momento da transmissão. Também chamado às vezes de "escuta" ("wiretap"). Considere a diferença entre uma solicitação para escuta e uma solicitação para acessar dados armazenados. Uma escuta permite que a autoridade policial acesse comunicações futuras, enquanto uma solicitação de dados armazenados dá acesso a registros de comunicações que ocorreram no passado. O governo dos Estados Unidos pode obter acesso em tempo real através do Wiretap Act e do Pen Register Act, ambos parte do Electronic Communications Privacy Act (ECPA); o governo da Rússia pode fazer o mesmo através do "Sistema para Atividades Operativas Investigativas" (SORM, na sigla em inglês).

Algoritmos – Algoritmo é um conjunto de instruções usadas para processar informação e oferecer um resultado baseado nessas instruções. Algoritmos podem ser códigos simples, mas também podem ser incrivelmente complexos, "codificando milhares de variáveis entre milhões de pontos de dados." No contexto de empresas de internet, celulares e telecomunicações, alguns algoritmos – devido à sua complexidade, às quantidades e aos tipos de informações do usuário que os alimentam, e à função de tomada de decisão a que servem – têm implicações significativas nos direitos humanos dos usuários, incluindo liberdade de expressão e privacidade. Veja: "Algorithmic Accountability: A Primer", (em tradução livre, "Responsabilidade de algoritmos: Uma introdução"), Data & Society, https://datasociety.net/wp-content/uploads/2018/04/Data_Society_Algorithmic_Accountability_Primer_FINAL-4.pdf.

Analista de segurança – Alguém que estuda como garantir a segurança de sistemas técnicos e/ou ameaças à segurança de um computador ou rede para encontrar uma solução.

Anunciante – Uma pessoa ou entidade que criou e/ou pagou por conteúdo publicitário. O anunciante geralmente determina os parâmetros de direcionamento de cada anúncio.

Anúncio / Publicidade – Uma mensagem paga por um anunciante para ser exibida para certos usuários, consistindo tanto em conteúdo publicitário como parâmetros de direcionamento.

Aplicativo – Programa ou software autônomo elaborado para servir a um propósito específico; um aplicativo de software, geralmente baixado por um usuário em um dispositivo móvel.

Arquivo público – Um instrumento disponível ao público que contém versões prévias das políticas de uma empresa, como os termos de serviço ou política de privacidade, ou que explica extensivamente cada mudança que a empresa fez nessas políticas.

Arquivo público de terceiros – Idealmente, empresas publicam informações sobre as solicitações que recebem para que o público tenha um melhor entendimento sobre a maneira como conteúdos são restringidos na plataforma. Empresas podem fornecer informação sobre as solicitações que recebem para um arquivo de terceiros, como o Lumen (chamado anteriormente de Chilling Effects), um projeto de pesquisa independente que administra uma base de dados pública contendo solicitações de remoções de conteúdo online. Este tipo de repositório ajuda pesquisadores e público a entender os tipos de conteúdo que têm remoção solicitada, como também um entendimento aprimorado de solicitações legítimas e ilegítimas. Veja: https://cyber.harvard.edu/research/lumen.

Atualização crítica (de software) – Uma correção amplamente divulgada de uma vulnerabilidade da segurança de um produto. Vulnerabilidades de segurança são classificadas de acordo com a gravidade: crítica, importante, moderada ou baixa.

Atualização de segurança – Um reparo amplamente disponibilizado para uma vulnerabilidade de segurança de um produto específico. Vulnerabilidades de segurança são classificadas de acordo com a gravidade: crítica, importante, moderada ou baixa.

Atualização de software – Uma atualização de software (às vezes chamada de "software patch") é o download gratuito de um aplicativo ou conjunto de softwares que fornecem reparos de recursos que não estão funcionando como deveriam ou que adicionam aprimoramentos e compatibilizações secundárias. Uma atualização também pode incluir atualizações de driver que melhoram a operação do hardware ou periféricos, ou dão apoio a novos modelos de periféricos.

Avaliação de Impacto em Direitos Humanos (HRIA) – Trata-se de uma abordagem sistemática de devida diligência. A empresa conduz esses estudos ou avaliações para averiguar como seus produtos, serviços e práticas de negócios afetam a liberdade de expressão e privacidade de seus usuários. Para mais informações sobre Avalições de Impacto em Direitos Humanos e as boas práticas para conduzi-los, veja esta página hospedada no website do Centro de Informação sobre Empresas e Direitos Humanos: https://business-humanrights.org/en/un-guiding-principles/implementation-tools-examples/implementation-by-companies/type-of-step-taken/human-rights-impact-assessments

O Danish Institute for Human Rights desenvolveu uma ferramenta relacionada, chamada Human Rights Compliance Assessment (https://hrca2.humanrightsbusiness.org), e o Business for Social Responsibility (BSR) desenvolveu um guia útil para conduzir uma Avaliação de Impacto em Direitos Humanos: http://www.bsr.org/en/our-insights/bsr-insight-article/how-to-conduct-an-effective-human-rights-impact-assessment

Para orientações específicas para o setor de TIC, veja o capítulo "Business, Human Rights and the Internet: A Framework for Implementation" (em tradução livre, "Negócios, Direitos Humanos e a Internet: Um Marco para Implementação") de Michael Samway no site do projeto: http://rankingdigitalrights.org/resources/readings/samway_hria.

Bloquear ou restringir acesso à rede – Bloqueio de rede ("shutdown") refere-se à suspensão intencional de comunicações eletrônicas ou de internet, incluindo serviços de telecomunicações como telefonia móvel e SMS. Abrange o bloqueio geral de todos os serviços de telefonia móvel e internet em uma determinada área geográfica ou o bloqueio direcionado de serviços específicos, como redes sociais ou aplicativos de mensagem.

Bot / robô – Uma conta online automatizada cujas ações ou posts não são, em sua maior parte, executadas por uma pessoa.

Botnet – Uma rede coordenada de bots que agem em concerto, geralmente porque estão sob o controle da mesma pessoa ou entidade.

Categorias de público-alvo para publicidade – Grupos de usuários, identificados para efeitos de distribuição direcionada de anúncios, que compartilham certas características e/ou interesses, determinados com base em informações do usuário coletadas ou inferidas pela empresa.

Coletar / Coleta – Todas as maneiras pelas quais uma empresa reúne informações sobre usuários. A empresa pode coletar essas informações diretamente em diversas situações, incluindo, por exemplo, quando usuários fazem upload de conteúdo para compartilhamento público, quando enviam números de telefone para verificação de conta, quando transmitem informações pessoais em conversas privadas etc. A empresa também pode coletar essas informações indiretamente, por exemplo, ao guardar registros de dados, informações de contas, metadados e outras informações relacionadas que descrevem usuários e/ou documentam suas atividades.

Compartilhamento – A empresa permite que terceiros acessem informações do usuário, seja fornecendo livremente a um terceiro (ou ao público ou outros usuários) ou vendendo.

Compromisso político – Uma declaração disponível ao público que representa a política oficial da empresa que foi aprovada pelos cargos mais altos da empresa.

Conselho diretor – Supervisão neste nível deveria envolver os membros do conselho na revisão direta de questões relativas à liberdade de expressão e privacidade. Não é necessário que exista um comitê formal, mas a responsabilidade dos membros do conselho em supervisionar as práticas da empresa nessas questões deveria estar articulada e divulgada claramente no website da empresa.

Conta / conta de usuário – Conjunto de dados associados a um usuário específico de um determinado sistema de computador, serviço ou plataforma. Uma conta de usuário é, no mínimo, composta de nome de usuário e senha, os quais são usados para autenticar o acesso do usuário a seus dados.

Conteúdo – Informação contida em uma comunicação por cabos, oral ou eletrônica (ex.: uma conversa que acontece pelo telefone, frente a frente ou texto escrito e transmitido via SMS ou e-mail).

Conteúdo publicitário – Qualquer conteúdo que alguém pagou para uma empresa mostrar para seus usuários.

Cookie(s) – "Os cookies são uma tecnologia da web que permite aos websites reconhecerem seu navegador. Eles foram originalmente criados para os sites oferecerem carrinhos de compra, salvar as preferências ou manter o seu login no site. Eles também permitem o rastreamento e a criação de perfis, de modo que possam reconhecê-lo e aprender mais sobre onde você vai, quais são os dispositivos que utiliza e em que está interessado, mesmo que não tenha uma conta ou feito login nesse site." Fonte: "Surveillance Self Defense: Cookies" (em tradução livre, "Autodefesa contra a vigilância: Cookies"), Electronic Frontier Foundation, https://ssd.eff.org/pt-br/glossary/cookies

Criptografia – Esta medida basicamente esconde o conteúdo das comunicações ou arquivos de forma que apenas quem detém uma chave poderá decifrar o conteúdo. O processo usa um algoritmo para converter a mensagem (plaintext) em formato codificado (cyphertext) de modo que a mensagem aparece como uma série de caracteres aleatórios para qualquer um que a observe. Apenas alguém com a chave criptográfica correta poderá descriptografar a mensagem, revertendo o ciphertext em plaintext. Dados podem ser criptografados para armazenamento e para transmissão.

Por exemplo, usuários podem criptografar dados em seus discos rígidos de forma que apenas aqueles com a chave criptográfica possam decifrar o conteúdo. Além disso, usuários podem enviar e-mail criptografado, o que evitaria que outros vissem o conteúdo durante sua transmissão na rede. Com a criptografia em trânsito (por exemplo, quando um site usa HTTPS), a comunicação entre o usuário e um site é criptografada, de modo que entidades de fora, como o provedor de internet do usuário, só pode ver a visita inicial ao site, mas não o que o usuário comunica naquele site ou visitas a subsites. Veja: http://www.explainthatstuff.com/encryption.html.

Criptografia de disco completo – Criptografia abrangente de todos os dados armazenados em um dispositivo físico, de forma que apenas o usuário é capaz de acessar seu conteúdo ao fornecer senha(s) gerada(s) pelo usuário e/ou outros meios de descriptografia (impressão digital, autenticação de dois fatores, dispositivo físico de autenticação etc.).

Criptografia de ponta a ponta – Com criptografia de ponta a ponta, apenas o remetente e o destinatário podem ler o conteúdo da comunicação criptografada. Terceiros, incluindo a empresa, não são capazes de descodificar o conteúdo.

Curar, recomendar e/ou classificar – A prática de usar algoritmos, aprendizado de máquina e outros sistemas de tomada de decisão automatizada para administrar, moldar e dirigir o fluxo de conteúdo e informação em uma plataforma, geralmente de forma personalizada para cada usuário.

Dados anônimos – Dados que não são, de nenhuma maneira, conectados a outras informações que permitam a identificação de um usuário. A abrangência da definição usada pela Ranking Digital Rights é necessária para refletir diferentes fatos. Em primeiro lugar, analistas experientes são capazes de desanonimizar grandes bases de dados. Isso torna impossíveis quase todas as promessas de anonimização. Basicamente, qualquer dado que possa ser ligado a um "identificador anônimo" não é anônimo; na verdade, esses dados são, em geral, pseudônimos que podem ser conectados à identidade offline de um usuário. Em segundo lugar, metadados podem ser tanto ou mais reveladores sobre as associações e interesses de um usuário do que dados de conteúdo, portanto esses dados são de interesse vital. E em terceiro, entidades que tem acesso a muitas fontes de dados, como data brokers e governos, podem ser capazes de juntar duas ou mais fontes de dados para revelar informações sobre usuários. Portanto, atores sofisticados podem usar dados que parecem anônimos para construir um grande retrato de um usuário.

Dados de localização – Informações coletadas por uma rede ou serviço sobre onde o telefone ou outro dispositivo do usuário está ou estava localizado – por exemplo, rastreamento da localização de um telefone celular através de dados coletados em estações da rede de telefonia ou através de posicionamento de GPS ou Wi-Fi.

Dados estruturados – "Dados que residem em campos fixos em um registro ou arquivo. Base de dados relacionais e planilhas são exemplos de dados estruturados. Embora os dados em arquivo XML não estejam fixados em um local, como em bases de dados tradicionais, são ainda assim estruturados, porque os dados estão etiquetados e podem ser precisamente identificados." Por outro lado, dados não estruturados são dados que "não residem em locais fixas. O termo geralmente se refere a um texto em forma livre, que são onipresentes. Exemplos são documentos de processamento de texto, arquivos em PDF, mensagens de e-mail, blogs, páginas de internet, e sites sociais". Fonte: PC Mag Encyclopedia. "dados estruturados" http://www.pcmag.com/encyclopedia/term/52162/structured-data; "dados desestruturados" http://www.pcmag.com/encyclopedia/term/53486/unstructured-data.

Desenvolvedor / desenvolvedor terceiro – Um indivíduo (ou grupo de indivíduos) que cria um software ou aplicativo que é então disponibilizado na loja de aplicativos de uma empresa.

Desidentificar (informações do usuário) – Este termo se refere a informações do usuário que as empresas coletam e retêm, mas somente após remover ou ocultar informações identificáveis. Isso significa remoção de identificadores explícitos como nomes, e-mail ou números de identidade emitidos pelo governo, assim como endereços de IP, cookies e números únicos de dispositivos.

Discriminação – Para efeitos do Índice da RDR, discriminação refere-se à prática de tratar pessoas, empresas ou produtos de forma diferente, especialmente de forma injusta. Fonte: Cambridge Business English dictionary, https://dictionary.cambridge.org/dictionary/english/discrimination.

Dispositivo / dispositivo manual / dispositivo móvel – Um objeto físico, como um smartphone ou celular convencional, usado para acessar redes de telecomunicação e elaborado para ser levado com o usuário e usado em diversas localizações.

Divulgar claramente – A empresa apresenta ou explica suas políticas e práticas em seu material dirigido ao público, de forma fácil de localizar e entender para usuários.

Documentação – A empresa fornece registros o qual usuários podem consultar, como por exemplo um registro de alterações nos termos de serviço ou na política de privacidade.

Documentos interativos de políticas – Termos de serviço ou políticas de privacidade que são divididos em seções por links, permitindo aos usuários que naveguem diretamente à seção de interesse.

Ecossistema de assistente digital pessoal – Um ecossistema de assistente digital pessoal (PDA) consiste em uma interface impulsionada por uma inteligência artificial instalada em dispositivos digitais que podem interagir com usuários através de texto ou voz para acessar informações na internet e desempenhar certas funções com base em dados pessoais compartilhados pelo usuário. Usuários podem interagir com ecossistemas de PDA através de **habilidades**, que são disponibilizadas por desenvolvedores/fornecedores terceiros ou pelo próprio PDA.

Ecossistema de dispositivo móvel – Conjunto indivisível de produtos e serviços oferecidos por uma empresa de dispositivos móveis, composto do hardware do dispositivo, sistema operacional, loja de aplicativos e conta de usuário.

Engajamento – Interações entre a empresa e as partes interessadas. Empresas ou as partes interessadas podem iniciar essas interações, e podem ocorrer de diversas formas, incluindo reuniões, comunicações etc.

Engajamento com as partes interessadas – Interações entre a empresa e as partes interessadas. Empresas ou partes interessadas podem iniciar essas interações, que podem tomar diversos formatos, incluindo reuniões, outras comunicações etc.

Equipe / programa – Um departamento definido dentro de uma empresa que tem responsabilidade sobre como os produtos e serviços relacionam-se, neste caso, com liberdade de expressão e/ou privacidade.

Estrangulamento ("throttling") – Uma forma brusca de moldagem de tráfego na qual um operador de rede retarda o fluxo de packets na rede. Operadores de celular podem estrangular o tráfego para aplicar limites de dados. Para mais informações, veja: "Data throttling: Why operators slow down your connection speed," (em tradução livre, "Estrangulamento de dados: Por que operadores diminuem a velocidade da sua conexão"), Open Signal, http://opensignal.com/blog/2015/06/16/data-throttling-operators-slow-connection-speed/.

Executivos sêniores – O CEO e/ou outros membros da equipe executiva listados no website da empresa e em outros documentos oficiais, como o relatório anual. Na ausência de uma lista definida pela empresa de sua equipe executiva, outras posições de nível de chefia e aquelas no nível mais alto da gerência (ex.: vice-presidente sênior/executivo, dependendo da empresa) são considerados executivos sêniores.

Explícito – Por exemplo, a empresa declara especificamente seu apoio à liberdade de expressão e privacidade.

Fácil de entender / maneira compreensível – A empresa tomou medidas para ajudar os usuários a entender seus termos de serviço e política de privacidade. Isso inclui, mas não se limita a fornecer resumos, dicas ou orientações que expliquem o que os termos significam, usando títulos de seções, tamanho de fonte legível; usar outros recursos gráficos que ajudem usuários a entender o documento; ou escrever os termos em linguagem acessível.

Fácil de localizar – Os termos de serviço ou a política de privacidade estão localizados em um ou dois cliques da página principal do website da empresa ou do serviço, ou estão num espaço lógico, que os usuários poderão localizar facilmente.

Forward secrecy / Perfect forward secrecy – Um método de criptografia notadamente usado em tráfego HTTPS e em aplicativos de mensagem no qual um novo par de chaves é gerado para cada sessão (HTTPS) ou para cada mensagem trocada entre as partes (aplicativos de mensagem). Assim, ainda que um adversário obtenha uma chave descriptográfica, não poderá descriptografar transmissões ou mensagens anteriores ou futuras daquela conversa. Forward secrecy se distingue de criptografia de ponta a ponta, a qual se refere a dados criptografados "em repouso" nos servidores remotos da empresa. Veja: "Pushing for Perfect Forward Secrecy," (em tradução livre, "Pressionando por Perfect Forward Secrecy"), Electronic Frontier Foundation, https://www.eff.org/deeplinks/2013/08/pushing-perfect-forward-secrecy-

important-web-privacy-protection.

Funcionalidade central – As funções ou usos essenciais de um produto ou serviço. Por exemplo, uma funcionalidade central de um smartphone incluiria fazer e receber chamadas, enviar e receber mensagens de textos e e-mails, baixar e executar apps e acessar a internet.

Funcionário encarregado – Um empregado sênior responsável por um conjunto explícito de riscos e impactos, neste caso, privacidade e liberdade de expressão.

Geolocalização – Identificação da localização geográfica de um objeto no mundo, como um radar, telefone celular ou um terminal de computador conectado à internet. Geolocalização pode se referir à prática de acessar a localização ou à localização em si.

Habilidades – Habilidades são capacidades de assistentes digitais pessoais, orientadas pelo uso da voz, que permitem que usuários realizem certas tarefas ou engajem com conteúdo online através de dispositivos equipados com um assistente digital pessoal. Habilidades dos ecossistemas de assistentes digitais pessoais são similares a aplicativos dos ecossistemas de dispositivos móveis: usuários podem ativar e desativar habilidades integradas ou instalar novas habilidades desenvolvidas por terceiros a partir de lojas de habilidades, parecidas com lojas de aplicativos.

Identificação emitida pelo governo – Um documento oficial com ou sem foto emitido pelo governo que pode ser usado para provar a identidade de uma pessoa. Isto inclui documentos de identidade governamentais ou qualquer forma de documentação que identifique uma pessoa por localização geográfica, família ou comunidade. Também inclui números de telefone, que são, em muitas jurisdições, conectados à identidade offline de uma pessoa.

Indicações geradas pelo usuário – Muitas empresas permitem que usuários rejeitem ("opt-ou") rastreamento por meio de um conjunto específico de cookies. Todavia, se um usuário deletar esses cookies pensando em proteger a privacidade, serão rastreados até que reconfigurem o cookie de "opt-out". Além disso, algumas empresas podem requerer que um usuário instale um add-on no navegador que evite rastreamento. Esses são dois cenários comuns em que o usuário é forçado a adotar indicações geradas especificamente pela empresa, e que, portanto, não serão consideradas. Indicações geradas pelo usuário, por outro lado, são uma mensagem universal de que o usuário não deveria ser rastreado. Atualmente, a principal opção de indicações geradas pelo usuário é o "Do Not Track", mas este verbete deixa a porta aberta para novos modos de um usuário indicar que não deseja ser rastreado. *Ver também: Não Rastrear.*

Inferência de dados – Empresas são capazes de inferir e prever comportamentos, preferências e as vidas privadas de seus usuários ao aplicar análise de big data e tecnologias de tomada de decisão via algoritmos. Esses métodos podem ser usados para inferir preferências e atributos dos usuários (ex.: raça, gênero, orientação sexual) e opiniões (ex.: posicionamentos políticos)

ou prever comportamentos (ex.: para atender a anúncios). Sem suficiente transparência ou controle do usuário sobre inferência de dados, inferências invasivas e não verificáveis podem não ser previstas, compreendidas ou refutadas pelos usuários. Veja: Wachter, Sandra and Mittelstadt, Brent. "A Right to Reasonable Inferences: Re-Thinking Data Protection Law in the Age of Big Data and AI," (em tradução livre, "O direito a inferências razoáveis: Repensando proteção de dados na era da Big Data e IA"), Columbia Business Law Review, 2019(2), https://ssrn.com/abstract=3248829.

Informações do usuário – Qualquer dado que esteja conectado a uma pessoa identificável, ou que possa ser conectado a essa pessoa combinando conjuntos de dados ou utilizando técnicas de extração de dados. Informações do usuário pode ser tanto coletada quanto inferida. Em resumo, informações do usuário são quaisquer dados que documentam as características e/ou atividades do usuário. Essa informação inclui, mas não se limita a, correspondência pessoal, conteúdo gerado pelo usuário, preferências e configurações de conta, dados de registro e acesso, dados sobre as atividades e preferências do usuário coletadas a partir de terceiros seja através de rastreamento de comportamento ou compra de dados, e todas as formas de metadados. Informações do usuário nunca são consideradas anônimas exceto quando incluídas para gerar métricas globais (ex.: número de usuários ativos mensais). Por exemplo, a declaração "nosso serviço tem um milhão de usuários ativos por mês" contém dados anônimos, uma vez que não revela informações suficientes para sabermos quem são esses um milhão de usuários.

Informações do usuário coletadas – Informações do usuário que uma empresa obtém diretamente ou adquire de terceiros.

Iniciativa multissetorial – Uma organização multissetorial legítima inclui e é dirigida por membros de pelo menos três outros setores além do corporativo: sociedade civil, investidores, acadêmicos, representantes de usuários ou consumidores, comunidade técnica e/ou governo. Seu modelo de financiamento conta com mais de um tipo de fonte (corporações, governos, fundações, doações públicas etc.). Sua independência, rigor e profissionalismo são de alto padrão, com forte participação de organizações de direitos humanos com trajetórias sólidas de independência de corporações ou governos. A Global Network Initiative é um exemplo de uma iniciativa multissetorial focada em liberdade de expressão e privacidade no setor de TIC.

Inteligência artificial – O termo apresenta diversos usos e significados. Para efeitos da metodologia da RDR, inteligência artificial refere-se a sistemas que parecem, executam ou imitam funções que em geral subentende-se precisar de inteligência. Exemplos incluem software de reconhecimento facial, processamento de linguagem natural etc. Seu uso por empresas de internet, celulares e telecomunicações tem implicações sobre o direito à liberdade de expressão e informação das pessoas. Veja: "Privacy and Freedom of Expression in the Age of Artificial Intelligence", (em tradução livre, "Privacidade e liberdade de expressão na era da inteligência artificial"), Privacy International, https://privacyinternational.org/sites/default/files/2018-

04/Privacy%20and%20Freedom%20of%20Expression%20%20In%20the%20Age%20of%20Artificial%20Intelligence.pdf

Limitação de uso e finalidade – De acordo com o princípio de minimização de uso e finalidade, entidades que lidam com informações dos usuários podem declarar seu objetivo para tal e devem limitar o uso dessa informação, evitando qualquer outro propósito, a não ser com o consentimento do usuário. *Ver também: Minimização de dados.*

Loja de aplicativos – Plataforma na qual a empresa disponibiliza para download seus próprios aplicativos ou aqueles criados por desenvolvedores terceiros. Uma loja de aplicativos (ou mercado de aplicativos) é um tipo de plataforma de distribuição digital de softwares de computador, frequentemente no contexto de dispositivos móveis.

Loja de habilidades – Plataforma na qual a empresa disponibiliza para download habilidades de produção própria ou criadas por desenvolvedores terceiros. Uma loja de habilidades (ou mercado de habilidades) é um tipo de plataforma de distribuição digital para softwares de computador.

Malware – Um termo guarda-chuva para descrever uma série de softwares hostis ou intrusivos, incluindo vírus de computador, worm, cavalo de troia, ramsomware, spyware, adware, scareware e outros programas maliciosos. Pode vir em forma de códigos executáveis, scripts, conteúdo ativo ou outro software.

Meios não técnicos – Empresas podem obter informações de usuários por meios não técnicos, como compras, acordos de compartilhamento de dados e outras relações contratuais com terceiros. Esses dados podem vir a fazer parte de um "dossiê digital" que as empresas podem manter sobre seus usuários, o qual forma a base para inferir ou compartilhar informações do usuário.

Meios técnicos – Empresas utilizam várias tecnologias, como cookies, widgets e botões, para rastrear as atividades dos usuários em seus serviços e sites e em serviços de terceiros. Por exemplo, uma empresa pode inserir conteúdo em sites de terceiros e coletar informações quando usuários "curtem" ou de alguma forma interagem com esse conteúdo.

Métricas de engajamento – Números descrevendo a popularidade de um conteúdo ou conta na plataforma, por exemplo, seguidores, conexões, contatos, amigos, comentários, curtidas, retuítes etc.

Minimização de dados – De acordo com o princípio da minimização de dados, empresas devem limitar a coleta de informações dos usuários àquilo que for relevante e necessário para realizar um objetivo claramente especificado. V*er também: Limitação de uso e finalidade.*

Moderação de conteúdo – É a prática de revisão de conteúdo gerado por usuários e postados

em sites de internet, redes sociais ou outros veículos online, de forma a determinar a adequação daquele conteúdo para um determinado site, localidade ou jurisdição. O processo pode resultar em remoção ou restrição do conteúdo por um moderador que atua como um agente da plataforma ou site em questão. Cada vez mais empresas dependem, além de moderadores humanos, de sistemas de algoritmos para moderar conteúdo e informação em suas plataformas. Fonte: "Content moderation", Encyclopedia of Big Data, https://doi.org/10.1007/978-3-319-32001-4_44-1.

Modificações no sistema operacional de um dispositivo móvel – Alterações feitas na versão padrão de um sistema operacional móvel que pode afetar as funcionalidades centrais, a experiência do usuário ou o processo de execução de atualizações. Por exemplo, entre as funcionalidades centrais de um smartphone está o envio e recebimento de chamadas, mensagens de texto e e-mails, download e execução de aplicativos e acesso à internet. Isso se aplica a smartphones Android produzidos por empresas que não o Google.

Moldagem de tráfego – Ajustes de fluxo de tráfego em uma rede. Pode envolver retardamento condicional de certos tipos de tráfego. Moldagem de tráfego pode ser usado para propósitos legítimos de gerência de rede (ex.: priorizar tráfego VoIP em detrimento do tráfego normal na web para facilitar comunicação em tempo real) ou por razões que vão de encontro a princípios de neutralidade de rede (ex.: intencionalmente retardar tráfego de vídeo para dissuadir usuários de utilizar aplicativos de banda larga).

Não rastrear – Também conhecido pela sigla em inglês "DNT" ("do not track"), o termo se refere a uma opção nas configurações do navegador do usuário que solicita empresas e terceiros a não "rastreá-los". Em outras palavras, toda vez que o usuário carrega um website, todas as partes envolvidas em disponibilizar aquela página (e geralmente há muitas, especialmente anunciantes) são solicitadas a não coletar ou armazenar nenhuma informação sobre a visita do usuário àquela página. No entanto, esta é apenas uma solicitação; uma empresa pode ignorar uma solicitação de DNT, e muitas o fazem.

Nível administrativo – Um comitê, programa, equipe ou funcionário encarregado que não faz parte do conselho diretor ou equipe executiva da empresa.

Non-content – Dados sobre um episódio de comunicação ou sobre um usuário. Empresas podem usar termos diferentes para se referir a esse tipo de dado, como metadados, informação básica de assinante, dados de transação "non-content", dados da conta ou informações do cliente.

Nos Estados Unidos, o Stored Communications Act define registros "non-content" de comunicação de clientes como "nome; endereço; registros locais ou de longa-distância de telefone, ou registros de horário e duração de sessões; duração do serviço (incluindo data de início) e tipos de serviço utilizados; número de telefone, equipamento ou outro número de assinatura ou identidade (incluindo endereços de rede atribuídos temporariamente); e meio e

fonte de pagamento para tal serviço (incluindo número de cartão de crédito ou conta bancária).” O Manual da Legislação Europeia sobre Proteção de Dados diz que a confidencialidade das comunicações eletrônicas “abrange não apenas o teor da comunicação como também dados de tráfego, tais como informações sobre quem comunicou com quem, quando e por quanto tempo, e dados de localização, tais como o local de onde os dados foram comunicados”. Veja: “18 U.S. Code § 2703. Required disclosure of customer communications or records,” (em tradução livre, “Solicitação de revelação de registros ou comunicações de clientes”), Cornell Law School Legal Information Institute, https://www.law.cornell.edu/uscode/text/18/2703. “Manual da Legislação Europeia sobre Proteção de Dados,” Tribunal Europeu dos Direitos Humanos, https://www.echr.coe.int/Documents/Handbook_data_protection_ENG.pdf.

Notificação / notificar – A empresa comunica ou informa os usuários sobre algo relacionado à empresa ou serviço.

Notificar diretamente / notificação direta – Por notificação direta, queremos dizer que quando uma empresa muda ou atualiza a política de um determinado serviço, esperamos que ela notifique os usuários sobre essas mudanças através do próprio serviço. O método de notificação direta pode variar de acordo com o tipo de serviço. Para serviços que têm contas de usuários, notificação direta pode envolver o envio de e-mail ou SMS. Para serviços que não exigem uma conta, a notificação direta pode envolver a publicação de um aviso destacado na página principal onde usuários acessam o serviço.

Opções de controle – A empresa fornece ao usuário um mecanismo direto e de fácil compreensão para aderir ou rejeitar coleta, uso ou compartilhamento de dados. Dar a opção de aderir (“opt-in”) significa que a empresa não coleta, usa ou compartilha dados com um objetivo determinado antes que os usuários sinalizem explicitamente que eles querem que ela o faça. Dar a opção de rejeitar (“opt-out”) significa que a empresa usa os dados com um objetivo determinado como padrão, mas para de fazê-lo uma vez que o usuário instrui a empresa a parar. Note que essa definição é potencialmente controversa já que muitos defensores da privacidade acreditam que apenas adesão (“opt-in”) constitui controle aceitável. No entanto, para efeitos da RDR, escolhemos considerar rejeição (“opt-out”) como uma forma de controle.

Ordens judiciais – Ordem emitida por um tribunal, em processos civis ou criminais.

Parâmetros de direcionamento – As condições, normalmente definidas pelo anunciante, que determinam para quais usuários o conteúdo publicitário em questão será mostrado. Pode incluir dados demográficos, localização, comportamento, interesses, conexões dos usuários, entre outras informações.

Partes interessadas (“stakeholders”) – Pessoas que têm interesse em jogo (“stake”) porque são afetadas de algum modo pelas ações ou decisões da empresa. Observe que partes interessadas não são os “detentores de direitos” e que há diferentes tipos de pessoas interessadas: as que são

diretamente afetadas e aquelas cujo papel é defender os direitos das primeiras ("intermediary stakeholders" ou representantes). Detentores de direitos são indivíduos cujos direitos humanos podem ser diretamente impactados. Eles interagem com a empresa e seus produtos e serviços diariamente, normalmente como empregados, clientes ou usuários. "Intermediary stakeholders" incluem indivíduos e organizações informadas sobre os detentores de direitos e capazes de falar em seu nome, como organizações da sociedade civil, grupos de ativistas, acadêmicos, formadores de opinião, e formuladores de políticas públicas" (p. 10 de 28). Fonte: "Stakeholder Engagement in Human Rights Due Diligence: Challenges and Solutions for ICT Companies by BSR", (em tradução livre, "Engajamento com as partes interessadas em devida diligência de direitos humanos: Desafios e soluções para empresas TIC, por BSR"), BSR, setembro de 2014, http://www.bsr.org/reports/BSR_Rights_Holder_Engagement.pdf.

Patch – Um software cujo objetivo é atualizar um programa de computador ou seus dados de apoio para corrigi-lo ou melhorá-lo. Inclui correção de vulnerabilidades de segurança e outros bugs, cujos patches são geralmente chamados de bugfixes ou bug fixes, e melhoria da usabilidade ou performance do programa de computador, aplicativo ou sistema operacional.

Plataforma – Uma plataforma computacional é, de maneira geral, algo elaborado para a execução interna de um software de computador ou código, obedecendo suas limitações e fazendo uso de suas estruturas. O termo plataforma computacional pode se referir a diferentes níveis de abstração, incluindo a arquitetura de determinado hardware, um sistema operacional, e bibliotecas de tempo de execução.[1] Em resumo, pode ser descrita como o palco onde programas de computador atuam.

Plataformas digitais – Para efeitos da metodologia do Índice da RDR, plataformas digitais referem-se a uma categoria que inclui empresas de ecossistemas de internet e de dispositivos móveis, como também empresas que operam serviços de e-commerce e ecossistemas de assistentes pessoais digitais.

Política de bots – Um documento que descreve as regras da empresa sobre o uso de bots para geração e distribuição de conteúdo, ou para executar outras ações. Pode ser parte dos termos de serviço ou outro documento da empresa.

Política de privacidade – Documentos que descrevem as práticas da empresa com relação à coleta e uso de informações, principalmente informações sobre usuários.

Política de publicidade direcionada – Documentos que descrevem as regras da empresa sobre quais parâmetros de direcionamento de anúncios são permitidos na plataforma.

Políticas de conteúdo publicitário – Documentos que descrevem as regras da empresa sobre o tipo de conteúdo publicitário permitido na plataforma.

Políticas de desenvolvimento de sistemas de algoritmos – Documentos que descrevem as

regras da empresa para o desenvolvimento e testagem de algoritmos, aprendizado de máquina e tomada de decisão automatizada.

Políticas de uso de sistemas de algoritmos – Documentos que descrevem as práticas da empresa envolvendo o uso de algoritmos, aprendizado de máquina e tomada de decisão automatizada.

Priorização – Ocorre quando um operador de rede "administra sua rede de forma a beneficiar um conteúdo, aplicativos, serviços ou dispositivos" (p. 7 de 400). Para efeitos do Índice da RDR, esta definição inclui a decisão de uma empresa de bloquear acesso a determinado aplicativo, serviço ou dispositivo. Fonte: U.S Federal Communications Commission's 2015 Open Internet Rules (em tradução livre, "Regras da internet aberta de 2015 da Comissão Federal de Comunicações dos Estados Unidos") https://apps.fcc.gov/edocs_public/attachmatch/FCC-15-24A1.pdf.

Processos não oficiais – Processos ou canais através dos quais o governo faz solicitações de restrição de conteúdo ou contas, em vez de processos oficiais, como lei ou regulamento. Por exemplo, um agente oficial local pode fazer uma requisição ou protesto sobre certo conteúdo através de um canal não oficial.

Processos privados – Solicitações feitas através de processo privado, e não através de um processo judicial ou governamental. Solicitações privadas para restringir conteúdo ou contas podem vir de um órgão autorregulatório, como a Internet Watch Foundation, ou um sistema de notificação e retirada, como o U.S. Digital Millennium Copyright Act (em tradução livre, "Legislação dos direitos autorais do milênio digital", dos Estados Unidos). Para mais informações sobre notificação e retirada, assim como sobre o DMCA especificamente, ver pp 40-52 de 211 do "Fostering Freedom Online: The Role of Internet Intermediaries," (em tradução livre, "Promovendo a liberdade online: O papel dos intermediários de internet"), UNESCO, http://unesdoc.unesco.org/images/0023/002311/231162e.pdf.

Solicitações privadas são frequentemente informais e não partem de nenhum processo judicial. De acordo com a Fundação Wikimedia – que publica relatórios de transparência com dados sobre os tipos de solicitações que recebe --, solicitações privadas de informações do usuário incluem casos em que outra empresa envia uma carta ou um e-mail pedindo "informações não públicas" de algum usuário. Esse pedido pode incluir o endereço de IP ou o e-mail do usuário.

Programa de whistleblower – Um programa através do qual funcionários podem denunciar infrações que venham a testemunhar dentro de uma empresa, incluindo aquelas relacionadas a direitos humanos. Normalmente essas denúncias são feitas por meio de um hotline anônimo e em geral está sob a responsabilidade do chefe de compliance ou do chefe de ética.

Programa de zero-rating – "Zero-rating" refere-se à prática de não cobrar dos usuários os

dados usados para acessar certos serviços ou plataformas online. Zero-rating é visto como um tipo de priorização de tráfego que prejudica o princípio da neutralidade de rede.

Protocolo – Um conjunto de regras que regem a troca ou transmissão de dados entre dispositivos.

Publicidade direcionada – Publicidade direcionada, também conhecida como "publicidade segmentada em interesses", "publicidade personalizada" ou "publicidade programática", refere-se à prática de entregar anúncios sob medida para usuários com base em seu histórico de navegação, informações de localização, perfis de redes sociais e atividades, como também características demográficas e outros atributos. Publicidade direcionada depende de práticas de coleta de dados, que podem envolver o rastreio de atividades dos usuários na internet por meio de cookies, widgets e outras ferramentas de rastreio, para assim criar perfis segmentados de usuários.

Reclamação – RDR usa a definição de reclamação (grievance) dos Princípios Orientadores das Nações Unidas sobre Empresas e Direitos Humanos: "Percepção de uma injustiça que afete os direitos de uma pessoa ou grupo de pessoas com base em uma lei, contrato, promessas explícitas ou implícitas, práticas tradicionais ou noções gerais de justiça de uma comunidade afetada" (p. 32 de 42). Fonte: "Guiding Principles on Business and Human Rights: Implementing the United Nations 'Protect, Respect and Remedy Framework," (em tradução livre, "Princípios Orientadores sobre Empresas e Direitos Humanos: Colocando em prática o marco das Nações Unidas de "proteger, respeitar, retificar"), 2011, http://www.ohchr.org/Documents/Publications/GuidingPrinciplesBusinessHR_EN.pdf.

Recurso – Para os propósitos da RDR, esta definição de recurso inclui processos através dos quais usuários solicitam uma modificação formal em uma decisão de moderação de conteúdo ou restrição de conta feita pela empresa.

Rede de publicidade – Uma empresa ou serviço que conecta anunciantes a websites que querem hospedar anúncios. A principal função de uma rede de publicidade é agregar espaços de oferta de anúncios e conectá-los à demanda de anunciantes.

Registro de alterações – Um registro que mostra as mudanças sofridas por um documento, neste caso, os termos de serviço ou a política de privacidade.

Reparação – "A reparação pode incluir pedido de desculpas, restituição, reabilitação, compensações econômicas ou não-econômicas e sanções punitivas (por exemplo multas, sejam penais ou administrativas), assim como medidas de prevenção de novos danos como, por exemplo, liminares ou garantias de não-repetição. Os procedimentos de reparação devem ser imparciais e estar protegidos contra toda forma de corrupção ou tentativa política ou de outra natureza para influir em seu resultado." (p. 19 de 24). Fonte: "Empresas e Direitos Humanos: Parâmetros da ONU para proteger, respeitar e reparar", versão em português de

2012), https://site-antigo.socioambiental.org/sites/blog.socioambiental.org/files/nsa/arquivos/conectas_principiosorientadoresruggie_mar20121.pdf
Fonte original: "Report of the Special Representative of the Secretary-General on the issue of human rights and transnational corporations and other business enterprises", John Ruggie. Guiding Principles on Business and Human Rights: Implementing the United Nations 'Protect, Respect and Remedy' Framework", 2011.

Requerer – O requerimento ou solicitação pode acontecer quando um usuário cria uma conta ou mais tarde, sob requisição da empresa.

Restrição de conta / restrição de conta de usuário – Limitação, suspensão, desativação, exclusão ou remoção de uma conta de usuário específica, ou de suas permissões.

Restrição de conteúdo – Medida tomada por uma empresa que torna um conteúdo gerado pelo usuário invisível ou menos visível na plataforma ou serviço. A medida pode consistir em remoção integral do conteúdo ou tomar uma forma menos absoluta, como escondê-lo de certos usuários (ex.: residentes de um certo país ou pessoas de uma certa faixa-etária), limitar a habilidade dos usuários de interagir com esse conteúdo (ex.: tornando impossível de "curti-lo"), adicionar conteúdo alternativo (ex.: informações corretivas em posts antivacina) ou reduzir sua amplificação pelos sistemas de curadoria da plataforma.

Retenção de informações do usuário – Uma empresa pode coletar dados e depois exclui-los. Se a empresa não os excluir, os dados são "retidos." O tempo entre coleta e exclusão é o "período de retenção." Esses dados podem entrar na nossa definição de "informações do usuário" ou podem ser anônimos. Ressalta-se que dados verdadeiramente anônimos de modo algum podem ser ligados a um usuário, sua identidade, comportamento ou preferência, o que é muito raro.

Um tópico relacionado é o "período de retenção". Por exemplo, uma empresa pode coletar dados de registro de maneira contínua, mas excluir todos os dados uma vez por semana. Nesse caso, o período de retenção é de uma semana. No entanto, se o período de retenção não for especificado, o padrão é pressupor que os dados nunca são excluídos e que o período de retenção é, portanto, indeterminado. Em muitos casos, usuários podem querer que seus dados sejam retidos enquanto estiverem ativamente usando o serviço, mas que fossem excluídos (e, portanto, não retidos) se e quando pararem de usar o serviço. Por exemplo, usuários podem querer que um serviço de rede social mantenha todas as suas mensagens privadas, mas, quando o usuário deixar a rede social, pode querer que suas mensagens privadas sejam excluídas.

Riscos à cibersegurança – Situações em que a segurança, privacidade ou outros direitos correlatos do usuário por estar ameaçados por um ator malicioso (incluindo, mas não limitado a criminosos, detentores de informações privilegiadas ou estados-nações), que pode obter

acesso não autorizado a dados do usuário através de hacking, phishing ou outras técnicas enganosas.

Roll out – Uma série de anúncios de produtos relacionados que são lançados ao longo do tempo; o processo de disponibilizar patches, atualizações de software e upgrades de software para usuários.

Sinalização (flag) – O processo de detectar e alertar a empresa sobre um conteúdo ou conta pode estar violando as regras da empresa ou a sinalização que comunica essa informação à empresa. Este processo pode ocorrer dentro da plataforma ou de modo externo. Sinalizadores incluem usuários, sistemas de algoritmos, equipe da empresa, governos ou outras entidades privadas.

Sinalização (flag) / detecção enviada por pessoas – Uma sinalização (flag) detectada e enviada por um ser humano, seja um usuário, funcionário ou prestador de serviço de uma empresa, funcionário ou representante do governo, ou um funcionário ou representante de uma empresa. *Ver também: Sinalização automática.*

Sinalização automática (automated flag) – Uma detecção sinalizada via sistema de algoritmos. *Ver também: Sinalização (flag) / detecção enviada por pessoas.*

Sinalizador – Indivíduo ou entidade que alerta a empresa sobre um conteúdo ou conta que pode estar violando as regras da empresa. Este processo pode ocorrer dentro da plataforma ou de modo externo. Sinalizadores incluem usuários, sistemas de algoritmos, equipe da empresa, governos ou outras entidades privadas.

Sistema de algoritmos – Um sistema que usa algoritmos, aprendizado de máquina e/ou tecnologias relacionadas para automatizar, otimizar e/ou personalizar processos de tomada de decisão.

Sistema operacional (SO) – O software que sustenta as funções básicas de um computador, como programar tarefas, executar aplicativos e controlar periféricos. Um sistema operacional móvel é o SO de um dispositivo móvel, como um smartphone ou um tablet.

Sistemas de algoritmos de curadoria, recomendação ou classificação – Um sistema que usa algoritmos, aprendizado de máquina (machine learning) e outras tecnologias de automação de tomada de decisão para administrar, moldar e dirigir o fluxo de conteúdo e informação em uma plataforma, geralmente de forma personalizada para cada usuário.

Solicitações governamentais – Inclui solicitações de ministérios ou agências governamentais, assim como requerimentos da polícia e ordens judiciais em casos criminais e civis.

Solicitações governamentais não judiciais – Solicitações que vêm de entidades governamentais que não são órgãos judiciais, juízes ou tribunais. Podem incluir solicitações de ministérios, agências, departamentos de polícia, agentes policiais (agindo em suas atribuições oficiais) ou de outros gabinetes, autoridades e entidades governamentais não judiciais.

Supervisão / Supervisionar – Os documentos de governança ou processos de tomada de decisão da empresa atribuem a um comitê, programa, equipe ou funcionário encarregado a autoridade formal de supervisão sobre uma função específica. Esse grupo ou pessoa é responsável pela função e é avaliada na medida em que cumpre essa responsabilidade.

Supervisão no nível executivo – O comitê executivo ou um membro da equipe executiva da empresa supervisiona diretamente questões relacionadas à liberdade de expressão e privacidade.

Tecnologias de publicidade – Sistemas de tomada de decisão via algoritmos que determinam a quais usuários será mostrado um conteúdo publicitário específico. Tal determinação pode levar em conta os parâmetros de direcionamento escolhidos pelo anunciante ou pode ser totalmente automatizada.

Terceiros – Uma parte ou entidade que não é nem o usuário nem a empresa. Para efeitos desta metodologia, terceiros podem incluir organizações governamentais, tribunais ou outras partes privadas (ex.: uma empresa, uma ONG, um indivíduo).

Termos de serviço – Este documento também pode ser chamado de Termos de Uso, Termos e Condições etc. Os termos de serviço "em geral, fornecem as regras básicas sobre como diversos serviços online devem ser usados", como dito pela Electronic Frontier Foundation (EFF), e representam um acordo legal entre a empresa e o usuário. Empresas podem tomar medidas contra usuários e seu conteúdo baseadas nas informações dos seus termos de serviço. Fonte: "Terms of (Ab)uso" (em tradução livre, "Termos de (ab)uso"), Electronic Frontier Foundation, https://www.eff.org/issues/terms-of-abuse.

Tomada de decisão automatizada – Tecnologia que toma decisões sem revisão ou contribuição humana significativa, como através do uso de inteligência artificial ou algoritmos.

Upgrade de software – Um upgrade de software é uma nova versão de um software que oferece mudanças ou aprimoramentos significativos em relação à versão atual.

Usuário afetado – Usuário que teve conteúdo restringido por uma ação de moderação de conteúdo ou o usuário associado a uma conta de usuário restringida por moderação de conteúdo, ou, se aplicável, o(s) usuário(s) que enviaram a denúncia que levou à avaliação de um conteúdo ou conta pela moderação.

Usuários – Indivíduos que usam um produto ou serviço. Incluem pessoas que publicam ou

transmitem conteúdo online, como também aqueles que tentam acessar ou receber o conteúdo. Nos indicadores da categoria de liberdade de expressão, inclui desenvolvedores terceiros que criam aplicativos hospedados ou distribuídos através do serviço ou produto de uma empresa.

Vazamento de dados – Um vazamento de dados ocorre quando alguém não autorizado obtém acesso a informações do usuário coletadas, retidas ou de alguma forma processadas pela empresa, o que compromete a integridade, segurança e confidencialidade daquela informação.

Vulnerabilidade de segurança – Uma fraqueza que permite que um invasor reduza a segurança da informação de um sistema. Uma vulnerabilidade é a interseção de três elementos: uma susceptibilidade ou falha do sistema, o acesso de um invasor à falha e a capacidade do invasor de explorar a falha.

Widget – Um código que permite que o usuário ou a empresa incorpore aplicativos e conteúdo de um site ou serviço a um site ou serviço de terceiros. Em alguns casos, empresas usam widgets em um site terceiro e coletam informações sobre os visitantes daquele site sem que tenham conhecimento.

Ranking Digital Rights

Esta tradução da Metodologia RDR 2020 foi concluída em setembro de 2022.