

Relatório Assédio Cibernético

As 25 recomendações da RSF

Aos Estados

- **Reforçar o arcabouço legal para restringir o assédio a jornalistas online e aplicá-lo com rigor.** Os Estados devem investigar sistematicamente os casos de assédio online, processar e condenar seus autores e, para tal, alocar os recursos humanos e financeiros necessários para a justiça e a polícia.
- **Reforçar a responsabilidade das plataformas online com relação aos conteúdos que são partilhados em seus serviços,** sem, contudo, dar-lhes poder de controle dos conteúdos ou de censura. O regime de responsabilidade das plataformas deve ser adaptado de acordo com o impacto que sua atividade exerce sobre a qualidade do debate público. Os Estados devem, igualmente, reforçar as obrigações que são impostas às plataformas, sobretudo, com relação à transparência dos algoritmos curadores e de conformidade da política de moderação das plataformas com os princípios da liberdade de expressão e de informação.
- **Instaurar mecanismos de alerta e de intervenção rápida** em casos de assédio e garantir sua boa articulação com os serviços judiciais.
- **Garantir que as regras da luta contra os conteúdos de ódio sejam aplicadas de maneira proporcional e com discernimento,** para que não acarretem nenhuma restrição abusiva à liberdade de expressão e de informação online. Mais especificamente, os Estados devem instaurar procedimentos que permitam proteger-se contra os desvios dessas regras e dos mecanismos de sinalização com o objetivo de censurar ou reprimir jornalistas.
- **Instaurar mecanismos de reparação** das violências sofridas pelas vítimas de assédio cibernético (indenização financeira, auxílio médico e psicológico, realocização, etc.).
- **Abster-se de recorrer a agentes de influência e de desestabilização online** com o objetivo de manipular a opinião pública e de assediar jornalistas ("trolls").

- **ÂMBITO INTERNACIONAL**

- Junto às Nações Unidas, os Estados devem pleitear a criação de um mecanismo de controle do respeito pelos Estados de suas obrigações, na forma de um **Representante Especial do Secretário Geral para a Segurança dos Jornalistas**
- **Na Europa, os Estados devem assinar e ratificar o protocolo adicional à Convenção da Cibercriminalidade do Conselho da Europa.** Os Estados membros da União Africana também devem ratificar a Convenção sobre a Segurança Cibernética e a Proteção dos Dados de Caráter Pessoal. Os Estados membros das outras organizações regionais (Organização dos Estados Americanos, ASEAN, União Africana) devem trabalhar na elaboração de convenções semelhantes.
- **Os Estados devem encorajar a pesquisa** multidisciplinar e internacional sobre as técnicas de censura - em constante mutação - os modos de operação e as respostas a dar ao assédio cibernético em geral e ao que afeta os jornalistas em particular.

- **EDUCAÇÃO**

Os Estados devem reforçar a educação digital, para sensibilizar os usuários da Internet quanto ao impacto do assédio online e às consequências criminais que recaem sobre quem o pratica.

- **Todas as políticas públicas relativas à questão da violência online deverão levar em consideração a dimensão de gênero das violências online** que visam, com mais frequência, as mulheres jornalistas.

Às organizações internacionais

- **Continuar a pleitear junto aos Estados para que o princípio segundo o qual "os direitos dos quais os indivíduos gozam offline devem igualmente ser protegidos online, sobretudo o direito de cada indivíduo à liberdade de expressão"**¹.
- **Contribuir com a pesquisa sobre os mecanismos de assédio online.** Devem participar do financiamento da pesquisa e emitir recomendações aos Estados em matéria de luta contra o assédio cibernético.
- **Os mecanismos internacionais e regionais de proteção dos direitos humanos devem integrar a questão do assédio online ao seu monitoramento dos abusos cometidos contra jornalistas.**

¹ resolução A/HRC/RES/20/8 sobre a promoção, a proteção e o exercício dos direitos humanos na Internet - 16 de julho de 2012

Às plataformas

- **Ser transparentes com relação a suas regras de moderação dos conteúdos online.** Devem reforçar a publicidade e a transparência de suas ações de luta contra o assédio online, instaurando mecanismos de sinalização de conteúdos de ódio.
- **Estar atentas para que as regras não sejam desviadas de suas finalidades para calar os jornalistas.** Todas as sinalizações de conteúdos ilícitos devem fazer objeto de um exame minucioso e as plataformas devem saber discernir entre as sinalizações abusivas, realizadas com o único objetivo de restringir um discurso que incomoda, e as sinalizações que tratam de conteúdos de fato abusivos.
- **Facilitar para as vítimas a sinalização de violências, instaurando um ponto de alerta de urgência para os jornalistas que sofram ameaças e ataques online.**
- **Colaborar ativamente com a justiça** nas investigações sobre a violência cibernética contra os jornalistas (identificação dos autores de violências online, etc.)
- **Lutar contra as campanhas elaboradas de assédio online, especialmente levando em conta as "fábricas de trolls"**, aumentando, sobretudo, o número de moderadores humanos.
- **Desenvolver campanhas de comunicação e de sensibilização ao tema da violência online**, visando especificamente jornalistas, sobretudo as mulheres.

Aos meios de comunicação

- **Adaptar-se à ameaça e antecipá-la melhor.** Os meios de comunicação devem sensibilizar seus diretores, assim como os funcionários e jornalistas, instaurando dispositivos de urgência internos (linha direta de assédio cibernético) para garantir o suporte e a proteção do jornalista assediado.
- **Encorajar a criação de redes de troca de boas práticas desenvolvendo uma abordagem holística** (responsáveis editoriais, gestores comunitários, responsáveis pela segurança digital, pessoal jurídico, jornalistas), de maneira interna, mas também com outras redações, de outros países, até mesmo de outros setores.
- **Apropriar-se do tema do assédio online de jornalistas**, multiplicar as reportagens e investigações, com o objetivo de informar e sensibilizar o público em geral, a profissão e as autoridades sobre esses desafios ainda pouco conhecidos.

Aos anunciantes

- **Recusar-se a veicular publicidades em sites** que contribuam com a disseminação de conteúdos de ódio, ou que não lutem o suficiente contra a cibercriminalidade.

- **Desenvolver manuais de ética** e de boas práticas com relação à publicidade online, em conexão com a sociedade civil, para garantir que esta não contribua com o financiamento do assédio online.

Anexo 1.

Formando jornalistas

“Você não pode mudar o canhão, mas sempre poderá se esconder por trás de paredes mais altas e mais grossas.” (Wired)

Jornalistas: como enfrentar os exércitos de trolls?

Diante da violência cibernética, a RSF recomenda a todos os meios de comunicação e aos jornalistas reforçar os elementos básicos de formação em segurança digital.

Antes (prevenção):

- Compreender que os jornalistas são especialmente expostos aos ataques online baseados no desvio de informações pessoais, e que a violência desses ataques pode ser um fator de desestabilização e ter graves repercussões, incluindo para os jornalistas mais experientes.
- Levantar em consideração a especificidade desses ataques, que visam, principalmente, as mulheres ².
- Os jornalistas devem adotar regras indispensáveis de segurança digital³ :
 - ★ Remover qualquer informação pessoal online (gerenciar os critérios de confidencialidade nas redes sociais, por exemplo, passando sua conta de Instagram para modo privado, etc.)
 - ★ Se não fizer isso, avaliar sempre os riscos e, sobretudo, o equilíbrio entre o risco envolvido para você (desvio de fotos de seus filhos, etc.) e as vantagens (prazer de compartilhar suas fotos pessoais)
 - ★ Cuidado com as geolocalizações automáticas, que o localizam imediatamente.
 - ★ Proteger os seus nomes de domínio no Whois.
 - ★ Associar alertas do Google ao seu nome.
 - ★ Usar programas como Securedrop, privacy badger⁴.
 - ★ Não deixar o seu número de telefone pessoal disponível online (ou em uma resposta automática de ausência, por exemplo).
 - ★ Usar a identificação dupla para os seus e-mails, desconectar a cada sessão.

² <https://gijn.org/2017/09/28/scourge-of-the-profession-online-harassment-of-female-journalists/>

³ Procure periodicamente pelo seu nome online e remova informações de identificação pessoal de agregadores de dados como Spokeo, Pipl, Intelius, e <https://www.propublica.org/article/cheap-tricks-the-low-cost-of-internet-harassment>. Ou pague por um serviço que faça isso por você. Além disso, instale serviços, como EFF's Privacy Badger, Ghostery ou Abine, que podem ajudar a evitar uma parte do rastreamento e coleta de dados online.#

⁴ <https://www.eff.org/privacybadger>

- ★ Escolher uma frase como senha (frase-senha), em vez de uma palavra.
- ★ Cuidado com os ataques do tipo *phishing*, nunca clicar em um link suspeito.
- ★ Designar vários administradores para as páginas que criar, e não todos oficialmente ligados ao seu veículo de comunicação.
- ★ De maneira geral, estabelecer regras de segurança digital como detalhado no Safety Guide for Journalists da RSF⁵. Consultar também os outros recursos online: [A TrollBusters propõe, hoje, um teste para saber se somos vítimas de assédio](#)⁶. A ONG PEN America publicou, em abril de 2018, um manual de luta contra o assédio online, quer sejamos escritores, jornalistas ou empregadores de jornalistas⁷. O coletivo Tactical Technology também publicou um site de recursos para mulheres vítimas de assédio cibernético⁸.

Durante o ataque:

- Sinalize e bloqueie os conteúdos abusivos nas plataformas em questão, reiterar a ação.
- Informe seus colegas e superiores.
- Guarde provas, formando um dossiê com todos os rastros do assédio. Pedir a alguém próximo que faça este trabalho caso você não suporte ler os insultos e ameaças contra você.
- Aposte na solidariedade jornalística. Alguns jornalistas vítimas de assédio online respondem com uma contraofensiva, reunindo apoio por meio de uma *hashtag*, como faz o site TrollBusters, que defende as mulheres jornalistas vítimas de violência cibernética⁹.
- Não alimente os trolls. Os ataques são, geralmente, extremamente violentos, mas de duração limitada. Desconecte-se por algumas horas, se necessário.
- Faça capturas de tela.

Após o ataque:

- Sua conta foi hackeada: avise suas fontes, ou a RSF, para protegê-las, pois elas podem ser visadas. assédio = comunicação (lembrar ferramentas preexistentes)
- Utilize os mecanismos de comunicação de casos de assédio disponibilizados pelas plataformas e pelas autoridades (como o PHAROS, na França)
- Se possível, você pode prestar um testemunho para fornecer uma prova

⁵ https://rsf.org/sites/default/files/guide_journaliste_rsf_2015_en_0.pdf

⁶ https://yoursosteam.files.wordpress.com/2017/01/tb_infographic_watermark.jpg

⁷ A ONG PEN lançou, em abril de 2018, um manual de luta contra o assédio online que detalha as boas práticas para os .

<https://onlineharassmentfieldmanual.pen.org/>

⁸ <https://xyz.informationactivism.org/en/online-harassment-of-politically-active-women-overview>

⁹ <https://www.troll-busters.com/>

incontestável.

- Você pode prestar queixa na delegacia (e insistir para que seja de fato uma queixa, não um registro de ocorrência) ¹⁰

¹⁰ https://www.buzzfeed.com/mariekirschen/que-faire-quand-vous-etes-victime-ou-temoin-de-cyberharcelem?utm_term=.nePjP8Ddyk#.nx2Kgm03AY