CADERNOS CGI.br Referências

6.2

Internet & Jurisdição: Abordagens operacionais em dados, conteúdo e domínios

Rede de Políticas Internet & Jurisdição

INTERNET & JURISDICTION POLICY NETWORK

cgi.br
Comitê Gestor da Internet no Brasil

Edição em português publicada com autorização da Rede de Políticas Internet & Jurisdição. O conteúdo deste relatório é de responsabilidade da Rede de Políticas Internet & Jurisdição.

Para mais informações, consultar: <https://www.internetjurisdiction.net/>

Núcleo de Informação
e Coordenação do Ponto BR

6.2
CADERNOS CGI.br **Referências**

Internet & Jurisdição: Abordagens operacionais em dados, conteúdo e domínios

Rede de Políticas Internet & Jurisdição

Comitê Gestor da Internet no Brasil
Dezembro 2021

Núcleo de Informação e Coordenação do Ponto BR

Diretor Presidente
Demi Getschko

Diretor de Assessoria às Atividades do CGI.br
Hartmut Richard Glaser

Diretor Administrativo
Ricardo Narchi

Diretor de Serviços e Tecnologia
Frederico Neves

Diretor de Projetos Especiais e de Desenvolvimento
Milton Kaoru Kashiwakura

Produção dos Cadernos CGI.br
Diretoria de Assessoria às Atividades do CGI.br

Coordenação Executiva e Editorial
Carlos Francisco Cecconi e Jean Carlos Ferreira dos Santos

Produção Editorial
Caroline D'Avo (Comunicação NIC.br) e Carolina Carvalho (Comunicação NIC.br)

Produção desta publicação

Tradução
Ana Zuleika Pinheiro Machado

Projeto Gráfico e Ilustrações
Pilar Velloso

Revisão da Tradução
Luiza Brandão
Paula Côrte Real

Revisão Técnica e Preparação
Carlos Francisco Cecconi, Everton Teles Rodrigues, Jean Carlos Ferreira dos Santos e Vinicius Wagner Oliveira Santos

Diagramação
Daniele Doneda

Fotos
Shuterstock e IStockphoto

Título original
Data & Jurisdiction Program Operational Approaches / Content & Jurisdiction Program Operational Approache / Domains & Jurisdiction Program Operational Approaches / Berlin Roadmap Secretariat Summary and I&J Programs Work Plans. Disponível em: <https://www.internetjurisdiction.net/publications/>

Dados Internacionais de Catalogação na Publicação (CIP)
(Câmara Brasileira do Livro, SP, Brasil)

Internet & jurisdição (livro eletrônico): abordagens operacionais em dados, conteúdo e domínios / Rede de Políticas Internet & Jurisdição; (editor) Núcleo de Informação e Coordenação do Ponto BR; tradução Ana Zuleika Pinheiro Machado. --1. ed. -- São Paulo, SP: Comitê Gestor da Internet no Brasil, 2021.
PDF
Título original: Data & Jurisdiction Program Operational Approaches; Domains & Jurisdiction Program Operaciol Approaches; Berlin Roadmap Secretariat Summary and I & J Programs Work Plans.
Vários colaboradores.
ISBN 978-65-86949-47-6
1.Ciberespaço 2.Direito e Tecnologia 3.Governança da Internet 4.Internet - Leis e Legislação 5.Transnacionalização 6.Regulação I.Rede de Políticas Internet & Jurisdição. II.Núcleo de Informação e Coordenação do Ponto BR.

21-86755 CDD-004.6

Índices para catálogo sistemático:
1. Governança digital : Tecnologia da informação : Relatórios 004.6
Eliete Marques da Silva - Bibliotecária - CRB -8/9380

Esta publicação está disponível também em formato digital em <http://www.cgi.br>

Comitê Gestor da Internet no Brasil (CGI.br)

Composição em Dezembro de 2021

Integrantes

Representantes do Setor Governamental
Evaldo Ferreira Vilela
Jackeline de Souza Conca
Jeferson Denis Cruz de Medeiros
José Gustavo Sampaio Gontijo
Leonardo Euler de Morais
Luis Felipe Salin Monteiro
Maximiliano Salvadori Martinhão
Orlando Oliveira dos Santos
Patrícia Ellen da Silva

Representantes do Setor Empresarial
Henrique Faulhaber
José Alexandre Novaes Bicalho
Nivaldo Cleto
Rosauro Leandro Baretta

Representantes do Terceiro Setor
Bia Barbosa
Domingos Sávio Mota
Laura Conde Tresca
Percival Henriques de Souza Neto

Representantes da Comunidade Científica e Tecnológica
Marcos Dantas Loureiro
Rafael de Almeida Evangelista
Tanara Lauschner

Representante de notório saber em assuntos de Internet
Demi Getschko

Coordenador
José Gustavo Sampaio Gontijo

Secretário Executivo
Hartmut Richard Glaser

Nota dos Editores

Este livro é uma compilação de quatro documentos produzidos separadamente pela Rede de Políticas Internet & Jurisdição. São três documentos gerados, respectivamente, pelos grupos de contato dos programas temáticos Dados e Jurisdição, Conteúdo e Jurisdição e Domínios e Jurisdição; além de um anexo, intitulado "Roteiro de Berlim". A compilação é o resultado do trabalho permanente dos grupos de contato da Rede I&J para a produção de soluções concretas aos principais desafios de Internet & Jurisdição nas três áreas mencionadas, indicando normas, critérios e mecanismos operacionais que visam a facilitar e habilitar a cooperação entre atores para a resolução de problemas. Este trabalho foi especialmente consolidado por ocasião da 3ª Conferência Global da Rede I&J, realizada em Berlim, na Alemanha, em 2019, para a qual serviu de material-base para as discussões. O Roteiro de Berlim, por sua vez, apresenta os planos de trabalho detalhados para os três programas temáticos da Rede, que foram implementados na sequência da 3ª Conferência Global.

É preciso destacar que a Rede I&J implementa um padrão de cores específico, com o objetivo de identificar seus programas temáticos. Por essa razão, apesar de os Cadernos CGI.br tradicionalmente trazerem um design próprio, optou-se por manter o esquema de cores original utilizado pela Rede de Políticas I&J, de modo a garantir o máximo de coesão de sentido e fidelidade ao conteúdo original.

Agradecemos ao Secretariado da Rede de Políticas Internet & Jurisdição que, gentilmente, autorizou a tradução destes e de outros documentos para o português e vem prestando valiosas contribuições para que o resultado final seja uma publicação de qualidade.

Apresentação à Edição Brasileira

por DIEGO R. CANABARRO

Mestre em Relações Internacionais e Doutor em Ciência Política pela UFRGS. Trabalhou entre 2014 e 2019 na equipe de Assessoria do CGI.br.

Uma das questões mais desafiadoras da governança global da Internet contemporânea diz respeito a como lidar com conflitos jurisdicionais que decorrem da natureza transnacional de fluxos, interações e transações digitais de todos os tipos, em um mundo segmentado em Estados soberanos, delimitado por fronteiras físicas. O desafio imposto atualmente não decorre apenas do caráter transfronteiriço de fatos e atos jurídicos mediados pelas tecnologias da informação e da comunicação (sobretudo a Internet) que são relevantes para as relações internacionais. Afinal, ainda que com limitações, a transnacionalidade tem sido objeto de atenção do Direito Internacional Público e do Direito Internacional Privado há séculos (e, nas últimas décadas, tem ganhado relevância na agenda de ambos os campos. O desafio atual decorre, também (e principalmente), da escala, da multidimensionalidade e da complexidade do "quebra-cabeças"[1] inerente à interface de Internet e Jurisdição.

Esse "quebra-cabeças" (expressão do professor Dan Svantesson) é desafiador por três razões principais: primeiro, porque a Internet representa um mosaico de setenta mil redes interconectadas, espalhadas de maneira não uniforme pelo espaço geográfico do planeta, que sustenta um ecossistema digital que está em permanente transformação. Segundo, porque essa

1 Svantesson, Dan Jerker B. Solving the Internet jurisdiction puzzle. Oxford University Press, 2017.

transformação é pautada por variáveis técnicas, culturais, socioeconômicas e políticas que se influenciam e se retroalimentam de maneira multidirecional. E, terceiro, porque os usuários (individuais e corporativos, públicos e privados) da Internet não são meramente usuários passivos da tecnologia; eles são sujeitos ativos da evolução e do desenvolvimento do ecossistema digital criado a partir dela.

Não é simples tratar dessa complexidade. E pode-se dizer que se avançou muito pouco nesse sentido quase duas décadas depois de o caso "UEJF & Licra versus Yahoo! Inc & Yahoo France"[2] ter escancarado o potencial de conflito de sistemas de valores socioculturais e ordens jurídicas que pode surgir a partir de uma simples página na Web. Há um ajuste fino e um equilíbrio frágil entre aspectos técnicos e não técnicos relacionados ao ecossistema digital, suas interpenetrações e suas constantes reconfigurações, que devem ser levados todos em consideração no tratamento do tema. Tais requisitos quase sempre extrapolam a capacidade posta e as metodologias de trabalho utilizadas em arenas tradicionais da política internacional onde se trata da coordenação da ação coletiva (das relações de cooperação e conflito) no nível global. Resolver o enigma envolto na pluralidade de peças e partes, de modo a chegar sempre na reprodução perfeita de uma imagem anteriormente desconstruída talvez não funcione muito bem para ambientes dinâmicos como aquele que circunda a Internet. Svantesson usa a metáfora do "quebra-cabeças" justamente para alertar dos riscos de se tentar conformar a Internet e tudo aquilo que lhe diga respeito a noções preconcebidas e a soluções já testadas anteriormente para dar conta de questões jurisdicionais.

Em superação a essas limitações, o trabalho da "Rede de Políticas Internet & Jurisdição" (sob a batuta dos maestros Bertrand de la Chapelle e Paul Fehlinger) representa um dos desenvolvimentos mais sólidos na institucionalidade da governança da Internet em direção ao tratamento de parte das questões jurisdicionais que hoje se impõem: (a) no tratamento

2 Okoniewski, Elissa A. "Yahoo!, Inc. v. LICRA: The French Challenge to Free Expression on the Internet." American University International Law Review 18, no. 1 (2002): 295-339. Duh, Christine. "Yahoo! Inc. v. LICRA." Berkeley Technology Law Journal, vol. 17, no. 1, 2002, pp. 359-378.

do acesso transfronteiriço a dados e informações para instruir a persecução penal; (b) na moderação (pública e privada) de conteúdos acessíveis por meio da Internet; e (c) no combate e tratamento de abusos online por meio de restrições e ações requeridas dos operadores do sistema de nomes de domínio da Internet (DNS). Esse esforço combina a adoção de metodologias ágeis, aplicadas a problemas bem delimitados, e é pautado pela participação em pé de igualdade de uma pluralidade de atores.

Em um processo conduzido entre 2016 e 2019 (um hiato de tempo relativamente rápido, considerando-se o fluxo regular das coisas na governança global), a "Rede I&J" conseguiu produzir um compêndio de parâmetros normativos, critérios e limiares de ação para o setor público e o setor privado, bem como mecanismos operacionais detalhados para guiar a ação prática, nas três áreas destacadas acima. De tudo o que se pode dizer a respeito (e do que já foi dito até aqui), deve-se sempre sublinhar que esse conjunto de diretrizes está plenamente alinhado com a noção de que a Internet deve seguir uma rede de alcance global, aberta, segura e estável, sem fragmentações.

É salutar que esse conjunto importantíssimo de materiais ganhe versão em português a partir de uma iniciativa do Comitê Gestor da Internet no Brasil (CGI.br) e por meio de um processo conduzido com esmero, rigor e dedicação da 'intrépida' Assessoria que corporifica em ação os desígnios do colegiado. É salutar, porque indica uma vez mais a disposição do CGI.br de contribuir com o avanço da governança da Internet no país em direção a soluções inovadoras (que passam não apenas pelas mãos do Estado) para o tratamento de questões regulatórias, legislativas e de políticas públicas pertinentes à Internet. Mas é, finalmente, salutar, pois dá ao público brasileiro a possibilidade de conhecer uma parte extremamente relevante do trabalho que o CGI.br desempenha no plano internacional e por vezes passa batido no cenário nacional.

*As opiniões expressas neste texto são de responsabilidade do autor e não refletem necessariamente a política ou posição oficial de nenhuma instituição mencionada anteriormente.

Preâmbulo

por BERTRAND DE LA CHAPELLE
Diretor Executivo
Secretariado da Rede de Políticas Internet & Jurisdição

Quando a Rede de Políticas Internet & Jurisdição foi fundada em 2012, a importância de abordar questões jurisdicionais online era pouco reconhecida pela maioria dos atores. A visão dominante era simplesmente que o esperado aumento em massa da penetração da Internet permitiria que pessoas em todo o mundo se conectassem e compartilhassem melhor suas ideias, contribuíssem para uma maior liberdade e criassem novas oportunidades econômicas. Em grande medida, muitos aspectos dessa visão se materializaram nos últimos sete anos e agora damos por garantidos os muitos benefícios que essa criação coletiva sem precedentes da humanidade nos trouxe. Apesar disso – ou talvez por causa disso – a atenção mudou significativamente nos últimos anos: dificilmente passa um dia sem que os grandes jornais estampem manchetes sobre abusos on-line e a dificuldade de enfrentá-los, dada a natureza transnacional da rede. Racionalmente, reconhecemos que tais abusos permanecem limitados em proporção à atividade online geral, mas o tremendo volume da última torna legitimamente a primeira uma preocupação crescente para todos os atores. Abordar os conteúdos nocivos, as atividades criminosas e outros desafios regulatórios de uma forma que respeite os direitos e seja economicamente sustentável passou a ser uma questão crucial para o século XXI digital.

Pode ter sido ingênuo pensar que o lado escuro da natureza humana não se expressaria também no espaço digital, mas cabe a todos nós agora evitar que o pêndulo oscile muito na outra direção. Temos de encontrar soluções coletivas que não só protejam o precioso acervo de uma rede global, mas também permitam que a nossa sociedade digital se desenvolva de forma equilibrada. Isto só pode ser conseguido através de uma cooperação semelhante à que permitiu o surgimento da própria Internet. Infelizmente, o atual sistema internacional de soberanias territoriais independentes frequentemente representa um obstáculo a essa cooperação.

Na ausência de acordos internacionais claros, após um longo período de inatividade, os últimos anos testemunharam uma série de propostas e regulamentos distintos para lidar com abusos online. Por muito bem intencionados que alguns deles possam ser, as decisões unilaterais adotadas de forma descoordenada sob a pressão da urgência podem ter consequências prejudiciais indesejadas. No entanto, a própria proliferação de iniciativas demonstra uma preocupação comum em abordar estas questões. Esta convergência na vontade de agir deve ser acompanhada de uma maior comunicação, coordenação e cooperação entre os intervenientes. É mais do que nunca crucial reiterar a nossa firme convicção na necessidade de abordar os problemas comuns de forma coletiva.

Dada a evolução das mentalidades, discursos e ações dos atores que testemunhamos nos últimos sete anos, em particular no contexto da Rede de Políticas Internet & Jurisdição, devemos estar otimistas quanto ao desenvolvimento de arcabouços comuns que beneficiem todas as partes interessadas. Trabalhando intensamente e com um espírito construtivo na busca incessante de soluções escalonáveis, interoperáveis e resilientes, podemos, em conjunto, abordar as questões mais prementes da sociedade digital. O seguinte documento *Abordagens Operacionais* representa um passo encorajador nesta direção, ilustrando concretamente o que pode ser produzido quando os atores se comprometem a trabalhar em conjunto na defesa do interesse público comum.

EM DIREÇÃO À INTEROPERABILIDADE JURÍDICA

A Internet cada vez mais corrobora as interações políticas, econômicas e sociais. No entanto, à medida que a penetração da Internet aumenta, crescem também os problemas jurídicos transfronteiriços. A natureza transnacional da rede desafia o fundamento territorial dos sistemas jurídicos nacionais. O número de usuários da Internet mais do que duplicou na última década, e mais de metade da população mundial está agora online. Como enfrentar em conjunto os desafios jurídicos prementes na intersecção da economia digital global, dos direitos humanos e da segurança tornou-se um dos maiores desafios do século XXI que definirá o futuro da Internet transfronteiriça e da sociedade digital.

Desde 2012, atores de todo o mundo trabalham juntos na Rede de Políticas Internet & Jurisdição para lidar com a tensão entre a natureza transfronteiriça da Internet e as jurisdições nacionais. O seu Secretariado possibilita a cooperação multissetorial e facilita um processo político global envolvendo mais de 200 entidades importantes de mais de 40 países e todos os grupos interessados: governos, as maiores empresas de Internet do mundo, operadores técnicos, grupos da sociedade civil, universidades e organizações internacionais.

As partes interessadas da Rede de Políticas Internet & Jurisdição trabalham juntas em três Programas temáticos (Dados e Jurisdição, Conteúdo e Jurisdição e Domínios e Jurisdição) para desenvolver conjuntamente padrões de políticas e soluções operacionais por meio de reuniões virtuais e físicas regulares, incluindo sessões regionais e Conferências Globais. O Secretariado também mantém o Banco de Dados Retrospectivos da I&J, rastreando tendências globais e, em 2019, lançará o primeiro Relatório de Status Global sobre Internet & Jurisdição do mundo.

As Conferências Globais regulares da Rede de Políticas Internet & Jurisdição são institucionalmente apoiadas por seis organizações internacionais: Conselho da Europa, Comissão Europeia, ICANN, OCDE, CEPAL das Nações Unidas e UNESCO. As Conferências Globais anteriores foram organizadas em parceria com a França (2016) e o Canadá (2018). O trabalho das partes interessadas da Rede de Políticas Internet & Jurisdição

foi apresentado e reconhecido pelos principais processos internacionais, incluindo o Fórum de Governança da Internet das Nações Unidas, G7, G20 e o Fórum da Paz de Paris, e divulgado por meios de comunicação como The Economist, New York Times, Washington Post, Financial Times, Politico ou Fortune. O trabalho da Rede de Políticas é apoiado financeiramente por uma coalizão única de mais de 20 governos, empresas e organizações.

De questões de conjuntura até áreas de cooperação

Após quatro anos de consultas e reuniões internacionais na Rede de Políticas Internet & Jurisdição, fundada em 2012, os atores se reuniram pela primeira vez em nível global em Paris, de 14 a 16 de novembro de 2016, para abordar o futuro da jurisdição transfronteiriça na Internet. Naquela ocasião, mais de 200 altos representantes de todos os setores sublinharam a urgência de encontrar mecanismos de comunicação, coordenação e cooperação, a fim de estabelecer a interoperabilidade jurídica e assegurar o devido processo legal transfronteiriço. Durante a 1ª Conferência Global, eles reconheceram que nenhum ator ou setor é capaz de resolver estes novos desafios por conta própria: a ação coletiva é necessária para evitar a escalada de uma corrida armamentista jurídica e a proliferação da insegurança jurídica. Com base nos Documentos de Conjuntura1[1] de cada um dos três Programas Temáticos do I&J, foram identificadas as principais Áreas de Cooperação2[2] para prosseguirem em conjunto.

Das opções de políticas ao roteiro de Ottawa

As Áreas de Cooperação serviram de mandato para os três Grupos de Contato de Programas temáticos, formados a partir da 1ª Conferência Global. Composto por membros de diversas entidades e especialistas mais engajados nas questões, eles foram incumbidos de propor o que pode ser realisticamente e pragmaticamente alcançado em cada um dos Programas do I&J.

Os membros, com o apoio do Secretariado, mapearam suas respectivas perspectivas, compararam abordagens, promoveram a coerência das políticas e identificaram possíveis medi-

1 <https://www.internetjurisdiction.net/news/framing-papers-released-for-data-content-and-domains>

2 <https://www.internetjurisdiction.net/uploads/pdfs/GIJC-Secretariat-Summary.pdf>

das para ações coordenadas. Os resultados dessas discussões foram sintetizados em documentos de *Opções de Políticas*3[3] publicados para consulta pelos atores em novembro de 2017.

Os documentos contribuíram para estruturar as discussões durante a 2ª Conferência Global da Rede de Políticas Internet & Jurisdição, realizada em Ottawa, de 26 a 28 de fevereiro de 2018. Mais de 200 participantes de mais de 40 países decidiram sobre foco e prioridades concretos, chegando pela primeira vez a um acordo sobre os objetivos comuns e as questões conjunturais de cada um dos três programas da Rede de Políticas. Estes Planos de Trabalho foram consolidados no *Roteiro de Ottawa* (Ottawa Roadmap)[4].

Abordagens operacionais

Com base na metodologia de trabalho dos Programas do I&J desenvolvidos entre a 1ª e 2ª Conferências Globais, mais de 120 membros de todos os continentes e setores começaram oficialmente seu trabalho em agosto de 2018 em novos Grupos de Contato para implementar os Planos de Trabalho do *Roteiro de Ottawa*. Três Coordenadores neutros foram nomeados para facilitar as discussões. Respectivamente:

- DADOS & Jurisdição: Robert Young, Conselheiro Jurídico, Assuntos Globais Canadá.
- CONTEÚDO & Jurisdição: Wolfgang Schulz, Diretor, Instituto Humboldt para Internet e Sociedade.
- DOMÍNIOS & Jurisdição: Maarten Botterman, Diretor, GNKS Consultoria.

Os Membros dos Grupos de Contato dos três Programas se comprometeram a trabalhar juntos e desenvolver abordagens operacionais de políticas em preparação para a 3ª Conferência Global da Rede de Políticas Internet & Jurisdição. O mandato dos Grupos de Contato dos três Programas foi definido com base nas Questões Estruturantes dos Planos de Trabalho do *Roteiro de Ottawa*. Em cada programa foram criados grupos de trabalho específicos para cada tema, com o intuito de realizar

3 <https://www.internetjurisdiction.net/news/policy-options-documents-released-for-the-2nd-global-Internet-and-jurisdiction-conference>

4 https://www.internetjurisdiction.net/news/outcomes-of-the-2nd-global-conference-of-the-Internet-jurisdiction-policy- network>

um trabalho focado e permitir interações mais intensas sobre questões específicas.

Os documentos *Abordagens Operacionais* apresentam o resultado deste processo. Eles representam um esforço dos Membros do Grupo de Contato de cada Programa para abordar questões transfronteiriças importantes relativas ao acesso à evidência eletrônica, restrições e moderação de conteúdo online e solicitações de suspensão de domínio, de forma consistente com o devido processo legal e a proteção dos direitos humanos.

3ª Conferência Global e mais além

A 3ª Conferência Global da Rede de Políticas Internet & Jurisdição será realizada de 3 a 5 de junho de 2019, em Berlim, Alemanha. Quando se reunirem em Berlim, as partes interessadas discutirão, com base nas *Abordagens Operacionais*, como avançar o desenvolvimento de normas de políticas e soluções operacionais concretas. O Roteiro de Berlim resultante desta 3ª Conferência Global orientará a próxima fase do trabalho das partes interessadas nos Programas da Rede de Políticas Internet & Jurisdição, em particular:

- Como as propostas contidas nas *Abordagens Operacionais* (Normas, Critérios e Mecanismos) podem ser utilizadas para melhorar a interoperabilidade jurídica,
- Como estruturar o trabalho futuro com base nas questões já identificadas que requerem ou justificam discussões mais aprofundadas;
- Como abordar as novas questões identificadas na 3ª Conferência Global de uma forma orientada a soluções.

Sumário

01.
Dados e Jurisdição

Abordagens Operacionais
Normas, critérios, mecanismos

CONTEXTO

Acesso transfronteiriço a provas eletrônicas – o desafio

O acesso a provas eletrônicas tornou-se central para as investigações policiais relativas não só à criminalidade online, mas também às atividades ilegais no espaço físico. As investigações, cada vez mais, exigem o acesso a provas eletrônicas armazenadas[1] em nuvem por empresas privadas em jurisdições fora do país solicitante.

De acordo com um relatório recente da UE[2], baseado em dados dos Estados-membros e nos relatórios de transparência dos provedores de serviços, as provas eletrônicas, sob qualquer forma, são relevantes em 85% do total das investigações criminais. Em quase dois terços (65%) das investigações em que as provas eletrônicas são relevantes, é necessário apresentar um pedido aos provedores estabelecidos em outra jurisdição. Consequentemente, 55% do total das investigações exigem o acesso transfronteiriço a provas eletrônicas. Espera-se que esta tendência se acelere ainda mais.

Neste contexto, os mecanismos existentes para pedidos transfronteiriços de dados de usuários estão sob pressão:

- O sistema dos Tratados de Assistência Jurídica Mútua (MLATs, na sigla em inglês) foi inicialmente concebido para tratar de casos relativamente raros, sendo geralmente considerado lento, complexo e carente de reforma. Ainda que melhorado, o sistema não está, de forma alguma, adaptado ao fato de que a grande maioria dos pedidos (94% para a UE) diz respeito a investigações em que a infração, a(s) vítima(s) e o(s) autor(es) do crime se encontram no próprio país que apresenta o pedido.
- Um grande volume dos pedidos diz respeito a grandes provedores estabelecidos nos Estados Unidos, mas o arcabouço atual da Lei de Privacidade das Comunicações Eletrônicas (Electronic Communications Privacy Act –

1 Este documento abrange o acesso aos dados armazenados e não a intercepção em tempo real. Também não aborda as consequências potenciais da utilização crescente da criptografia.

2 Ver Comissão Europeia, "Commission Staff Worlking Documents ", p. 14-15, disponível em <https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=SWD:2018:0118:FIN:EN:PDF>

ECPA) de 1986 apenas permite a comunicação voluntária por empresas americanas de dados que não sejam de conteúdo. Esta é a razão pela qual a maioria dos pedidos diretos atualmente abrange informações básicas do assinante e dados de tráfego.

Esta situação cria uma insegurança jurídica significativa e a arquitetura jurídica internacional pode efetivamente impedir a cooperação necessária para combater a criminalidade. Ações descoordenadas para enfrentar este desafio podem ter consequências indesejadas, incluindo o aumento de leis conflitantes entre si. É necessário um pensamento inovador para desenvolver, para além dos arcabouços legais existentes, mecanismos de cooperação transfronteiriça que protejam plenamente os direitos e a privacidade dos cidadãos, tendo em conta os cenários jurídicos e os procedimentos de investigação estabelecidos, bem como as diferenças de dimensão, natureza e capacidade das partes interessadas.

Dentro de cada país, as investigações policiais e o acesso a provas eletrônicas são regulamentados de acordo com procedimentos nacionais rigorosos, mas com diferenças locais significativas. Um desafio comum a todos os atores consiste, por conseguinte, em desenvolver mecanismos que permitam aos provedores o acesso a provas eletrônicas que se baseiem em normas elevadas de devido processo e de proteção dos direitos humanos.

A falta de mecanismos claros para o acesso transfronteiriço a provas eletrônicas incentiva a introdução de requisitos obrigatórios de localização de dados. Para além das questões significativas de viabilidade técnica, a generalização desta abordagem conduziria a grandes obstáculos para os agentes econômicos menores e colocaria em risco a natureza transfronteiriça da Internet.

Mais importante ainda, uma evolução significativa deve ser destacada no que diz respeito à localização dos dados. Enquanto a localização é um fator crítico para as provas físicas, a situação é marcadamente diferente para as provas eletrônicas. Não apenas é provável que as provas sejam armazenadas fora do território do país investigador, mas o uso crescente de serviços em nuvem torna a localização real mais incerta: a localização é determinada em função dos serviços técnicos

e não de razões legais e os dados podem ser divididos e distribuídos em vários locais. Assim, gradualmente assistimos ao reconhecimento de que se deve atribuir menos peso – se é que se deve atribuir algum – ao local de armazenamento dos dados solicitados. O ideal seria que qualquer regime aplicável aos pedidos transfronteiriços de provas eletrônicas funcionasse independentemente da localização dos dados.

Iniciativas existentes

Atores do ecossistema e do Programa Dados e Jurisdição da Rede de Políticas Internet & Jurisdição expressaram seu interesse em explorar de que maneira funcionam os regimes que permitem que as autoridades públicas emitam solicitações de provas eletrônicas diretamente aos provedores de serviços. Em 2016, estabeleceu-se um objetivo para identificar padrões de políticas que respeitem a privacidade e o devido processo legal, e definir as condições em que as autoridades policiais autorizadas podem solicitar às empresas estrangeiras o acesso aos dados armazenados de usuários, necessários para investigações lícitas de crimes.

O Programa Dados e Jurisdição procurou abordar as seguintes questões:

- De que maneira os fluxos de dados transnacionais e a proteção à privacidade podem ser conciliados com os requisitos legais de acesso para combater a criminalidade?
- Quais são as salvaguardas e os procedimentos necessários para estabelecer arcabouços legais viáveis e moduláveis que abordem a questão acima referida?

Iniciativas específicas recentes exploram diferentes abordagens para esta questão, nomeadamente:

- O **US CLOUD Act** foi assinado em março de 2018. Contém duas partes: em primeiro lugar, estabelece que os mandados emitidos pelos EUA a provedores dos EUA podem aplicar-se às provas eletrônicas que controlam, independentemente da sua localização; a lei prevê igualmente que o estatuto de bloqueio da ECPA seja suprimido para permitir que os provedores transfiram dados (incluindo dados de conteúdo) para autoridades públicas de países estrangeiros que tenham celebrado um acordo executivo com os Estados Unidos.

- **A Proposta de Regulação da UE** relativa às provas eletrônicas, apresentada pela Comissão Europeia em abril de 2018, foi revista pelo Conselho Europeu em novembro de 2018 e atualmente está sendo analisada pelo Parlamento Europeu. Prevê "Ordens de Produção de Provas" que permitam às autoridades competentes dos Estados-membros obrigar a transmissão de provas eletrônicas (de conteúdos e não conteúdos) diretamente dos operadores que "proveem serviços" aos usuários na UE. Estes provedores seriam obrigados a designar separadamente um representante legal na UE para esse efeito.
- O Comitê da Convenção sobre a Cibercriminalidade do Conselho Europeu atualmente está elaborando um **Protocolo Adicional à Convenção de Budapeste sobre a Cibercriminalidade**, a fim de permitir o acesso mais eficaz às provas eletrônicas.

Estas propostas introduzem ou preveem diferentes regras, salvaguardas e procedimentos para permitir que as autoridades responsáveis pela execução da lei emitam pedidos ou ordens transfronteiriças aos provedores de serviços para o acesso a provas eletrônicas.

Um arcabouço geral

O trabalho do Grupo de Contato da Rede de Políticas Internet & Jurisdição, tal como apresentado neste documento de *Abordagens Operacionais*, visa a contribuir para esta discussão, fornecendo um arcabouço geral sobre os componentes-chave que os regimes de pedidos transfronteiriços devem abordar, sua potencial escalabilidade e a forma de promover a interoperabilidade entre diferentes iniciativas deste tipo.

Secretariado da Rede de Políticas Internet & Jurisdição

Mensagem do coordenador

Foi uma honra atuar como Coordenador do Grupo de Contato do Programa Dados e Jurisdição. Agora posso confessar que não foi sem alguma hesitação que aceitei o papel no ano passado, por dois motivos. Em primeiro lugar, devido à formidável, e mesmo assustadora, experiência dos membros do Grupo de Contato, com participantes vindos de todo o mundo, que em muito excede a minha. A segunda foi a natureza premente das questões a abordar. Eu tinha consciência de que estas questões são complexas e a conciliação de interesses e perspectivas diferentes para produzir resultados úteis estava longe de estar garantida. Daí a minha hesitação.

Felizmente, os meus medos eram infundados em ambas as frentes. Os Membros do Grupo de Contato partilharam generosamente os seus conhecimentos, com paciência, modéstia e respeito mútuo, ao longo de inúmeras horas de videoconferência do Grupo de Contato e dos seus diferentes Grupos de Trabalho, sem falar no tempo de preparação e acompanhamento.

O Grupo de Contato era diversificado e verdadeiramente global – o nosso esforçado Secretariado enfrentou o desafio de agendar nossas reuniões, com membros provenientes de vários fusos horários na Europa, América do Norte, Austrália, Ásia, África e América do Sul. Além dessa diversidade geográfica, os Membros do Grupo de Contato trouxeram perspectivas de todos os setores de interesse que dão legitimidade e força à Rede de Políticas Internet & Jurisdição – governos, as maiores empresas de Internet do mundo, operadores técnicos, representantes da sociedade civil, da academia e de organizações internacionais.

Aproveito esta oportunidade para expressar a minha sincera gratidão aos Membros do Grupo de Contato pelo seu empenho, tempo e abordagem construtiva consistente. Um agradecimento especial aos Facilitadores que dedicaram esforços significativos para encontrar formulações que reflitam posições consensuais dentro do Grupo de Contato. Foi a expertise dos Membros, o alcance global e a diversidade de perspectivas, e o seu compromisso sustentado, que tornaram possíveis os resultados concretos do nosso trabalho, refletidos neste documento contendo as *Abordagens Operacionais*. Permitam-me também expressar a minha gratidão à equipe do Secretariado em Paris, sem a qual o trabalho não seria possível.

Eu realmente acredito que esses resultados serão de alto valor prático para as muitas partes interessadas que enfrentam as questões abordadas pelo Programa Dados e Jurisdição, e que os resultados também fornecerão uma base sólida para futuras discussões. Aguardo com expectativa esses intercâmbios, não só na próxima Conferência Global em Berlim, mas também no trabalho de acompanhamento nos próximos meses e anos.

Robert Young Coordenador
Grupo de Contato do Programa Dados e Jurisdição

Membros do Grupo de Contato do Programa Dados e Jurisdição

O Secretariado nomeou um Coordenador neutro para facilitar o trabalho do Grupo de Contato:

Robert Young
Consultor Jurídico
Canadá, Departamento de Assuntos Globais

As discussões nos Grupos de Trabalho, que ajudaram a realizar trabalhos concentrados em tópicos específicos, foram moderadas por Facilitadores neutros:

Sharon Bradford Franklin
Diretora
Política de Vigilância e Segurança Cibernética
Instituto de Tecnologia Aberta da Fundação New America

Debrae Kennedy-Mayo
Membro do Corpo Docente de Pesquisa
Instituto de Tecnologia da Georgia Scheller College of Business

MEMBROS DO GRUPO DE CONTATO

Sunil Abraham
Diretor Executivo
Centro para Internet e Sociedade

Waiswa Abudu Sallam
Chefe de Assuntos Jurídicos
Uganda
Comissão de Comunicações

Karen Audcent
Assessora Jurídica Sênior e Chefe de Equipe
Canadá
Ministério da Justiça

Kerry-Ann Barrett
Especialista em Políticas de Cibersegurança
Organização dos Estados Americanos

Cathrin Bauer-Bulst
Vice Chefe de Unidade
Luta contra o Cibercrime
Comissão Europeia
DG HOME

Eduardo Bertoni
Diretor
Argentina
Agência Nacional de Acesso à Informação Pública

Joseph Cannataci
Relator Especial do Direito à Privacidade
Nações Unidas

Jennifer Daskal
Professora Associada
American University
Washington College of Law

Fernanda Domingos
Procuradora Federal
Brasil
Ministério Público Federal

Brendan Eiffe
Chefe
Autoridade Central Irlandesa para Assistência Jurídica Mútua
Irlanda
Ministério da Justiça e da Igualdade

Thomas Fitschen
Diretor
Política Externa Cibernética e Segurança Cibernética
Alemanha
Ministério Federal das Relações Exteriores

Sharon Bradford Franklin
Diretora
Política de Vigilância e Cibersegurança
Instituto de Tecnologia Aberta da Fundação New America

Eric Freyssinet
Diretor de Estratégia Digital
França
Gendarmerie Nationale

Hartmut Glaser
Secretário-Executivo
Comitê Gestor da Internet no Brasil (CGI.br)

Nicole Gregory
Chefe
Políticas de Dados e Danos Online
Reino Unido
Ministério de Relações Exteriores e Commonwealth

Jane Horvath
Diretora Sênior
Privacidade Global
Apple

Gail Kent
Líder Global em Aplicação da Lei e Vigilância
Facebook

May-Ann Lim
Diretora Executiva
Asia Cloud Computing Organization

Drew Mitnick
Assessor Jurídico para Políticas
Acess Now

Vivek Narayanadas
Diretor de Proteção de Dados e Assessor Jurídico Geral
Shopify

Greg Nojeim
Advogado Sênior e Diretor
Projeto para a Liberdade
Segurança e Tecnologia
Center for Democracy & Technology

Barrack Otieno
Diretor-Geral
African Top-Level Domains
Organization (AfTLD)

Marc Porret
Advogado Sênior
Comitê das Nações Unidas contra o
Terrorismo
Diretoria Executiva (UNCTED)

Katitza Rodriguez
Diretora de Direitos Internacionais
Electronic Frontier Foundation (EFF)

Alberto Rodriguez Alvarez
Assessor para a Estratégia
Digital Nacional
México
Gabinete do Presidente

Alexander Seger
Secretário-Executivo
Comitê de Cibercrime e Convenção
e Chefe da Divisão de Cibercrime
Conselho da Europa

Acadia Senese
Advogada Sênior
Google

Bernard Shen
Advogado Geral Adjunto
Microsoft

Christoph Steck
Diretor
Políticas Públicas e Internet
Telefónica

Dan Suter
Diretor
iJust

Dan Svantesson
Co-Diretor
Bond University
Centre for Commercial Law

Peter Swire
Professor
Instituto de Tecnologia da Georgia
Scheller College of Business

Chris Wilson
Gerente Sênior
Políticas Públicas (Governança
de Internet)
Amazon Web Services

Herbert Gustav Yankson
Diretor de Cibercrime
Unidade do Departamento
de Investigação Criminal (CID)
Gana
Serviço de Polícia

Moctar Yedaly
Chefe
Departamento de Sociedade
da Informação
African Union Commission

Robert Young
Consultor Jurídico
Canadá
Departamento de Assuntos Globais

Além dos membros do Grupo de Contato, o Secretariado gostaria de agradecer aos seguintes atores por seu engajamento nos debates realizados no âmbito do Grupo de Contato e seus Grupos de Trabalho.

Melissa Blagitz
Procuradora da República
Brasil, Ministério Público Federal

Diego Canabarro
Assessor Especialista ao Conselho
Comitê Gestor da Internet no Brasil
(CGI.br)

Andrea Fabra
Gerente
Políticas Públicas e Internet
Telefónica

Camille Fischer
Stanton Fellow
Electronic Frontier Foundation (EFF)

Sebastian Kay
Chefe
Dados da UE e Internacionais
Reino Unido
Ministério de Relações Exteriores
e Commonwealth

Debrae Kennedy-Mayo
Membro do Corpo Docente de
Pesquisa do Instituto de Tecnologia
da Georgia
Scheller College of Business

Emmanuelle Legrand
Assessora Jurídica e de Políticas
Comissão Europeia
DG JUST

Toma Milieskaite
Assessor Jurídico
Comissão Europeia
DG JUST

Han Soal Park
Assessora Jurídica Associada
Direção Executiva do Comitê de
Combate ao Terrorismo das Nações
Unidas (UNCTED)

Kimberly Pearce
Advogada
Canadá
Departamento de Justiça

Paloma Villa Mateos
Gerente
Políticas Públicas e Internet
Telefónica

SÍNTESE DAS ABORDAGENS OPERACIONAIS

O documento *Abordagens Operacionais* a seguir é o resultado dos melhores esforços dos Membros do Grupo de Contato do Programa Dados e Jurisdição para abordar as questões importantes identificadas no *Roteiro de Ottawa* da 2ª Conferência Global da Internet & Jurisdiction Policy Network, realizada de 26 a 28 de fevereiro de 2018. O Plano de Trabalho que foi ajustado durante a Conferência identificou 15 importantes Questões Estruturantes para orientar ainda mais as interações dentro do Programa Dados e Jurisdição. Estas *Abordagens Operacionais* constituem uma contribuição conjunta de alguns dos especialistas mais envolvidos nessa área para fazer avançar o debate em curso sobre as complexas questões do acesso transfronteiriço a provas eletrônicas. **No entanto, elas não devem ser entendidas como o resultado de uma negociação formal validada pelas organizações desses Membros**.

Assim sendo, o Grupo de Contato do Programa, com a ajuda do Secretariado, elaborou o conjunto anexo de normas, critérios e mecanismos operacionais que contêm as disposições que o Grupo recomenda que sejam incluídas em qualquer arcabouço (incluindo leis nacionais e acordos internacionais aplicáveis) para pedidos/ordens transfronteiriças diretas de cumprimento da lei aos provedores de provas eletrônicas. Algumas das disposições recomendadas contêm requisitos obrigatórios (por exemplo, elementos que devem ser cumpridos de acordo com a abordagem recomendada) e algumas das disposições são recomendações que podem exigir um maior aperfeiçoamento ou adaptação para satisfazer as necessidades de países específicos.

Tendo em conta o pouco tempo disponível para abordar estas questões complexas, o trabalho dos Membros do Grupo de Contato do Programa foi distribuído em quatro Grupos de Trabalho temáticos, para propor, redigir e aperfeiçoar elementos que estão documentados de acordo com a estrutura tripartite apresentada na página 16.

Estas *Abordagens Operacionais* alimentarão a 3ª Conferência Global da Rede de Políticas Internet & Jurisdição, a ser realizada entre 3-5 de junho de 2019 em Berlim, organizada em parceria com o Governo da República Federal da Alemanha, e institucionalmente apoiada pelo Conselho da Europa, Comissão Europeia, ICANN, OCDE, CEPAL das Nações Unidas e UNESCO.

ESTRUTURA DAS ABORDAGENS OPERACIONAIS

O documento *Abordagens Operacionais* está organizado de acordo com a seguinte estrutura tripartite.

Normas operacionais

Esta seção identifica um conjunto de normas que podem ajudar a organizar o comportamento dos atores e suas interações mútuas. Concentram-se no nível operacional, no contexto dos princípios de alto nível existentes.

As Normas Operacionais de Dados e Jurisdição identificam elementos relativos a qualquer regime que permita o acesso transfronteiriço a provas eletrônicas e a pedidos/ordens individuais.

Critérios operacionais

Esta seção contém listas de elementos ou critérios que podem ser usados por todas as categorias de tomadores de decisão ao desenvolver, avaliar e implementar soluções. O objetivo é que todos os atores sejam capazes de discutir ideias, avaliar iniciativas e debater propostas usando arcabouços comuns de referência e questões estruturantes.

Os Critérios Operacionais de Dados e Jurisdição abordam três temas importantes do debate sobre o acesso às provas eletrônicas: **(I) Normas do regime** relativas ao escopo (tipos de crime e dados abrangidos), normas específicas aplicáveis a diferentes tipos de atores (autoridades, provedores e usuários) e mecanismos de transparência/responsabilidade; **(II) Escalabilidade**, levando em conta a diversidade dos provedores e das autoridades públicas e explorando modelos para a escalabilidade geográfica; e **(III) Padrões de pedidos/ordens** que explorem a questão da transmissão de pedidos/ordens individuais, os seus componentes e formatos necessários e o estabelecimento de nexos pelas autoridades públicas.

Mecanismo operacional

Esta terceira seção apresenta uma proposta para a qual os esforços de operacionalização podem ser dirigidos no período após a 3ª Conferência Global da Rede de Políticas Internet & Jurisdição, em Berlim.

A nota conceitual detalha a ideia de identificadores de interoperabilidade para componentes de pedidos/ordens, a fim de permitir a transferência e o tratamento de pedidos transfronteiriços de provas eletrônicas de uma forma eficiente e que respeite as mais elevadas garantias aos direitos substantivos e processuais.

NORMAS OPERACIONAIS

Uma abordagem geral relativa ao acesso transfronteiriço a provas eletrônicas pode basear-se nos seguintes elementos.

Regime[3]

Qualquer regime que permita a apresentação de pedidos/ordens transfronteiriças aos provedores de serviços de prova eletrônica deve considerar

Devido Processo Legal, para isso:

- Garantias processuais de alto nível mutuamente acordadas definem as condições em que as autoridades públicas podem emitir pedidos/ordens válidos e aos quais os provedores devem atender;
- Os provedores e usuários devem ter à sua disposição requisitos e procedimentos de notificação e vias para apresentação de recurso claros;
- As regras e os procedimentos relevantes devem estar disponíveis de forma transparente e acessíveis ao público.

Escalabilidade, para que o regime possa:

- Gerenciar um número crescente de pedidos/ordens e se adaptar de forma flexível conforme necessário;
- Ser resiliente em um contexto de rápidas evoluções tecnológicas;

---

3 Uma definição clássica de um regime internacional é: "Princípios, normas, regras e processos de decisão implícitos ou explícitos em torno dos quais convergem as expectativas dos atores numa determinada área das relações internacionais" - Krasner, Stephen D. 1983 in International Regimes, Cornell University Press. Ver também a definição de governança da Internet na Agenda de Túnis para a Sociedade da Informação (WSIS). [N.E.: Para edição em português da Agenda de Túnis: <https://www.cgi.br/media/docs/publicacoes/1/CadernosCGIbr_DocumentosCMSI.pdf>]

- Acomodar autoridades públicas relevantes em vários níveis e provedores com diversos papéis, tamanhos e capacidades;
- Envolver progressivamente um número crescente de países diversos ou ser replicável de forma sustentável, de acordo com rigorosos requisitos fundamentais;
- Interoperar com outras estruturas com finalidades semelhantes e o mesmo nível de padrões.

Pedidos /ordens

Os pedidos/ordens individuais transfronteiriços de acesso a provas eletrônicas devem permitir a verificação de:

Completude, incluindo:

- Informações de autenticação verificáveis que permitam ao destinatário confirmar o país e a entidade que fazem o pedido;
- Informações de apoio suficientemente detalhadas, com componentes de formato claros e acordados, que permitam a avaliação da adequação à legislação nacional aplicável, do direito internacional e do regime ao abrigo do qual o pedido/ordem é emitido.

Respeito às normas relevantes, na medida em que o pedido/ordem:

- É emitido e redigido em plena conformidade com as disposições da legislação nacional aplicável e com o regime a que está sujeito;
- Fornece uma certificação independente de que a norma acordada e os requisitos mínimos para este tipo específico de pedido/ordem foram cumpridos.

Nexo, pelo estabelecimento pelo país emissor de:

- Sua ligação substancial com o crime;
- Seu legítimo interesse em obter os dados específicos pretendidos;
- Sua consideração aos interesses potenciais de outros atores.

A comunicação, coordenação e cooperação entre vários países podem ser necessárias para garantir o respeito aos direitos, assegurar a máxima eficácia, distribuir responsabilidades e evitar comprometer os procedimentos existentes.

CRITÉRIOS OPERACIONAIS

Os seguintes critérios representam os melhores esforços dos Membros do Grupo de Contato do Programa Dados e Jurisdição e seus Grupos de Trabalho, conforme compilados pelo Secretariado da I&J, na identificação de listas concisas de elementos ou critérios que podem ser usados por todas as categorias de tomadores de decisão ao desenvolver, avaliar e implementar soluções. O objetivo é que todos os atores sejam capazes de discutir ideias, avaliar iniciativas e debater propostas usando arcabouços de referência e questões estruturantes comuns.

Os seguintes documentos devem ser entendidos como uma base para referência e futuros trabalhos da Rede de Políticas Internet & Jurisdição, após sua 3ª Conferência Global. Abaixo listamos Critérios Operacionais para o Programa Dados e Jurisdição:

Parte I - Normas do Regime

- CRITÉRIOS A - Escopo do Regime
- CRITÉRIOS B - Autoridades Públicas
- CRITÉRIOS C - Provedores
- CRITÉRIOS D - Usuários
- CRITÉRIOS E - Transparência / Accountability*

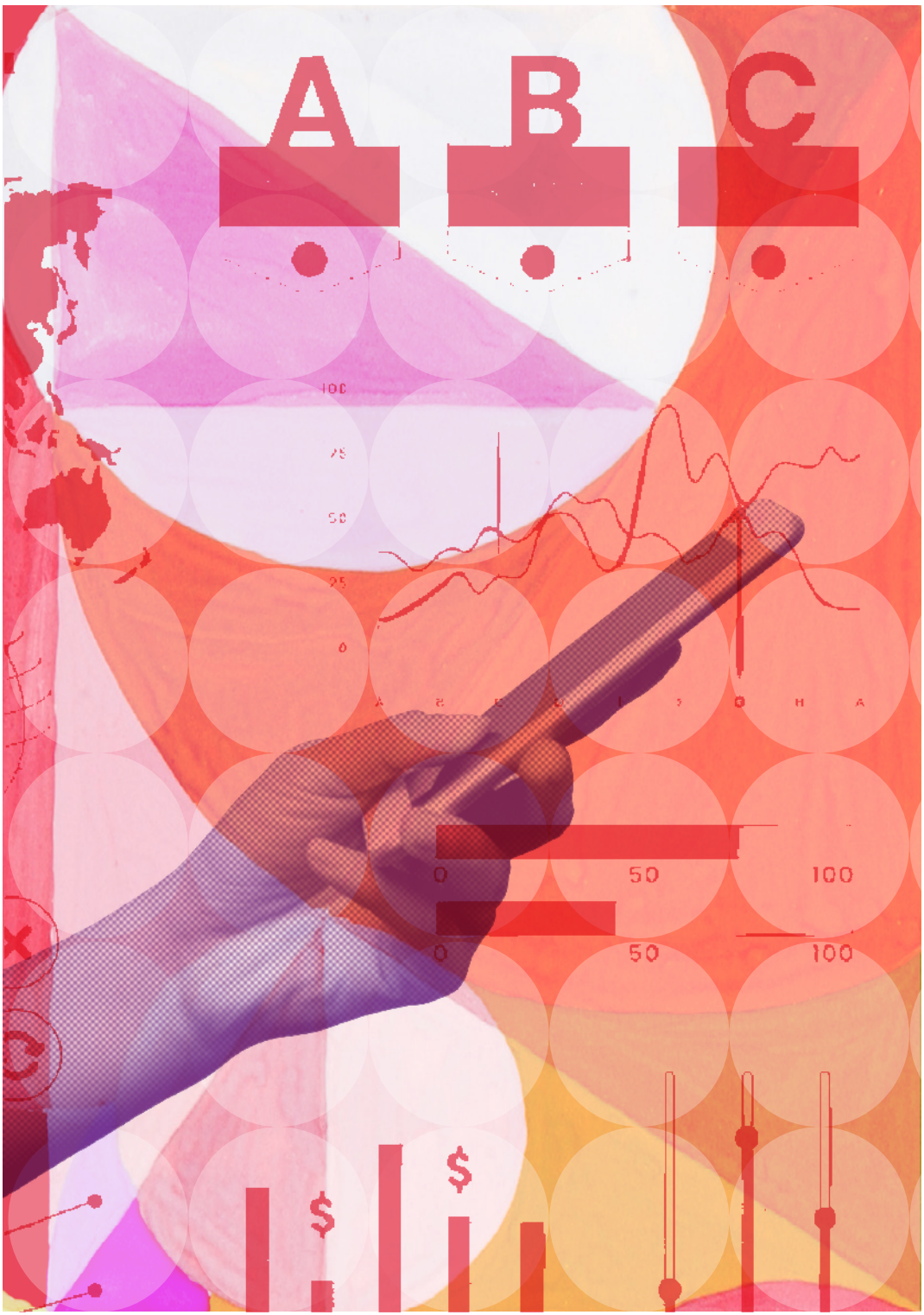
Parte II - Escalabilidade

- CRITÉRIOS F - Diversidade de Autoridades Públicas
- CRITÉRIOS G - Diversidade de Provedores
- CRITÉRIOS H - Escalabilidade Geográfica

Parte III - Normas para Pedidos / Ordens

- CRITÉRIOS I - Transmissão
- CRITÉRIOS J - Formatos de Pedido
- CRITÉRIOS K - Nexo

*Para fins desta publicação, optou-se por manter a palavra "accountability" no original em inglês, para maior consistência de sentido.


A
B
C
100
75
50
25
0
0
50
100
0
50
100
$
$

PARTE I - NORMAS DO REGIME

Critérios A - Âmbito de Aplicação do Regime

1. Dados abrangidos:

Conteúdo e demais informações privadas e protegidas, conforme definido pela lei aplicável, detidos pelos provedores.

2. Tipo(s) de crime(s) abrangido(s):

Os pedidos/ordens para o envio de dados podem ser emitidos com o intuito de obter informações que possam contribuir para a detecção, investigação ou repressão a crimes

a. Considerados crimes graves[4]; e
b. Quando a detecção, investigação e/ou acusação não infringe os direitos humanos internacionais[5].

Critérios B - Autoridades Públicas

1. Grau de validação judicial/independente, com base em cada pedido (e em situações de emergência):

Para cada pedido/ordem de envio de conteúdo ou outra informação privada e protegida, as leis nacionais e/ou acordos internacionais aplicáveis devem exigir a revisão e aprovação prévia obrigatória por um tribunal, juiz, magistrado ou outra autoridade independente, previstos por lei.

As jurisdições podem optar por permitir as seguintes exceções ao requisito de revisão e aprovação prévias:

a. em situações de emergência que impliquem perigo iminente de morte ou lesão física grave de uma pessoa[6], caso em que será necessário um controle e aprovação independentes por um tribunal, juiz, magistrado ou outra autoridade indepen-

---

4 Não houve consenso sobre a necessidade de acrescentar "puníveis no país requerente com uma pena de pelo menos 3 anos" como definição de crimes graves. Este critério deixa o termo "crimes graves" indefinido, o que permitiria uma maior variação entre países.

5 O Grupo não chegou a um consenso sobre a exigência da dupla incriminação, mas busca salvaguardas contra pedidos/ordens para o envio de dados para ações penais que infrinjam o direito internacional em matéria de direitos humanos.

6 Alguns Membros do Grupo gostariam de acrescentar aqui "ou ameaça iminente à infraestrutura essencial", mas outros membros se opuseram fortemente a essa redação. Notamos que esta é uma área onde há variação de abordagens entre os diferentes países que podem precisar ser resolvidas à medida que os acordos internacionais forem finalizados.

dente, previstos por lei, para que o país requerente possa utilizar os dados após o término da situação de emergência; e

b. para pedidos de preservação dos dados específicos solicitados, caso em que a legislação nacional aplicável e/ou os acordos internacionais exigem uma autorização independente de um tribunal, juiz, magistrado ou outra autoridade independente, prevista por lei, antes de poder ter acesso e utilizar os dados.

Os países devem dotar suas autoridades independentes com recursos suficientes para lhes permitir o cumprimento das regras e normas do regime.

2. Grau de provas:

As normas para análise e aprovação (conforme especificado no ponto 1 acima) dos pedidos/ordens para envio de dados devem:

a. exigir uma base jurídica e factual consistente que demonstre que a informação pretendida constitui prova de um crime que está sendo investigado e que é de competência do país requerente.

b. ser rigoroso, assegurando a proteção dos direitos humanos internacionais, incluindo a proteção adequada da privacidade pessoal, de acordo com os direitos humanos internacionais.

3. Necessidade e proporcionalidade:

Os países devem exigir que os pedidos/ordens cumpram as normas de necessidade e proporcionalidade da legislação internacional dos direitos humanos.

Critérios C - Provedores

1. Esclarecimento de pedidos/ordens:

O regime deve estabelecer um procedimento que proteja os direitos dos provedores de serviços de pedir esclarecimentos aos países requerentes sobre os pedidos/ordens para envio de dados.

2. Desafios referentes a pedidos/ordens por parte do provedor:

a. O regime deve estabelecer um procedimento claro para que uma autoridade independente ouça e julgue os recursos dos provedores em relação aos pedidos/ordens para envio de dados.

b. O regime deve estabelecer direitos processuais e substantivos para que os provedores possam contestar qualquer pedido/ordem de envio de dados[7], quando[8].

i. o pedido/ordem de envio de dados for excessivo, abusivo, violar os termos de um acordo internacional ou for ilegal;

ii. o pedido/ordem de envio de dados for feito para efeitos de procedimento penal ou punição de uma pessoa em virtude da raça, religião, nacionalidade, origem étnica, opinião política, sexo ou orientação sexual dessa pessoa, e/ou

iii. o cumprimento do pedido/ordem possa causar danos a essa pessoa por qualquer das razões acima, ou possa violar os direitos humanos internacionais ou os direitos de uma pessoa ao abrigo das leis aplicáveis;

c. Os provedores devem poder solicitar que os países onde estão localizadas suas sedes apresentem objeções aos pedidos/ordens quando o provedor acreditar que o pedido/ordem foi feito com a finalidade de processar ou punir uma pessoa por causa de sua raça, religião, nacionalidade, origem étnica, opinião política, gênero ou orientação sexual, ou que o cumprimento do pedido/ordem causaria danos a essa pessoa por qualquer desses motivos, ou violaria os direitos humanos de uma pessoa ou os direitos de uma pessoa sob as leis aplicáveis[9].

3. Situações de conflitos de leis, incluindo análise de cortesia:

Os acordos internacionais devem prever um mecanismo para resolver quaisquer questões relativas a conflitos de leis com outros países quando tais conflitos surgem em relação a pedidos/ordens.

7 Há um reconhecimento de que as empresas maiores estarão melhor posicionadas para exercer esses direitos do que os provedores menores.

8 Há falta de consenso sobre a lista de motivos abaixo.

9 Há falta de consenso sobre este ponto.

Critérios D - Usuários

1. Condições de notificação aos usuários e confidencialidade dos pedidos/ordens[10]:

a. A regra-padrão deve ser a de que os países requerentes têm o dever de notificar os usuários no momento em que um pedido/ordem que pretenda obter os seus dados é emitido. O regime deverá garantir que os provedores tenham o direito de avisar seus usuários. No entanto, o aviso pode ser adiado e o pedido/ordem pode ser mantido em sigilo durante um período de tempo limitado, caso a divulgação possa comprometer um inquérito em curso. A notificação só deve ser adiada pelo tempo que for necessário para proteger a investigação.

b. O regime deve prever que, ao solicitar o sigilo de uma ordem, os investigadores do país requerente devem (1) apresentar seus argumentos a favor do sigilo à autoridade independente que analisa e aprova os pedidos/ordens; e (2) apresentar fatos específicos para justificar por que razão o próprio país requerente não deve ser obrigado a notificar o usuário e por que razão deve limitar o direito do provedor de notificar seus clientes sobre o pedido. O regime deverá prever que qualquer ordem de não divulgação imposta a um provedor seja estritamente limitada em termos de duração e âmbito e não restrinja o direito de o provedor falar mais do que o necessário para responder à necessidade de sigilo prestado pelas autoridades judiciais. O regime deverá igualmente garantir que os provedores sejam autorizados a contestar as ordens de confidencialidade para garantir que tais ordens de confidencialidade satisfaçam esses requisitos.

10 Há falta de consenso sobre este ponto. Alguns se opõem por princípio e outros, pelo contrário, gostariam que esse aviso ao país de origem do provedor fosse feito simultaneamente ao pedido ao provedor, para ajudar a identificar potenciais abusos à medida que vão ocorrendo.

2. Acesso a vias de recurso (suspeitos e demais usuários relevantes) e informações sobre essas vias de recurso:

O regime deve garantir que todos os usuários cujos dados são solicitados (suspeitos e demais usuários relevantes) tenham uma oportunidade significativa de contestar a transmissão e utilização dos seus dados.

a. Isto inclui a capacidade de contestar o pedido/ordem com base nos seguintes fundamentos:
   i. o pedido/ordem é excessivo, irrelevante, ou abusivo, ou viola os termos de um acordo internacional ou é de outra forma ilegal;
   ii. o pedido/ordem foi apresentado com o objetivo de processar ou punir uma pessoa em virtude da sua raça, religião, nacionalidade, origem étnica, opinião política, sexo ou orientação sexual;
   iii. o cumprimento do pedido/ordem causaria prejuízo a essa pessoa por qualquer uma dessas razões, ou violaria os direitos humanos internacionais de uma pessoa ou os direitos de uma pessoa ao abrigo da legislação aplicável; e/ou
   iv. os usuários estão exercendo qualquer outro direito que possam ter ao abrigo da legislação aplicável.
b. Os procedimentos para tais contestações podem ser fornecidos através de qualquer processo penal aplicável em que as autoridades governamentais procurem utilizar esses dados, através das autoridades de proteção de dados ou através de outros recursos legais e civis nacionais disponíveis.

Critérios E - Transparência / Accountability

1. Modalidades de coleta de estatísticas (incluindo informações de autoridades públicas) e disponibilidade pública desses dados:

a. A autoridade jurídica competente de cada país deve disponibilizar ao público as regras que regem os pedidos/ordens para envio de dados transfronteiriços, incluindo os procedimentos a seguir e as normas aplicáveis para avaliar se tais pedidos/ordens são autorizados e legítimos.
b. A autoridade jurídica competente de cada país deve publicar, de forma regular e periódica, estatísticas que indiquem o número de pedidos/ordens para envio de dados

transfronteiriços que emitiram durante o período relevante, os tipos de dados solicitados e o número de pedidos/ordens que deram origem à produção de dados.

c. Os provedores devem publicar, de forma regular e periódica, estatísticas que mostrem o número de pedidos/ordens para envio de dados transfronteiriços recebidos, bem como o número de contas e/ou usuários abrangidos por esses pedidos/ordens. Em seus relatórios, os provedores devem indicar o número de pedidos/ordens para os quais produziram dados e o número de pedidos/ordens rejeitados.

2. Notificação:

Numa base periódica, os países requerentes devem comunicar os pedidos/ordens para envio de dados ao país do provedor (país onde se situa a sede do provedor). As notificações devem conter informações suficientes para facilitar a accountability, ajudando o país que recebe as notificações a avaliar a observância do regime e a determinar se os acordos implementados devem ser renovados. O conteúdo destas notificações também deve ser adaptado na medida do necessário para proteger a privacidade e a confidencialidade[11].

10/11 Há falta de consenso sobre este ponto. Alguns se opõem por princípio e outros, pelo contrário, gostariam que esse aviso ao país de origem do provedor fosse feito simultaneamente ao pedido ao provedor, para ajudar a identificar potenciais abusos à medida que vão ocorrendo.

Critérios F - Diversidade de Autoridades Públicas

1. Estruturas administrativas

Os regimes devem poder ter em conta a heterogeneidade das possíveis organizações administrativas existentes nos países, incluindo, em especial, as diferenças entre países federativos e unitários.

2. Autoridades de origem habilitadas

Quaisquer que sejam as modalidades de validação e transmissão independente dos pedidos transfronteiriços (ver acima), os pedidos são apresentados pelos atores responsáveis pela investigação, em conformidade com a legislação e os procedimentos nacionais. Dada a diversidade da organização nacional de competências entre jurisdições, qualquer regime deve definir quais são os níveis autorizados a emitir pedidos aos provedores estrangeiros.

3. Autenticação

Os provedores devem poder autenticar a agência de execução da lei que inicia o pedido, ou seja, ter a certeza de que o requerente é efetivamente quem ou o que declara ser, em paralelo com os critérios pertinentes que determinam seu direito de emitir esses pedidos transfronteiriços. Esta autenticação deve fazer parte do sistema eletrônico através do qual o provedor recebe o pedido e pode ser estabelecida de várias formas possíveis[12], nomeadamente:

a. Pré-registro individual em portais de empresas, através, por exemplo, da utilização de uma conta de correio eletrônico governamental reconhecível, de uma declaração em papel timbrado oficial de um alto funcionário responsável pela aplicação da lei e/ou de uma ordem ou outro documento oficial de um tribunal, juiz ou outro órgão independente. Esta abordagem tem sido viável para países e empresas de maior dimensão, o que abrange a maioria dos pedidos globais. No entanto, esta abordagem pode não ser facilmente viável para todos os países ou empresas menores.

12 Esta lista descreve algumas abordagens de autenticação potenciais ou existentes, porém, sem prejudicar o nível de apoio de que gozam os diferentes métodos.

b. Um sistema de portais de transmissão entre países que integrem essas funcionalidades de autenticação.
c. Um mecanismo específico estabelecido em acordos bilaterais (como o previsto no CLOUD Act dos EUA) que confira a autoridade de autenticação a uma entidade específica no país solicitante, que, por sua vez, autorize as entidades de execução da lei apropriadas a usar o sistema de transmissão.
d. Uma entidade específica, diferente do país emissor ou do país destinatário, que credencie uma autoridade nacional para tratar do sistema de autenticação nacional ou que forneça endereços de correio eletrônico autenticados.
e. Um sistema geral de autenticação, potencialmente distribuído, que forneça tokens individuais a entidades de execução da lei previamente registradas.

Devem ser estabelecidos procedimentos específicos que permitam a autenticação em situações de pedidos/ordens urgentes ou sensíveis ao fator tempo, mesmo que a autoridade requerente não tenha sido previamente autenticada.

É necessária atenção especial para garantir a segurança do sistema de autenticação, a fim de evitar abusos.

Critérios G - Diversidade De Provedores

1. Tamanhos

Os pequenos provedores de serviços podem enfrentar desafios específicos. Independentemente das disposições especiais que lhes possam ser aplicáveis, tais disposições podem contemplar esforços mútuos para lidar com os pedidos, nomeadamente:

a. Representação local compartilhada para o recebimento de pedidos/ordens de regimes (como a proposta de regulamento da UE relativa à prova eletrônica) que assim o exijam,
b. A criação - ou assinatura - de portais conjuntos, preservando canais de comunicação separados para diferentes provedores, mas alavancando economias de escala.

2. Tipos de dados

Diferentes serviços armazenam diversos tipos de dados. Os provedores podem desenvolver documentação específica para ajudar as autoridades públicas a compreender quais são as informações que podem ser acessíveis e quais os procedimentos e salvaguardas correspondentes.

Critérios H - Escalabilidade Geográfica

1. Direitos humanos:

Qualquer regime que permita às autoridades responsáveis pela execução da lei exigir que os provedores de serviços forneçam provas eletrônicas transfronteiriças deve impor a todos os países participantes o respeito e a proteção dos direitos humanos internacionais.

2. Modelos de escalabilidade

As três abordagens atualmente previstas para estabelecer regimes para os pedidos transfronteiriços aproximam-se, de diferentes formas, da potencial escalabilidade geográfica de um número crescente de países:

a. O **CLOUD Act dos EUA** prevê a conclusão de sucessivos acordos executivos bilaterais entre os Estados Unidos e os países que eles consideram que apresentam garantias materiais e processuais suficientes em seu sistema jurídico. O arcabouço global exigirá significativas negociações de acordos país a país, e apenas um número limitado de países poderá cumprir as normas exigidas com o arcabouço jurídico atual.

b. O **Regulamento da UE sobre provas eletrônicas** (*E-evidence*) atualmente em discussão na União Europeia, visa a permitir a emissão de Ordens de Produção de Provas obrigatórias, de acordo com critérios detalhados de validade. Não se destina a ser aplicado para além dos membros da UE, mas países de outras partes do mundo podem ver nesta abordagem um modelo que pode ser replicado nacional ou regionalmente, permitindo, progressivamente, uma forma de escalabilidade geográfica. No entanto, nada garantirá que proteções suficientes de direitos humanos sejam sempre incorporadas em tais regimes, uma vez que eles serão estabelecidos unilateralmente.

c. O Protocolo Adicional à Convenção de Budapeste atualmente em discussão no Conselho da Europa estará, tal como a própria Convenção, aberto à adesão de qualquer país que subscreva às suas disposições. Seu modelo de escalabilidade, portanto, corresponde ao tradicional modelo multilateral de escalabilidade geográfica, com todos os seus benefícios e potenciais limitações.

3. Cumprimento dos requisitos de validação para cada pedido

Tal como indicado acima, o atual arcabouço jurídico de determinados países poderá não satisfazer os elevados padrões esperados num regime de acesso transfronteiriço a provas eletrônicas. Frequentemente argumenta-se que a incapacidade desses países de emitir pedidos transfronteiriços, mesmo em situações legítimas, constitui um incentivo para o estabelecimento de requisitos obrigatórios de localização de dados com potenciais consequências nocivas de ordem econômica e de segurança. Nesses casos, pode-se considerar pelo menos duas vias para remediar esta situação:

a. O país solicitante utiliza apenas determinados procedimentos de acordo com suas leis existentes: O país requerente compromete-se a utilizar apenas determinados procedimentos da legislação em vigor nesse país que assegurem que proteções suficientes são atendidas para a comunicação de provas eletrônicas.

Exemplo: As leis do país A permitem que um mandado seja obtido mediante a assinatura de um funcionário responsável pela execução da lei ou juiz. Os pedidos transfronteiriços só serão considerados válidos se forem aprovados em conformidade com a via judicial prevista na legislação em vigor no país A.

b. O país requerente adota disposições adicionais aplicáveis especificamente aos pedidos transfronteiriços.

Exemplo: As leis do país A podem prever a aprovação de um juiz somente após um mandado emitido por um funcionário responsável pela execução da lei não ter sido bem-sucedido na obtenção da prova pretendida. Uma pequena alteração à legislação do país permitiria a utilização da via judicial para os pedidos transfronteiriços.

Tais abordagens poderiam aplicar-se tanto no contexto de acordos bilaterais ao abrigo do US CLOUD Act quanto em qualquer esforço para implementar um regime nacional inspirado nos procedimentos propostos pela UE em matéria de provas eletrônicas. No entanto, isto aborda apenas a questão específica da introdução de uma validação judicial quando o sistema jurídico existente nem sempre a exige para os pedidos internos e não aborda outras limitações potenciais nos arcabouços jurídicos existentes nos países.


BLOG

PARTE III - NORMAS PARA PEDIDOS / ORDENS

Além das disposições do regime relativas ao grau de validação independente, ao nível de prova, à necessidade e à proporcionalidade (tal como descritas nos critérios B - Autoridades Públicas), devem ser considerados os seguintes elementos no que diz respeito aos pedidos/ordens individuais.

Critérios I - Transmissão

1. Canais seguros e rastreabilidade

Os pedidos/ordens para envio de dados devem ser transmitidos aos provedores de forma segura, seguindo as melhores práticas de segurança de dados, como a criptografia de ponta-a-ponta. O sistema de transmissão dos pedidos/ordens deve ser rastreável, para que os provedores e os usuários possam avaliar a autenticidade dos pedidos/ordens e permitir auditorias regulares.

2. Autoridades emissoras

Os países devem limitar[13] o número de Pontos de Contato (POCs) autorizados a transmitir pedidos/ordens para envio de dados, a fim de garantir a qualidade dos pedidos/ordens e ajudar os provedores a verificar a autenticidade dos pedidos/ordens.

3. Certificação

A transmissão dos pedidos/ordens de emissão pode realizar, ainda, uma verificação não material dos pedidos/ordens no que se refere à integralidade e à conformidade com os requisitos processuais do regime específico ao abrigo do qual os pedidos/ordens são emitidos.

4. Identificação do destinatário (POC ou Representante)

O número de POCs por provedor deve ser limitado para simplificar a autenticação, mas os provedores devem ter permissão para ter mais de um POC conforme necessário. Os provedores devem divulgar os POCs aos países que deles necessitam e mantê-los atualizados.

---

13 Há falta de consenso sobre este ponto. Alguns receiam que isso crie gargalos na transmissão e só considerariam essa ideia se os pedidos/ordens forem automaticamente transmitidos e processados.

Critérios J - Formatos de Pedido

1. Formulário escrito

Todos os pedidos/ordens para envio de dados transfronteiriços dirigidos aos provedores de serviços devem ser feitos por escrito, incluindo por via eletrônica, mesmo em situações de emergência.

2. Idioma

Os pedidos/ordens devem ser enviados no idioma do país requerente e, sempre que necessário para assegurar que os funcionários do provedor compreendam o pedido/ordem, deverão também ser traduzidos para um dos principais idiomas falados no país do provedor.

3. Componentes e formatos do pedido[14]

GRUPO	ROTULAGEM	DESCRIÇÃO
REFERÊNCIA	Número do pedido	Número de ID da solicitação que identifica o pedido específico; usado para rastreamento de referência e potenciais auditorias.
	Horário	Data e hora de emissão pelo país requerente.
	País emissor	Indica o país de origem do pedido.
	Empresa destinatária	Indica o destino da solicitação, especificamente, o Ponto de Entrada (POE).
	Número do processo	Identifica o processo judicial correspondente no país requerente.
STATUS	Status da solicitação	Identifica se a demanda é nova ou se é para acompanhar um pedido de Assistência Jurídica Mútua (MLA) ou uma ordem de preservação anteriores.
	Pedidos/ordens de preservação ou pedidos de MLA anteriores	Informações sobre qualquer pedido/ordem de preservação ou pedido de MLA anteriOres.
	Status do processo	Identifica o status e o progresso do processo no país requerente, no momento do pedido (por exemplo, prejulgamento, julgamento, crime em curso, etc.).

14 Esta lista de componentes foi identificada com base em diferentes modelos e formatos elaborados no contexto, principalmente, da proposta da UE em matéria de provas eletrônicas, do Conselho da Europa T-CY, bem como de um estudo conjunto da UNCTED, UNODC e IAP.

GRUPO	ROTULAGEM	DESCRIÇÃO
DADOS BUSCADOS	Informações sobre a conta	Identifica o alvo específico da solicitação: endereço de IP específico, nome de domínio, URL, identificadores de usuário ou contas (critérios de especificidade).
	Dados solicitados	Dados específicos do usuário que estão sendo solicitados, com o mais alto grau de precisão.
	Intervalo de tempo/ Período	Período de tempo abrangido pelo pedido/ordem relacionados aos dados solicitados.
PRAZOS	Prazo de entrega	Identifica os prazos específicos associados ao pedido.
	Emergência	Identifica se as circunstâncias têm caráter de urgência.
	Justificativa para a emergência	Justificativa para a emergência (por exemplo, a sua natureza, relação do pedido à emergência, de que forma pode evitar a ocorrência de uma emergência, etc.).
CONFIDENCIALIDADE	Confidencialidade	Especifica se determinadas circunstâncias justificam que parte ou a totalidade do pedido não seja comunicada ao usuário em causa.
	Justificativa para a confidencialidade	Justificativa para a ausência de notificação.
	Prazo para confidencialidade	Duração da exceção de confidencialidade.

GRUPO	ROTULAGEM	DESCRIÇÃO
CASO	Ilícito	Descrição do ato ilícito alegado.
	Base jurídica	Arcabouço jurídico nacional no qual se baseia este pedido; um link direto a uma versão online da lei/jurisprudência correspondente em inglês poderia ser um requisito para validade/aceitabilidade do pedido.
	Resumo do processo	Fatos, relação com os dados, finalidade e necessidade, acusações formalizadas/lista dos crimes.
	Regime internacional	Arcabouço jurídico ao abrigo do qual o pedido transfronteiriço é emitido.
AUTORIDADES	Autoridade emissora	Autoridade e/ou o POC que emitiu o pedido e seus respectivos dados.
	Autoridade de validação	Autoridade que validou o pedido no país requerente e seus respectivos dados.
	Autoridade de investigação / judicial	Dados da autoridade responsável pela investigação ou pelo exercício da ação penal do crime no país requerente.

GRUPO	ROTULAGEM	DESCRIÇÃO
CONTATOS	Notificação de resposta	Dados de contato no país requerente para o qual as notificações de resposta devem ser encaminhadas.
	Recebimento de dados	Dados da autoridade do país requerente para a qual as informações do usuário/suspeito devem ser transferidas.
	Informações de Contato	Ponto de Contato no país solicitante que será o ponto focal para perguntas de acompanhamento ou informações adicionais.
CERTIFICAÇÃO	Certificação	Auto-certificação pela autoridade emissora.
ASSINATURA	Assinatura	Identifica a assinatura e/ou carimbo da autoridade de validação.
OUTROS		

A tabela abaixo e os asteriscos nela contidos são sugestões não exaustivas sobre como os itens correspondentes podem ser usados. Não se deve tirar conclusões prescritivas ou normativas pela presença ou ausência de um asterisco em qualquer célula.

GRUPOS		ROTULAGEM	NECESSÁRIO PARA A GESTÃO TÉCNICA	ÚTIL PARA RELATÓRIOS DE TRANSPARÊNCIA	RELEVANTE PARA DETERMINAR RESPOSTA(S) (SUBSTANTIVO)	DECISIVO PARA A VALIDADE DOS PEDIDOS OU ORDENS (PROCESSUAL)
REFERÊNCIA	1.1	Número do pedido				
	1.2	Horário				
	1.3	País emissor	x	x		x
	1.4	Empresa Destinatária	x	x	x	
STATUS	2.1	Status da solicitação				
	2.2	Pedidos/ordens de preservação ou pedidos de MLA anteriores	x			
	2.3	Status do processo				
DADOS BUSCADOS	3.1	Informações sobre a conta	x		x	
	3.2	Dados solicitados	x			x
	3.4	Período	x		x	

GRUPOS		ROTULAGEM	NECESSÁRIO PARA A GESTÃO TÉCNICA	ÚTIL PARA RELATÓRIOS DE TRANSPARÊNCIA	RELEVANTE PARA DETERMINAR RESPOSTA(S) (SUBSTANTIVO)	DECISIVO PARA A VALIDADE DOS PEDIDOS OU ORDENS (PROCESSUAL)
PRAZOS	4.1	Prazo	x			
	4.2	Emergência	x	x	x	
	4.3	Justificativa para a emergência			x	
	4.4	Sensibilidade a prazos	x	x	x	
	4.5	Justificativa para a sensibilidade a prazos			x	
CONFIDENCIALIDADE	5.1	Confidencialidade	x	x	x	
	5.2	Justificativa para a confidencialidade			x	
	5.3	Prazo para confidencialidade	x			
PROCESSO	6.1	Ilícito		x	x	
	6.2	Base jurídica		x	x	
	6.3	Resumo do processo			x	
	6.4	Número do processo				
	6.5	Nível de sanção			x	
	6.6	Regime internacional		x	x	x
AUTORIDADES	7.1	Autoridade emissora				x
	7.2	Autoridade de validação				x
	7.3	Autoridade de investigação/ judicial				x
CONTATOS	8.1	Notificação de resposta	x			
	8.2	Recebimento dos dados	x			
	8.3	Informações de contato	x			x
CERTIFICAÇÃO	9.1	Certificação				x
ASSINATURA	10.1	Assinatura				x

Critérios K - Nexo

1. Conexão substancial

A localização de um crime no território de um país é geralmente aceita como, e continua a ser, o principal critério que determina seu direito de investigar, e as regras, procedimentos e critérios nacionais para determinar a localização de crimes físicos estão bem estabelecidos.

No entanto, com relação aos crimes que envolvem a utilização de meios digitais, a determinação da localização do crime é frequentemente mais complexa, devendo levar em conta outros fatores, como a localização do(s) suspeito(s) no momento em que o crime é cometido e/ou a localização da(s) vítima(s).

Ao estabelecer o direito de investigar, as regras e os procedimentos nacionais também podem levar em conta:

a. A localização do dano, sem esquecer-se do risco de criar uma jurisdição universal de facto para crimes com danos muito distribuídos;
b. A nacionalidade do(s) suspeito(s) e da(s) vítima(s), uma vez que é um princípio geralmente aceito do direito internacional público, o fato de que os Estados podem proteger os seus cidadãos e podem investigar os atos dos seus cidadãos.

2. Interesse legítimo em obter os dados específicos buscados

No contexto de um regime específico de acesso transfronteiriço a provas eletrônicas, as autoridades públicas que emitem um pedido/ordem individual justificam o seu interesse legítimo nos dados específicos buscados quando:

a. O crime investigado está dentro do escopo da legislação penal do país e o acesso solicitado está dentro do escopo do poder de investigação legal das autoridades públicas;
b. O crime investigado insere-se no âmbito do regime, tendo em conta os potenciais limiares de fixação de pena em função do tipo de dados pretendido;
c. As normas do regime referentes às provas são atendidas (ver Critérios B - Autoridades Públicas, ponto 2 - "Grau de provas");
d. Podem demonstrar que a mesma informação não pode ser obtida por outros meios.

3. Interesses de terceiros

a. Os seguintes fatores podem ajudar as autoridades requerentes a identificar, no início ou no decurso do procedimento, os interesses potenciais de outros atores:
   i. Os direitos, em particular o direito à privacidade, do suspeito, da vítima e de qualquer outra parte cujos dados serão acessados, de acordo com a sua nacionalidade ou residência, logo que sejam conhecidos;
   ii. O risco de impor obrigações a uma parte que entre em conflito com os deveres ou direitos que essa parte possa deter ao abrigo da legislação estrangeira aplicável;
   iii. A probabilidade de que a medida investigativa possa ter impacto nas investigações em curso em outro Estado;
   iv. A potencial multiplicidade de países afetados pelo crime, de modo a assegurar o respeito da regra *"ne bis in idem"*.

b. À luz destes elementos, e no âmbito das disposições do regime de acesso direto pertinente, a autoridade requerente pode avaliar sua interação adequada com os países:
   i. Cujos cidadãos ou residentes são visados pelo pedido/ordem de envio de dados;
   ii. Onde o controlador de dados está localizado, quando aplicável.

c. Tal interação pode incluir:
   i. Abster-se de emitir a solicitação/ordem;
   ii. Notificar o Estado em causa;
   iii. Permitir que outro Estado assuma a liderança nas investigações;
   iv. Coordenação com um ou vários Estados na investigação;
   v. Mecanismos, incluindo a análise de cortesia, para evitar conflitos de leis com países terceiros e resolver esses conflitos, caso surjam.

MECANISMO OPERACIONAL
LINGUAGEM DE MARCAÇÃO (MARKUP) E TAGS DE INTEROPERABILIDADE

Contexto

Os dados armazenados por provedores de serviços sediados no estrangeiro constituem atualmente provas essenciais para uma porcentagem crescente de investigações criminais. Devido às limitações das formas tradicionais de obtenção destes dados, principalmente através dos Tratados de Assistência Jurídica Mútua (MLATs), as autoridades públicas enviam um número cada vez maior de pedidos transfronteiriços diretamente a estes provedores estrangeiros, tanto para a preservação quanto para a produção destas informações.

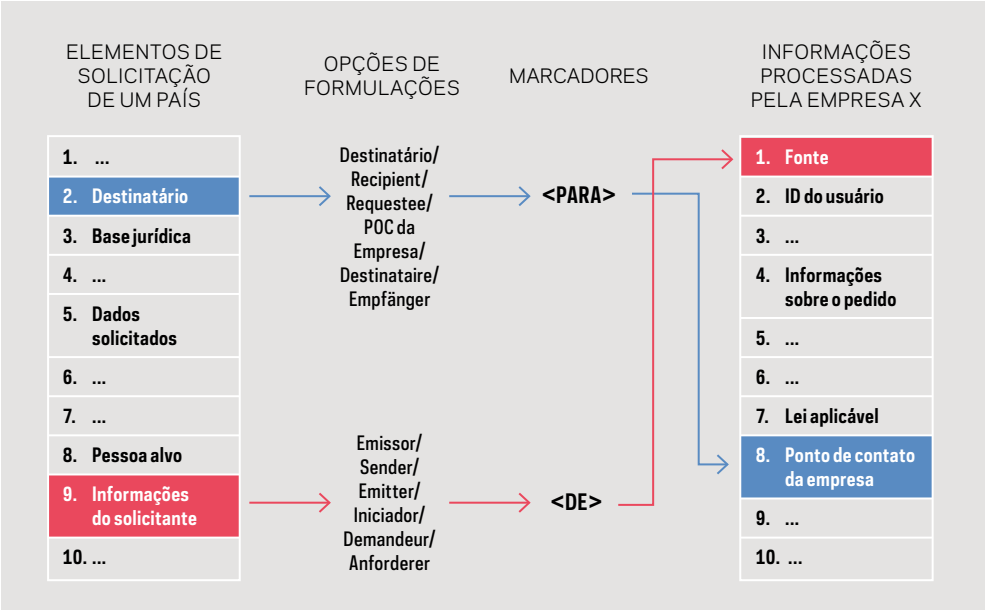
Várias autoridades públicas já desenvolveram ou estão desenvolvendo seus próprios formulários para esses pedidos. Algumas têm sistemas de arquivo exclusivos para produzi-los. Ao mesmo tempo, os maiores provedores desenvolvem seus próprios portais elaborados para apresentação de pedidos, enquanto os provedores menores têm apenas Pontos de Contato (POC) para o relato de abusos. Algumas autoridades consideram esta heterogeneidade ineficaz, porque pode conduzir a duplicações na introdução de informações, além de gerar a obrigação de aprender numerosos procedimentos.

No entanto, a padronização completa dos formatos dos pedidos e dos mecanismos de envio seria difícil. A total padronização também não é desejada pelos diferentes atores, que estão ligados às suas respectivas práticas. Entretanto, a harmonização não é necessária: uma abordagem orientada para a interoperabilidade trará mais benefícios.

De fato, a análise dos diferentes formatos de pedidos (existentes ou propostos) revela uma semelhança significativa. Embora a rotulagem das seções e a sua ordem possam diferir, o seu conteúdo é muito semelhante: informações sobre o requerente e o requerido, a base jurídica do pedido, o procedimento seguido, os dados específicos pretendidos, ou a justificativa para emergência, para citar apenas alguns. O mapeamento desses elementos comuns da forma sugerida abaixo pode permitir a interoperabilidade entre atores com benefícios significativos para todos.

A ideia de uma linguagem de marcação (markup)

Na Web, as etiquetas HTML anotam os elementos-chave de um determinado texto em um servidor, permitindo que o navegador do usuário exiba a página com precisão após a transmissão. Por analogia aproximada, um conjunto compartilhado de marcadores poderia ajudar a identificar e codificar os vários componentes típicos dos pedidos de acesso a dados. Isso permitiria uma comunicação clara entre os atores, independentemente da forma como os pedidos foram preparados ou serão tratados, das identificações utilizadas em ambos os lados, ou mesmo do idioma utilizado, como ilustrado nestes exemplos simples:



A implementação desta linguagem de marcação deve ser voluntária. Sua capacidade de promover a eficiência e a interoperabilidade deve, no entanto, incentivar uma ampla e progressiva adoção. Além disso, o desenvolvimento cooperativo e a atualização regular deste conjunto de marcações por parte de autoridades públicas, empresas e outros atores relevantes devem também promover uma maior confiança entre eles.

Benefícios operacionais

A existência de tal padrão de interoperabilidade proporcionaria os seguintes benefícios adicionais em termos de:

- **Neutralidade de ponta-a-ponta** - A abordagem é neutra em relação a qualquer sistema de transmissão já utilizado ou a ser desenvolvido;
- **Flexibilidade** - Acomoda diferentes estruturas e ordem de componentes de solicitação pelos diferentes atores;
- Facilidade de implementação - Solicitantes e destinatários que já desenvolveram seus próprios sistemas podem continuar a usá-los e só precisam desenvolver conversores de formato simples;
- **Escalabilidade** - Autoridades públicas e atores privados de pequeno porte podem facilmente desenvolver ferramentas (ou utilizar algumas desenvolvidas por terceiros) para produzir ou gerir pedidos de qualidade;
- **Devido processo legal** - a existência de tais pedidos estruturados facilitará a avaliação da sua completude e conformidade com qualquer norma de qualidade acordada no âmbito de um regime;
- **Fluxo de trabalho** - A empresa receptora pode classificar e distribuir automaticamente partes da solicitação para seus serviços relevantes, por exemplo: informações de base jurídica para seu departamento jurídico e informações sobre os dados solicitados para seu departamento operacional. Isto promove a eficiência e a confidencialidade;
- **Segurança** - Partes sensíveis das solicitações podem ser diferenciadas e criptografadas;
- **Transparência** - A informação estatística de nível superior pode ser facilmente separada e coletada, simplificando a elaboração de relatórios;
- **Versatilidade** - Os marcadores permitem um fácil mapeamento para rotulagens em vários idiomas.

Como nota final, embora atualmente explorado para pedidos diretos, esse conjunto de marcadores também poderia ser útil no contexto de pedidos de MLA e outras interações entre governos.

Próximos passos

A 3ª Conferência Global da Rede de Políticas Internet & Jurisdição em Berlim pode discutir a validade desta proposta, o mandato potencial e a cronologia desse grupo, bem como formas de assegurar o envolvimento dos atores mais relevantes.

02.
Conteúdo e Jurisdição

Abordagens Operacionais
Normas, critérios, mecanismos

CONTEXTO
CONTEÚDO ONLINE - OS DESAFIOS

Todos os dias, várias centenas de milhões de mensagens e imagens e centenas de milhares de horas de vídeos são carregados apenas nas principais plataformas da Internet e estão disponíveis em todo o mundo por natureza, em virtude da ausência de fronteiras técnicas da Internet. Uma grande diversidade de serviços privados online que acolhem conteúdos gerados pelos usuários tornou-se, assim, um instrumento fundamental para o exercício da liberdade de expressão e do debate público por bilhões de usuários, graças a serviços sem autorização prévia e com boa experiência de usuário.

No entanto, o conteúdo legal em um país pode ser ilegal em outro. Além disso, à medida que cresce o número de usuários da Internet, cresce também a diversidade das suas referências sociais, culturais, políticas ou religiosas e, por conseguinte, a sua sensibilidade em relação aos vários conteúdos. Os serviços online também podem ser utilizados indevidamente e existe uma crescente sensibilização para a presença de conteúdos ilegais ou nocivos online. Além disso, comportamentos e opiniões que antes eram efêmeros e confinados à esfera privada podem agora obter visibilidade significativa, amplo alcance geográfico, permanência temporal e até mesmo replicação viral.

O desafio comum a todos os atores é como lidar com os abusos de uma forma que seja oportuna e eficiente, mas que respeite plenamente os princípios internacionais de direitos humanos e permita o desenvolvimento da economia digital. O desafio é agravado porque várias jurisdições estão frequentemente envolvidas. São necessários esforços especiais para permitir a coexistência de diferentes normas em espaços online e garantir que as restrições de conteúdos sejam necessárias e proporcionais, com as devidas salvaguardas processuais.

Nenhum ator ou setor pode resolver este enigma por si só, mas podemos ter esperado, coletivamente, tempo demais para abordar estas questões. Consequentemente, os atores públicos e privados, sob a pressão da urgência, agora desenvolvem numerosas iniciativas de forma descoordenada, introduzindo mudanças significativas em dois aspectos.

EVOLUÇÃO DO CENÁRIO NORMATIVO

As legislações nacionais apresentam níveis muito diversos de coerência normativa em relação aos diferentes tipos de conteúdo. De fato, existe um consenso significativo sobre a inaceitabilidade global de alguns conteúdos (como material de abuso sexual de crianças); no entanto, há grande variação quanto aos critérios para restrições legítimas de muitos outros tipos de conteúdo[1], incluindo incitação à violência, discurso de ódio, assédio, difamação ou desinformação. As legislações podem legitimamente refletir as sensibilidades culturais, históricas, políticas e religiosas específicas das comunidades locais em relação ao conteúdo aceitável ou não. No entanto, por vezes, podem não respeitar plenamente as normas internacionais em matéria de direitos humanos e as garantias de um devido processo legal.

Nos últimos anos, as autoridades públicas em todo o mundo têm reforçado cada vez mais a aplicação da sua legislação em matéria de conteúdos online, tendo sido elaboradas ou propostas novas regulamentações. Garantir a compatibilidade destas diferentes regras e determinar a extensão geográfica adequada da sua aplicação continua sendo algo a ser resolvido e constitui uma potencial causa de tensões.

Paralelamente, os provedores têm desenvolvido termos de serviço e diretrizes de comunidade cada vez mais pormenorizados – e frequentemente atualizados – que estabelecem regras aplicáveis aos seus espaços online. Algumas dessas regras são específicas para a comunidade que o serviço pretende atender, mas outras são mais genéricas. Dado o papel proeminente desempenhado pelos principais atores no ecossistema, a aplicabilidade global destas normas influencia diretamente o conteúdo considerado legítimo ou não no ciberespaço no seu conjunto. Por conseguinte, as diretrizes de comunidade representam cada vez mais uma fonte adicional que deve ser levada em conta nesta conjuntura normativa complexa e híbrida.

Até pouco tempo atrás, as principais questões relativas às restrições online eram as seguintes: a aplicabilidade das legislações nacionais territorialmente delimitadas aos espaços online

1 O Programa Conteúdo e Jurisdição não aborda especificamente questões relacionadas à propriedade intelectual e direitos autorais.

transfronteiriços, os procedimentos adequados para as ordens de restrição de conteúdos emitidas por autoridades públicas e a forma como os provedores devem responder a essas ordens. No entanto, à luz da evolução descrita acima, os mecanismos através dos quais os conteúdos são restringidos pelos atores privados em aplicação das suas próprias regras tornam-se um tópico adicional e importante.

Evolução do papel dos intermediários

A Seção 230 da Communications Decency Act (Lei de Decência das Comunicações - CDA) de 1996, dos Estados Unidos, a Diretiva de Comércio Eletrônico na União Europeia, adotada em 2000 e alguns regulamentos similares de outros países[2] têm historicamente concedido ampla proteção aos intermediários de conteúdo gerado pelo usuário, desde que eles tenham agido rapidamente quando notificados da sua ilegalidade. No entanto, no contexto de uma maior conscientização sobre os abusos, alguns atores questionaram esses regimes de responsabilidade dos intermediários, defendendo uma mudança nas estruturas existentes de notificação e retirada de conteúdo para plataformas que assumam um papel mais proativo de monitoramento e moderação.

Como resultado, foram desenvolvidos códigos de conduta público-privados e novas legislações que impõem cada vez mais responsabilidades aos provedores privados, incluindo tempos de resposta curtos para certos tipos de conteúdo (em particular o extremismo violento), sob pena de multas significativas. Paralelamente ao crescente nível de detalhamento das suas diretrizes de comunidade, as grandes empresas, em resposta, desenvolvem cada vez mais ferramentas algorítmicas, incluindo algumas baseadas em inteligência artificial, para a detecção de conteúdos que justifiquem restrições e a prevenção de sua republicação, uma vez identificados. Um grande número de moderadores está sendo contratado, vias de encaminhamento internas estão sendo estabelecidas e mecanismos de recurso estão sendo previstos, à medida que os atores privados se tornam os principais tomadores de decisão em matéria de restrições de conteúdos online.

---

2 O "World Intermediary Liability Map" do Stanford CIS, disponível em <https://wilmap.law.stanford.edu/map>, enumera essas regulamentações em uma base nacional.

Estas evoluções alteram significativamente a distribuição de responsabilidades entre atores públicos e privados, bem como o nível das garantias processuais implementadas. As consequências podem ainda não ser totalmente compreendidas, dadas as diferentes dimensões, capacidades e tipos de serviços dos provedores. A existência de obstáculos adicionais à entrada no mercado poderá dificultar o surgimento de novos atores, impedindo a concorrência.

Quadros de cooperação

Os diferentes atores reconhecem a complexidade aguda desses desafios. Manifestaram interesse em trabalhar em conjunto para desenvolver procedimentos e normas que permitam conciliar os seguintes objetivos complementares: maximizar a necessária prevenção e reparação de danos, minimizar as restrições à liberdade de expressão e permitir o desenvolvimento contínuo da economia digital. São necessárias orientações e mecanismos comuns mais claros para lidar adequadamente com conteúdos abusivos: os instrumentos existentes baseados em jurisdições territoriais rigorosas são postos em cheque e poderá ser necessária alguma inovação institucional.

O trabalho do Grupo de Contato dedicado da Rede de Políticas Internet & Jurisdição, tal como apresentado neste documento *Abordagens Operacionais*, visa a contribuir para esta discussão, abordando os elementos-chave de um quadro geral relativo à moderação e restrição responsáveis de conteúdos.

Secretariado da Rede de Políticas Internet & Jurisdição

Mensagem do coordenador

Os debates sobre conteúdo e jurisdição não podem ser separados da questão da moderação e restrição de conteúdo online em geral, que, por natureza, têm uma forte dimensão de direitos humanos. No âmbito do arcabouço internacional de direitos humanos, a liberdade de expressão e o acesso à informação só podem ser restringidos pelos Estados se devidamente justificados por lei e proporcionais. No entanto, de acordo com os já bem estabelecidos Princípios Ruggie, as empresas também têm a responsabilidade de respeitar os direitos humanos e, portanto, respeitar o padrão de proporcionalidade. A proporcionalidade também é relevante para os efeitos transfronteiriços das restrições de conteúdo.

Tanto as leis nacionais quanto as normas de comunidade estabelecidas pelas empresas formam agora um ambiente normativo complexo que rege o tipo de conteúdo que é retirado ou permanece em plataformas online. Os Estados que emitem pedidos de restrição de conteúdo com base nas normas de comunidade das empresas, e não em suas leis nacionais, são um exemplo de potencial hibridação entre governança estatal e não estatal. Isto levanta questões delicadas que só podem ser abordadas com maior clareza jurídica, tal como salientado nas *Abordagens Operacionais* anexas.

O mesmo se aplica às garantias processuais e à transparência. Além da questão da base jurídica sobre a qual são feitas

as restrições de conteúdo, quem toma tais decisões também é importante. Neste contexto, são sugeridas diferentes formas de organismos externos para proporcionar vias de recurso, seja para uma ou várias plataformas, por iniciativa de uma determinada empresa (por exemplo, Facebook) ou com base em uma legislação nacional. O Grupo de Contato explorou, entre outros aspectos, as principais questões suscitadas pela criação de tais estruturas, caso se pretenda que sejam criadas de forma inclusiva e transparente.

Espera-se que o presente documento, *Abordagens Operacionais*, possa ajudar os tomadores de decisão (por exemplo, autoridades públicas, políticos, juízes, líderes de empresas) a desenvolver políticas e a tomar decisões, quando necessário, baseadas no pleno respeito ao princípio da proporcionalidade, incluindo no que se refere:

1. Ao âmbito geográfico das restrições,
2. À ação mais adequada em função do tipo de conteúdo em causa, ao dano potencial correspondente e ao contexto;
3. À utilização de tecnologia (filtragem algorítmica, incluindo sistemas baseados em IA)

As Normas, Critérios e Mecanismos Operacionais propostos certamente contribuirão para um arcabouço de políticas global que respeite os direitos humanos, no que diz respeito à moderação e restrições de conteúdo. O debate salienta igualmente a necessidade de uma reflexão fundamental sobre os atuais sistemas de governança da Internet e suas limitações. Poderão ser necessárias novas disposições institucionais para, pelo menos, assegurar a compatibilidade entre regimes de governança muito diferentes. Em particular, os debates sobre os respectivos papéis e responsabilidades dos atores são especialmente importantes. Esses desafios devem ser enfrentados e espera-se que este esforço aponte na direção certa.

Wolfgang Schulz, Coordenador,
Grupo de Contato do Programa Conteúdo e Jurisdição

Membros do Grupo de Contato do Programa Conteúdo e Jurisdição

O Secretariado nomeou um Coordenador neutro para facilitar o trabalho do Grupo de Contato:

Wolfgang Schulz
Diretor
Humboldt Institute for Internet and Society

As discussões nos Grupos de Trabalho, que ajudaram a realizar trabalhos centrados em tópicos específicos, foram moderadas por Facilitadores neutros:

Hawley Johnson
Diretor Associado
Columbia Univeristy
Projeto Global de Liberdade de Expressão

Juan Carlos Lara
Diretor de Conteúdo
Derechos Digitales

Jason Pielemeier
Diretor de Políticas
Global Network Initiative (GNI)

Membros do Grupo de Contato

Chinmayi Arun
Professora Assistente de Direito e Diretora Executiva
National Law University Delhi
Centro para Governança de Comunicação

Susan Benesch
Diretora de Projeto
Dangerous Speech Project

Guy Berger
Diretor de Liberdade de Expressão e Desenvolvimento de Mídia
UNESCO

Ellen Blackler
Vice-Presidente de Políticas Públicas Globais
The Walt Disney Company

Agnes Callamard
Diretora, Columbia University
Projeto Global de Liberdade de Expressão

Maria Paz Canales
Diretora Executiva
Derechos Digitales

Mark Carvell
Chefe de Política Internacional Online, Reino Unido
Departamento de Cultura, Meios de Comunicação Social e Esportes

Alexander Corbeil
Analista Sênior de Pesquisas
Canadá
Departamento de Segurança Pública

Jacques De Werra
Professor e Vice-Reitor
University of Geneva

Agustina Del Campo
Diretora
University of Palermo
Centro de Estudos sobre a Liberdade de Expressão (CELE)

Harlem Desir
Representante para a Liberdade de Imprensa, OSCE

Elena Dodonova
Administradora
Divisão de Meios de Comunicação e Internet
Conselho da Europa

Anriette Esterhuysen
Assessora Sênior de Governança da Internet
Association for Progressive Communication

Miriam Estrin
Gerente de Políticas Públicas
Google

Raquel Gatto
Assessora de Política Regional
Internet Society

Daniel Holznagel
Conselheiro Jurídico
Alemanha
Ministério Federal da Justiça e da Defesa do Consumidor

Raman Jit Singh Chima
Diretor para Políticas da Ásia e Assessor Jurídico Sênior Internacional
Access Now

David Kaye
Relator Especial para a Promoção e Proteção do Direito à Liberdade de Opinião e Expressão
Nações Unidas

Edison Lanza
Relator Especial para a Liberdade de Expressão
Organização dos Estados Americanos (OEA)

Emma Llanso
Diretora, Projeto de Livre Expressão, Center for Democracy & Technology

Rebecca Mackinnon
Diretora
Ranking Digital Rights
New America Foundation

Katherine Maher
Diretora Executiva
Wikimedia Foundation

Giacomo Mazzone
Chefe de Relações Institucionais e Relações com os Membros
European Broadcasting Union (EBU)

Corynne Mcsherry
Diretora Jurídica
Electronic Frontier Foundation (EFF)

Paul Nemitz
Assessor-chefe
Comissão Europeia
DG JUST

Juan Ortiz-Freuler
Policy Fellow
Fundação World Wide Web

Elena Perotti
Diretora Executiva
Relações Públicas e Política de Mídia
WAN-IFRA

Nick Pickles
Estrategista Sênior de Políticas Públicas
Twitter

Jason Pielemeier
Diretor de Políticas
Global Network Initiative (GNI)

Thomas Schneider
Vice-Diretor
Suíça, Departamento Federal de Comunicações

Wolfgang Schulz
Diretor
Alexander von Humboldt Institute for Internet and Society

Bernard Shen
Advogado Geral Adjunto
Microsoft

Carlos Affonso Souza
Diretor
Instituto de Tecnologia e Sociedade (ITS Rio)

Christoph Steck
Diretor
Políticas Públicas e Internet
Telefónica

Peter Stern
Gerente de Políticas
Relacionamento com as Partes Interessadas
Facebook

Além dos membros do Grupo de Contato, o Secretariado gostaria de agradecer aos seguintes atores pelo seu empenho nos debates realizados no âmbito do Grupo de Contato e dos seus Grupos de Trabalho.

Ana Andrijevic
Assistente de Pesquisa e Ensino
University of Geneva

Bach Avezdjanov
Diretor de Programa
Columbia University
Projeto Global de Liberdade de Expressão

Nikki Bourassa
Diretora de Programas e Políticas
Global Network Initiative (GNI)

Amy Brouillette
Gerente Sênior de Pesquisa e Editorial
Ranking Digital Rights

Jorge Cancio
Vice-Diretor de Relações Internacionais
Suíça
Departamento Federal de Comunicações

Giovanni De Gregorio
Pesquisador Jurídico
WAN-IFRA

Jan Gerlach
Gerente Sênior de Políticas Públicas
Wikimedia Foundation

Tonei Glavinic
Diretor de Operações
Dangerous Speech Project

Xianhong Hu
Especialista em Comunicação e Informação
UNESCO

Hawley Johnson
Diretora Associada
Columbia University
Projeto Global de Liberdade de Expressão

Gayatri Khandhadai
Coordenador de Projeto Association for Progressive Communications

Juan Carlos Lara
Diretor de Conteúdo
Derechos Digitales

Nathalie Marechal
Analista Sênior de Pesquisas
Ranking Digital Rights

Drew Mitnick
Assessor de Políticas
Access Now

Paula Real
Policy Fellow
Internet Society

Amos Toh
Consultor Jurídico ao Relator Especial das Nações Unidas para a Liberdade de Expressão

Sarvjeet Singh
Diretor Executivo
Centro para Governaça de Comunicação
National Law University Delhi

Paloma Villa Mateos
Gerente de Políticas Públicas e Internet
Telefónica

Liz Woolery
Vice-Diretora
Projeto para Liberdade de Expressão
Center for Democracy & Technology

SÍNTESE DAS ABORDAGENS OPERACIONAIS

O documento *Abordagens Operacionais* a seguir é o resultado dos esforços dos Membros do Grupo de Contato do Programa Conteúdo e Jurisdição para abordar as questões importantes identificadas no *Roteiro de Ottawa* da 2ª Conferência Global da Rede de Políticas Internet & Jurisdição, realizada de 26 a 28 de fevereiro de 2018. O Plano de Trabalho aprimorado durante a Conferência identificou 13 Questões Estruturantes importantes para orientar ainda mais as interações no âmbito do Programa Conteúdo e Jurisdição. Estas *Abordagens Operacionais* são uma contribuição conjunta de alguns dos especialistas mais engajados neste assunto para fazer avançar o debate em curso sobre as complexas questões das restrições transfronteiriças aos conteúdos online. **Não devem, no entanto, ser entendidas como o resultado de uma negociação formal validada pelas organizações às quais esses Membros estão ligados.**

Assim sendo, os Membros do Grupo de Contato do Programa, com a ajuda do Secretariado, elaboraram o conjunto de Normas, Critérios e Mecanismos Operacionais propostos em anexo para proporcionar um quadro comum de referência para os diversos atores. Estas *Abordagens Operacionais* pretendem ajudar os tomadores de decisão públicos e privados a ter em conta toda a gama de parâmetros relevantes ao desenvolver e implementar quadros, regras e práticas responsáveis para combater abusos, no pleno respeito pelos princípios internacionais dos direitos humanos.

Tendo em conta o pouco tempo disponível para abordar estas questões complexas, o trabalho dos Membros do Grupo de Contato do Programa foi distribuído em quatro Grupos de Trabalho temáticos, para propor, redigir e aperfeiçoar os elementos que estão documentados de acordo com a estrutura tripartite apresentada na página 16.

Estas *Abordagens Operacionais* irão alimentar a 3ª Conferência Global da Rede de Políticas Internet & Jurisdição, a ser realizada entre 3 e 5 de junho de 2019 em Berlim, organizada em parceria com o Governo da República Federal da Alemanha, e institucionalmente apoiada pelo Conselho da Europa, Comissão Europeia, ICANN, OCDE, CEPAL das Nações Unidas e UNESCO.

ESTRUTURA DAS ABORDAGENS OPERACIONAIS

O documento *Abordagens Operacionais* está organizado de acordo com a seguinte estrutura tripartite.

Normas Operacionais

Esta seção identifica um conjunto de normas que podem ajudar a organizar o comportamento dos atores em suas próprias ações e interações mútuas. Centram-se no nível operacional, no contexto dos princípios de alto nível já existentes.

As Normas Operacionais de Conteúdo e Jurisdição identificam especificamente elementos relativos à clareza da estrutura conceitual, padrões de proporcionalidade, garantias processuais e accountability.

Critérios Operacionais

Esta seção contém listas de elementos ou critérios que podem ser usados por todas as categorias de tomadores de decisão ao desenvolver, avaliar e implementar soluções. O objetivo é que todos os atores sejam capazes de discutir ideias, avaliar iniciativas e debater propostas usando arcabouços comuns de referência e questões estruturantes.

Os Critérios Operacionais de Conteúdo e Jurisdição abordam cinco temas importantes no debate sobre restrição de conteúdo online: **(I) Clareza da estrutura**, incluindo os tipos de conteúdo para os quais são emitidos pedidos de restrição e a base normativa para tais pedidos; **(II) Detecção**, incluindo a distinção entre avisos de terceiros e detecção pelos provedores; **(III) Ação proporcional**, incluindo elementos relativos à atualidade, avaliação, restrições geograficamente proporcionais e uma tipologia de ações; e **(IV) Escalabilidade**, para chamar a atenção para a diversidade de capacidade de provedores e países.

Mecanismo Operacional

Esta terceira seção apresenta uma proposta sobre a qual os esforços de operacionalização podem basear-se após a 3ª Conferência Global da Rede de Políticas Internet & Jurisdição, em Berlim.

A nota conceitual detalha como estruturar as discussões sobre os novos mecanismos de recurso após a restrição de conteúdo e como organizar melhor os próximos passos durante a 3ª Conferência Global e no trabalho de acompanhamento.

NORMAS OPERACIONAIS

Uma abordagem geral relativa às restrições de conteúdo[3] pode basear-se nos seguintes elementos.

Clareza da Estrutura

Definições - Um vocabulário compartilhado sobre os diferentes tipos de conteúdo ilegal ou nocivo e ações restritivas embasam o desenvolvimento e a implementação de regimes legais e práticas empresariais.

Base normativa - A redação inequívoca e compreensível das leis nacionais e das diretrizes de comunidades privadas garante a previsibilidade normativa para todos.

Responsabilidades - Os respectivos direitos e responsabilidades dos atores públicos e privados são claramente determinados, tendo em conta, se for o caso, a natureza e a dimensão dos serviços.

Proporcionalidade

Direitos - As decisões de restrição têm em conta e visam a conciliar, ou pelo menos equilibrar, os direitos potencialmente concorrentes de todos os atores relevantes.

Granularidade - As restrições são aplicadas ao menor item de conteúdo possível que permita resolver eficazmente o problema.

Restrições geograficamente proporcionais - As decisões das autoridades públicas e dos atores privados preservam a mais ampla disponibilidade de conteúdos legítimos.

---

3 As "restrições de conteúdo" abrangem as ações de provedores após pedidos com base na legislação nacional aplicável e a moderação com base nas diretrizes de comunidade.

Escolha da ação - Uma diversidade de soluções técnicas graduais oferece alternativas à remoção de conteúdos para garantir o maior respeito à proporcionalidade.

Garantias Processuais

Formatos - Os pedidos de restrições de conteúdo fornecem informações de apoio suficientes para a tomada de decisão, de acordo com formatos de apresentação claros.

Sensibilização - Os usuários têm acesso à informação sobre a inacessibilidade dos conteúdos e à justificativa para tal.

Sinalização - Canais fáceis de usar estão disponíveis para que os usuários sinalizem conteúdos que acreditam violar os padrões da comunidade do serviço.

Detecção - Uma combinação cuidadosa de detecção automatizada e análise humana permite uma ação oportuna, ao mesmo tempo em que considera totalmente o contexto para reduzir os riscos de restrições excessivas.

Notificação[4] - Os usuários são notificados antes da aplicação das decisões de restrição relativas ao seu conteúdo. Se ficar justificadamente demonstrado, de acordo com critérios claros e previamente acordados, que a notificação prévia não é exequível, aconselhável ou admissível, os usuários são rapidamente notificados após a execução de uma decisão de restrição. Algumas situações podem justificar uma exceção ao princípio geral da notificação do usuário.

Emergência - Disposições específicas estabelecem condições aplicáveis em situações justificáveis de emergência.

Recurso/remediação - Estão disponíveis mecanismos de recurso acessíveis, rápidos, claramente documentados e disponíveis ao público, com conteúdos que permanecem ativos sempre que possível durante o recurso.

4 As questões específicas relativas aos meios de comunicação e aos procedimentos e princípios de notificação aos meios de comunicação foram levantadas e merecem uma discussão especial.

Responsabilidade

Cadeia de decisão - Os critérios, procedimentos e as vias de encaminhamento do provedor de serviços relativos à restrição de conteúdos estão suficientemente documentados e disponíveis ao público.

Coerência - Os provedores de serviços utilizam critérios consistentes na aplicação das suas diretrizes de comunidade e no tratamento dos pedidos jurídicos, dedicando recursos adequados para tal.

Transparência - Relatórios periódicos detalhados, em formatos acessíveis e exportáveis, tanto das autoridades públicas quanto dos atores privados, conferem legitimidade e transparência aos mecanismos e às decisões de restrição de conteúdo.

Supervisão - O monitoramento contínuo permite a supervisão adequada das restrições de conteúdo para aumentar a confiança no devido processo e accountability.

CRITÉRIOS OPERACIONAIS

Os seguintes critérios representam os melhores esforços dos membros do Grupo de Contato do Programa Conteúdo e Jurisdição e seus Grupos de Trabalho, conforme compilados pelo Secretariado da I&J, na identificação de listas concisas de elementos que podem ser usados por todas as categorias de tomadores de decisão no desenvolvimento, avaliação e implementação de soluções. O objetivo é que todos os atores sejam capazes de discutir ideias, avaliar iniciativas e debater propostas usando arcabouços comuns de referência e questões estruturantes.

Os seguintes documentos devem ser entendidos como base para futura referência e trabalho da Rede de Políticas Internet & Jurisdição, após sua 3ª Conferência Global. Abaixo está a lista de Critérios Operacionais para o Programa Conteúdo e Jurisdição:

Parte I – Clareza da Estrutura

- CRITÉRIOS A - Tipologia do Conteúdo
- CRITÉRIOS B - Base Normativa

Parte II - Detecção

- CRITÉRIOS C - Avisos de Terceiros
- CRITÉRIOS D - Detecção de Provedores

Parte III - Medidas Proporcionais

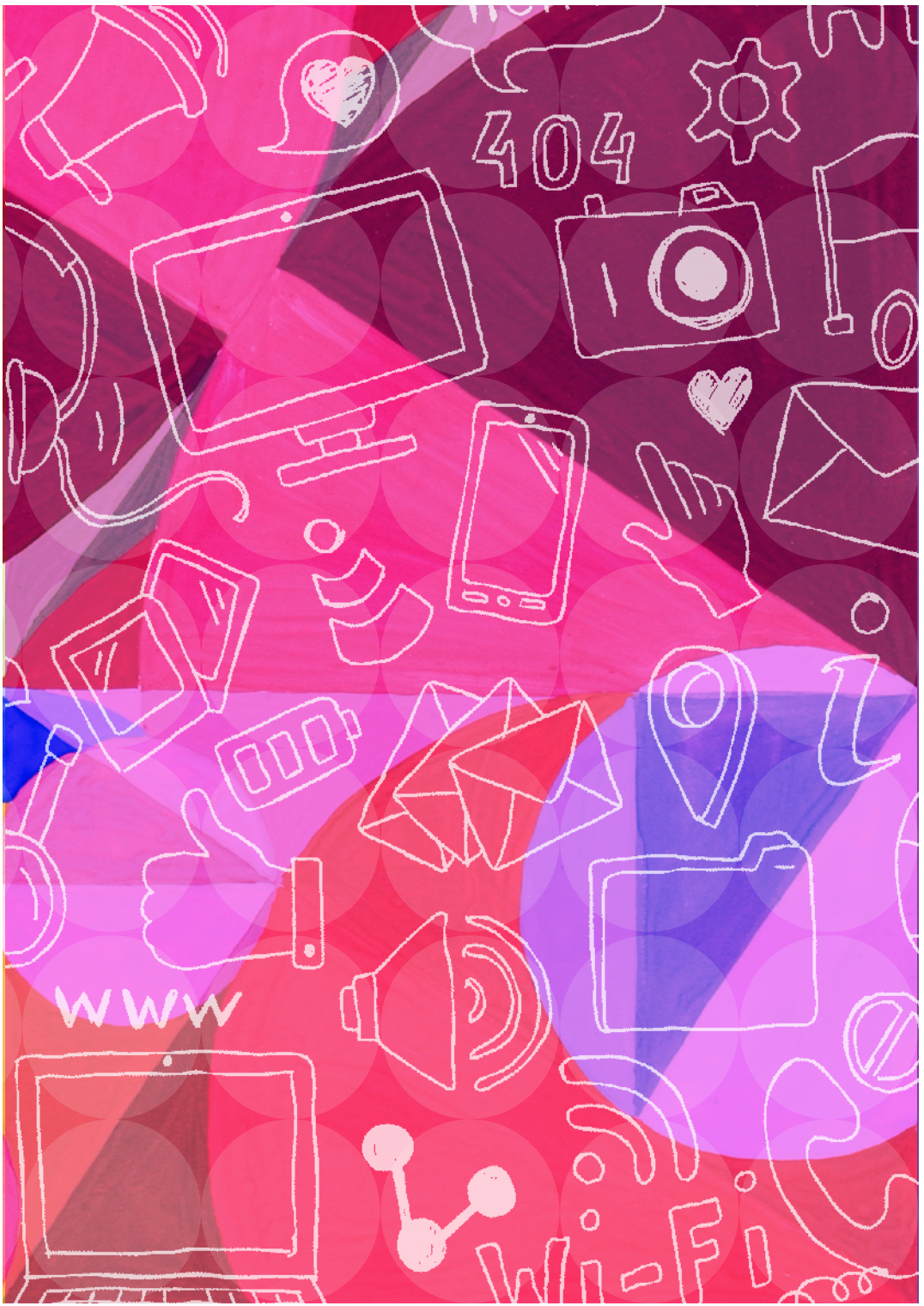
- CRITÉRIOS E - Tempestividade
- CRITÉRIOS F - Avaliação
- CRITÉRIOS G - Proporcionalidade Geográfica
- CRITÉRIOS H - Escolha da ação

Parte IV - Notificação / Recurso

- CRITÉRIOS I - Notificação ao Usuário
- CRITÉRIOS J - Recurso

Parte V - Escalabilidade

- CRITÉRIOS K - Capacidade de Pequenos Provedores / Países


404
www
Wi-Fi

PARTE I – CLAREZA DA ESTRUTURA

Critérios A - Tipologia do Conteúdo

Uma grande diversidade de tipos de conteúdos pode ser potencialmente ilegal em certos países ou representar um risco de danos aos usuários. A facilidade de acesso público e a propagação viral da expressão que antes era mantida em privado também geram novos desafios. Em um contexto de falta de definições internacionais suficientemente claras e acordadas, a tabela abaixo é uma tentativa não exaustiva (que pode estar sujeita a um maior aperfeiçoamento) de descrever as principais questões que estão em jogo, para ajudar todos os atores a desenvolver abordagens diversificadas e matizadas para cada tipo de desafio, no campo dos direitos humanos internacionais. Esta tabela *não* deve ser entendida como um índice normativo de conteúdo que *deve* ser restrito.

TIPOS DE CONTEÚDO	DESCRIÇÃO
DIREITOS DA CRIANÇA: ART. 24 PIDCP	
O artigo 24 estabelece que toda criança terá direito, sem qualquer discriminação de raça, cor, sexo, língua, religião, origem nacional ou social, situação econômica ou nascimento, às medidas de proteção que sua condição de menor requer por parte da sua família, da sociedade e do Estado. A Declaração dos Direitos da Criança declara que "a criança, em razão da sua imaturidade física e mental, necessita de salvaguardas e cuidados especiais...". A Convenção Internacional sobre os Direitos da Criança define crianças como indivíduos com menos de 18 anos de idade e o artigo 17 exige que os Estados-membros "incentivem a elaboração de diretrizes apropriadas à proteção da criança contra informações e materiais prejudiciais ao seu bem-estar, tendo em vista o disposto nos artigos 13 e 18". A Declaração Universal de Direitos Humanos proclama que a infância tem direito a cuidados e assistência especiais.	
MATERIAL QUE CONTENHA ABUSO INFANTIL OU ALGO CONDENÁVEL QUE ENVOLVA MENORES DE IDADE	Conteúdo que inclui conteúdo sexual ou sexualmente sugestivo envolvendo menores de idade, imagens de abuso infantil ou outro conteúdo publicado com a intenção de causar danos e tirar proveito de sua pouca idade. Pode incluir direitos à privacidade e à imagem para crianças entre 13 e 18 anos, dependendo da jurisdição e do contexto.
ALICIAMENTO OU CORRUPÇÃO DE MENORES	Aliciamento online é quando uma pessoa usa as mídias sociais para deliberadamente cultivar uma conexão emocional com uma criança com o intuito de abusar sexualmente ou explorar essa criança.

TIPOS DE CONTEÚDO	DESCRIÇÃO
DIREITO À PRIVACIDADE: ART. 17 PIDCP	
O artigo 17 protege o direito à privacidade, à família, ao lar e à correspondência, bem como à proteção da honra e da reputação. Declara que "ninguém poderá ser objeto de ingerências arbitrárias ou ilegais em sua vida privada, em sua família, em seu domicílio ou em sua correspondência, nem de ofensas ilegais à sua honra e reputação. Toda a pessoa tem direito à proteção da lei contra essas ingerências ou ofensas." Quaisquer restrições devem ser legais, necessárias e proporcionais. Ver também PIDCP/C/GC/161[1].	
VIOLAÇÕES DE INFORMAÇÕES PESSOAIS	Informações Pessoalmente Identificáveis (PII, na sigla em inglês), Informações Pessoais Sensíveis (SPI, na sigla em inglês), ou informações confidenciais divulgadas sem o consentimento da pessoa. As definições variam entre jurisdições, mas geralmente incluem qualquer informação que revele a identidade de uma pessoa. Também pode incluir conteúdo que facilite o roubo de identidade ao postar ou solicitar informações pessoais identificáveis, ao compartilhar informações pessoais através de link externo, ao compartilhar informações financeiras confidenciais sobre negócios, sobre si mesmo ou sobre terceiros, e compartilhar informações pessoais de contato. "Phishing", por exemplo, é o uso de e-mails ou mensagens de texto falsas ou sites que imitam os originais (copycat websites) para roubar PII.
CONTEÚDO PESSOAL DIFAMATÓRIO	Conteúdo que pode causar danos à dignidade, reputação ou direitos da personalidade. As plataformas geralmente não restringem este tipo de conteúdo, a menos que ele ultrapasse o limite da incitação ao ódio ou à violência. As plataformas pesquisadas restringem o conteúdo supostamente difamatório apenas quando ele tem a intenção de prejudicar. Os direitos individuais de ser protegido contra "ataques ilegais" à sua "honra e reputação" devem ser equilibrados com o direito à liberdade de expressão e opinião e o direito de acesso à informação do emissor. No entanto, o discurso ou opinião política, as críticas de funcionários públicos no exercício de suas funções ou o discurso que seja de interesse público, mesmo que seja considerado difamatório, receberão o mais alto nível de proteção sob o direito internacional. Dependendo do contexto e da intenção, o conteúdo difamatório pode ser sujeito a restrições legítimas ao abrigo do art. 19(a), por respeito aos direitos ou à reputação de outros.
TENTATIVAS DE DIFAMAÇÃO COORDENADAS/ ORGANIZADAS	O conteúdo difamatório é coordenado quando um indivíduo ou grupo organizado espalha o conteúdo contestado simultaneamente em várias plataformas.
SUGESTÕES DE "AUTOCOMPLETAR" DIFAMATÓRIAS OU RESULTADOS DE BUSCA QUE APONTEM PARA CONTEÚDOS DIFAMATÓRIOS ("GOOGLE BOMBING", "GOOGLEWASHING")	Estes termos se referem à prática de elevar artificialmente uma determinada página da web nos resultados de busca, ligando-o a um termo de pesquisa que pode ser depreciativo ou difamatório. As motivações podem ser pessoais, políticas, ou ser apenas um trote.

1 PIDCP/C/GC/16: <https://www.refworld.org/docid/453883f922.html>

"DIREITO AO ESQUECIMENTO"	Estas reivindicações envolvem pedidos de exclusão de informações que deixaram de ser pertinentes devido à passagem do tempo e à mudança de circunstâncias, e a acessibilidade contínua da informação constitui uma violação aos direitos de reputação.
USURPAÇÃO (CONTAS/ PERFIS/PÁGINAS FALSOS)	Copiar o layout de um usuário, usar um nome de usuário semelhante ou posar como outra pessoa em perfis, páginas, comentários, e-mails ou vídeos. Muitas vezes isso é feito com a intenção de prejudicar um indivíduo ou enganar os visualizadores. Também inclui bots ou outras aplicações para propaganda. Inclui a usurpação de um canal (por ex., Youtube), de um indivíduo (por ex., Facebook ou Twitter) ou de uma empresa/corporação. A personificação para fins satírico ou artístico seria protegida.
"DEEP FAKES"	Foi descrito pelo Governo do Reino Unido como "áudio e vídeos que parecem e soam como uma pessoa real, dizendo algo que essa pessoa nunca disse". Dependendo do contexto e da intenção, bem como da jurisdição (p. ex., a Primeira Emenda dos EUA) esse conteúdo pode ser protegido.
OBJETIFICAÇÃO SEXUAL	Conteúdo que objetifica seus alvos, inclusive por meio de fotografias manipuladas e descrições sexualmente explícitas de seus corpos. As fotografias são frequentemente utilizadas sem consentimento e manipuladas para que apareçam em cenas pornográficas ou usadas em memes.
DISSEMINAÇÃO NÃO AUTORIZADA DE IMAGENS ÍNTIMAS ("PORNOGRAFIA DE VINGANÇA")	Distribuição de imagens sexualmente explícitas sem o consentimento do sujeito das imagens. O abusador obtém imagens ou vídeos no decurso de uma relação anterior, ou invade o computador, contas de redes sociais ou telefone da vítima. Normalmente isso é feito com o objetivo de assediar, humilhar e ferir a pessoa.

TIPOS DE CONTEÚDO	DESCRIÇÃO
DIREITO À LIBERDADE DE EXPRESSÃO: ART. 19 PIDCP	
Art. 19 (1): Direito a expressar opiniões sem interferência. Artigo 19(2): Toda pessoa tem direito à liberdade de expressão; este direito compreende a liberdade de procurar, receber e divulgar informações e ideias de toda a índole, sem consideração de fronteiras, oralmente, de forma impressa ou artística ou por qualquer outro processo que escolher. O Comentário Geral 34 (PIDCP/C/GC/34[2]) também destaca como os Estados-membros devem ser proativos na implementação de "medidas eficazes de proteção contra ataques destinados a silenciar aqueles que exercem seu direito à liberdade de expressão" (parágrafo 23).	
DESINFORMAÇÃO	Desinformação inclui a distribuição de informações falsas ou imprecisas (ou seja, "fake news") para ganhos políticos, ideológicos ou econômicos, seja por indivíduos ou bots. Os exemplos extremos visam a influenciar as eleições e perturbar os processos democráticos. Pode assumir a forma de "notícias" baseadas parcialmente em fatos e desinformações, tuítes, postagens ou comentários. Este tipo de conteúdo muitas vezes não atravessa fronteiras jurídicas e deve ser cuidadosamente distinguido das opiniões e sátiras que são formas de expressão protegidas.
DESINFORMAÇÃO MÉDICA	Conteúdo que divulgue informações falsas ou enganosas que possam ter efeitos prejudiciais à saúde e à segurança individual ou pública. Exemplos incluem a promoção de falsas curas para doenças e conselhos contrários à vacinação. Pode ser feito para obter ganhos financeiros ou simplesmente por ignorância, e não com a intenção de prejudicar. Este tipo de conteúdo tem sido sujeito a restrições nos casos em que foi considerado uma ameaça à saúde pública.
CONTEÚDO SEXUALMENTE EXPLÍCITO; NUDEZ OU PORNOGRAFIA	Imagens de atividade sexual explícita ou fetiches e pessoas nuas ou parcialmente nuas em poses sexualmente sugestivas. Este tipo de conteúdo pode ser protegido para adultos, dependendo da jurisdição ou das diretrizes de comunidade, mas é restrito para crianças ou jovens. A nudez artística, científica, documental ou educativa está protegida. Imagens que identificam um indivíduo e são publicadas sem o seu consentimento podem estar sujeitas a restrições.
CONTEÚDO CRÍTICO A RELIGIÃO (BLASFÊMIA/ APOSTASIA)	Conteúdos críticos à religião, incluindo opiniões ou obras artísticas (como caricaturas satíricas) estão protegidos pelo art. 19 do PIDCP, mas ele deve ser equilibrado com restrições legítimas ao abrigo do art. 18 (3) (A liberdade de manifestar sua religião ou crença pode estar sujeita apenas às limitações previstas na lei e que são necessárias para proteger a segurança, ordem, saúde ou moral públicas ou os direitos e liberdades fundamentais de terceiros) e pelo art. 20, caso promova o ódio religioso, o que constitui incitação à discriminação, hostilidade ou violência. Alguns Estados restringem este tipo de conteúdo sob leis de blasfêmia/apostasia. As leis da blasfêmia, que restringem o discurso considerado ofensivo a profetas ou líderes religiosos, são muitas vezes arcaicas e excessivamente abrangentes e abusivas. Em particular, elas são usadas para punir minorias religiosas ou mulheres (por ex. assassinatos em nome da honra) em países religiosos conservadores. Apesar dos esforços internacionais para revogar essas leis, elas permanecem em vigor em dezenas de Estados e 13 Estados ainda promulgam sentenças de morte pela ofensa.

2 PIDCP/C/GC/11: <https://www.ohchr.org/Documents/Issues/Opinion/CCPRGeneralCommentNo11.pdf>

TIPOS DE CONTEÚDO	DESCRIÇÃO
Art. 19(a): Restrição legítima por respeito aos direitos ou reputações de outros. O Comentário Geral 34 (PIDCP/C/CG/34 parágrafo 35)[3] salienta que "Quando um Estado-membro invoca um motivo legítimo de restrição à liberdade de expressão, deve demonstrar de forma específica e individualizada a natureza exata da ameaça e a necessidade e proporcionalidade da ação específica tomada, nomeadamente estabelecendo uma ligação direta e imediata entre a expressão e a ameaça".	
CONTEÚDO PESSOAL DIFAMATÓRIO	Ver Conteúdo Pessoal Difamatório em Direito à Privacidade (p. 21). O Comentário Geral 342 convida os Estados-membros a "considerar a descriminalização da difamação" e recomenda que, em qualquer caso de difamação, "a prisão nunca é uma pena apropriada" (parágrafo 47).
BULLYING	Conteúdo que se destina propositadamente a indivíduos com a intenção de degradá-los ou envergonhá-los. A forma extrema de bullying é chamada "flaming". O bullying não se aplica a figuras públicas de quem se espera níveis mais elevados de tolerância a críticas dentro do limite do razoável, na medida em que tais críticas não incluam discursos de ódio ou ameaças críveis.
ASSÉDIO	Conteúdo disseminado em múltiplas ocasiões para causar estresse individual, humilhação, ansiedade ou medo de violência. O conteúdo pode conter xingamentos direcionados, comentários grosseiros e ofensivos, ameaças de danos físicos ou até mesmo de morte. Dependendo da intenção e contexto, apenas o discurso considerado incitação ao ódio ou uma ameaça crível pode sofrer restrição. Muitos Estados têm estatutos contra assédio que são aplicáveis a violações online.
DANOS COORDENADOS/ ORGANIZADOS	Sabotar ou invadir deliberadamente vários espaços online com o propósito de assediar um alvo. Atualmente, os usuários não podem relatar esse escopo e o contexto do assédio, pois cada plataforma só considera o assédio que acontece em seus próprios sites.
PERSEGUIÇÃO ONLINE (CYBERSTALKING)	Não existe nenhuma definição legal, mas os exemplos incluem o envio repetido de e-mails ou mensagens de texto ameaçadoras ou obscenas, envio de spams, “flaming” (abuso verbal online direcionado), e “baiting” através do envio de mensagens contendo insultos ou ameaças.
DEADNAMING	Usar/divulgar o nome de nascimento de uma pessoa transgênero para assediar, invalidar a sua identidade e/ou infligir stress emocional.
DOXING	Procurar e publicar informações privadas ou identificar informações sobre um indivíduo em particular, muitas vezes através de hackeamento e com intenção maliciosa. "Dox" é uma gíria para "documentos". O objetivo do doxing é provocar medo, estresse e pânico, mesmo quando os agressores julgam ou dizem que é "inofensivo".

3 PIDCP/C/GC/34: <https://bangkok.ohchr.org/programme/documents/general-comment-34.aspx>

TIPOS DE CONTEÚDO	DESCRIÇÃO
Art. 19 (3)(b): Restrição legítima para proteção da segurança nacional ou da ordem pública (ordre public), ou da saúde ou moral públicas, quando em conformidade com rigorosos testes de necessidade e proporcionalidade. Ver PIDCP/C/GC/34[4] .	
CONTEÚDO VIOLENTO/ EXPLÍCITO	Conteúdo sensacionalista ou gratuitamente violento ou que glorifica a violência. Deve ser distinguido de conteúdos explícitos que podem ter fins educativos, científicos ou de interesse público, tais como informações sobre acontecimentos históricos ou atuais, que seriam protegidas pelo direito internacional dos direitos humanos. Dependendo do tipo de conteúdo, pode exigir verificação de idade ou conter restrições de idade.
PROMOVER OU DIVULGAR O CRIME	Conteúdo que incite ou estimule atividades criminosas e que se acredite ser uma ameaça crível à segurança pessoal, pública ou à propriedade.
CONTEÚDO PARA ORGANIZAR ATOS VIOLENTOS OU APOIAR ORGANIZAÇÕES VIOLENTAS	Conteúdo que faça ameaças críveis de danos físicos graves (violência organizada, assassinato, tráfico de pessoas) contra um indivíduo específico ou grupo definido de indivíduos ou que expresse apoio ou louvor a grupos, líderes ou indivíduos envolvidos nessas atividades.
VIOLÊNCIA E EXPLORAÇÃO SEXUAL	Conteúdo que retrate, ameace ou promova violência, agressão ou exploração sexual.
INCITAÇÃO À AUTOMUTILAÇÃO OU SUICÍDIO	Conteúdo que promova comportamentos prejudiciais, ou que encoraje ou sugira autolesão, como mutilação, transtornos alimentares ou uso de drogas. Conteúdo que identifique e vise negativamente vítimas ou sobreviventes de automutilação ou suicídio.
VAZAMENTO DE INFORMAÇÕES CONFIDENCIAIS OU SECRETAS	Alguns Estados podem justificar a restrição a informações sensíveis divulgadas por motivos de segurança nacional. No entanto, as informações de interesse público que são divulgadas pelos "denunciantes" podem ser protegidas ao abrigo da Convenção das Nações Unidas contra a Corrupção. O art. 33 recomenda que os Estados ofereçam proteção aos “denunciantes", que relatam "de boa fé e com motivos razoáveis, às autoridades competentes quaisquer feitos relacionados com os delitos" abrangidos pela Convenção. O art. 32 oferece proteção às testemunhas, peritos e vítimas.
LESA-MAJESTADE (LÈSE-MAJESTÉ) OU COMENTÁRIOS CRÍTICOS DE PERSONAGENS HISTÓRICOS	Algumas jurisdições restringem o discurso considerado ofensivo à monarquia ou a personagens históricos com o argumento de que se trata de traição ou ameaça à ordem pública. No entanto, a discussão aberta e crítica de líderes políticos e figuras públicas é protegida pelo direito internacional. Só ameaças críveis de incitação podem justificar restrições.

4 PIDCP/C/GC/11: <https://www.ohchr.org/Documents/Issues/Opinion/CCPRGeneralCommentNo11.pdf>

TIPOS DE CONTEÚDO	DESCRIÇÃO
PROIBIÇÃO DA PROPAGANDA A FAVOR DA GUERRA E DE INCITAÇÃO AO ÓDIO NACIONAL, RACIAL OU RELIGIOSO: ART. 20	
Art. 20(2) A apologia ao ódio nacional, racial ou religioso que constitui incitação à discriminação, à hostilidade ou à violência serão proibidas por lei.	
DISCURSO DE ÓDIO	A incitação ao ódio inclui ataques graves a pessoas com base em sua raça, etnia, nacionalidade, casta, religião, identidade de gênero, orientação sexual, deficiência, condição de veterano ou condição médica. Pode também incluir pessoas com base na idade, peso, imigração ou condição de veterano. Exemplos disso são discursos violentos ou desumanizadores, declarações de inferioridade ou apelos à exclusão ou segregação. Também pode incluir imagens, como de linchamento, ou conduta coordenada para discriminar ou desumanizar. A transmissão ao vivo ou a publicação de vídeos de eventos ao vivo que amplificam ou incitam a crimes de ódio pode exigir restrições imediatas (por ex. o Massacre de Christchurch). Artigos 18, 19, 20 e 26 do Pacto Internacional sobre os Direitos Civis e Políticos (PIDCP). Convenção Internacional sobre a Eliminação de Todas as Formas de Discriminação Racial (ICERD, na sigla em inglês), art. 4º. Embora não haja uma definição ou limiar internacionalmente acordados para o discurso de ódio, os Estados têm a obrigação, nos termos do PIDCP, de proibir a defesa do ódio nacional, racial ou religioso que constitua uma incitação à discriminação, à hostilidade ou à violência. Esta garantia está relacionada à garantia de proteção equitativa perante e pela lei. A avaliação dos discursos de ódio pode ser muito subjetiva e, por conseguinte, é necessário ter muito cuidado, uma vez que restrições demasiado amplas podem violar outros direitos fundamentais. Ver também PIDCP/C/GC/113 e o Plano de Ação de Rabat.
CONTEÚDO EXTREMISTA VIOLENTO	A maioria das plataformas proíbe conteúdos que definem como "extremistas". As definições incluem conteúdos que "incitam" a violência, "celebram" atos terroristas, "instruem", solicitam ou defendem pessoas ou grupos de pessoas a participarem de atividades de um grupo terrorista ou fornecem instruções sobre a fabricação ou o uso de armas. Algumas plataformas negam contas a organizações rotuladas como terroristas ou que se envolvam em atividades violentas premeditadas contra pessoas ou bens como um ato de intimidação com um propósito político, religioso ou ideológico. Isto inclui boatos terroristas. O PIDCP art. 20 proíbe qualquer propaganda em favor da guerra. No entanto, quaisquer restrições devem excluir expressamente os conteúdos divulgados para "fins educativos, jornalísticos, artísticos ou investigativos ou atividades de sensibilização contra o terrorismo". Os conteúdos assinalados como "terroristas" podem, em alguns casos, constituir documentação de crimes de guerra ou atrocidades, motivo pelo qual não devem ser eliminados, mas sim compartilhados com as autoridades policiais competentes. Embora o art. 19 (3)(b) preveja uma restrição legítima para a proteção da segurança nacional, não existe uma definição acordada para conteúdo terrorista ao abrigo do direito internacional e, para tal efeito, as definições de conteúdo terrorista devem ser "claras, previsíveis e limitadas, a fim de evitar interferências ilícitas nos direitos fundamentais". Ver também Art. 6º PIDCP (Direito à Vida); Instrumentos Internacionais (ONU)[5].

5 Art. 6 - International Legal Instruments: <https://www.un.org/counterterrorism/ctitf/en/international-legal-instruments>

TIPOS DE CONTEÚDO	DESCRIÇÃO
DIREITOS DE PROPRIEDADE INTELECTUAL	
DIREITO AUTORAL	Direito autoral é um direito legal que protege obras criativas originais, como música, filmes, obras de arte ou livros. Não protege fatos ou ideias.
MARCA REGISTRADA	Uma marca registrada é uma palavra, frase, símbolo e/ou desenho (por ex. logotipos, nomes de marcas) utilizado para identificar um produto/serviço e distinguir a origem de um produto/serviço de outros similares. Ao contrário de alguns direitos autorais, as marcas registradas não expiram.

BENS E SERVIÇOS REGULAMENTADOS	
Os conteúdos relativos a bens e serviços regulamentados ou ilegais variam dependendo da jurisdição.	
BENS E SERVIÇOS REGULAMENTADOS	Os Estados e as plataformas restringem os conteúdos que facilitam a compra, o comércio ou a venda de drogas ilegais, serviços ilegais (jogos de azar online, documentos falsos), mercadorias roubadas, armas de fogo ou outras armas, com base na legislação vigente na jurisdição. Alguns Estados ou plataformas também podem restringir conteúdos que promovam o uso de drogas ou armas ilegais ou que forneçam instruções para fabricação de armas (por ex. impressão 3D).
INCITAÇÃO SEXUAL	Conteúdo divulgado com a intenção de envolver em atividade sexual por uma taxa ou o equivalente funcional a uma taxa.

TIPOS DE CONTEÚDO	DESCRIÇÃO
FRAUDE	
O conteúdo fraudulento procura enganar deliberadamente os indivíduos para obter ganhos ilícitos ou privá-los dos seus direitos. A maioria das jurisdições abarca atividades fraudulentas nos seus estatutos civis ou penais.	
METADADOS ENGANOSOS (TÍTULO, DESCRIÇÃO, MARCADORES, ANOTAÇÕES E MINIATURAS)	Inclui títulos, descrições, marcadores, anotações e miniaturas usadas para manipular ou enganar os algoritmos em pesquisa de vídeo online, em vez de ser representativo do conteúdo real do vídeo.
CHANTAGEM/EXTORSÃO	Conteúdo ou mensagens que ameaçam revelar informações ou fotos embaraçosas da vítima (que podem ter sido colhidas ilegalmente ou com o consentimento da vítima), a menos que a vítima forneça favores, bens ou dinheiro. "Sextorsão" é uma forma de chantagem em que informações ou imagens sexuais são usadas para extorquir favores sexuais, dinheiro, entre outros, da vítima.
GOLPES: ENGANAR OS OUTROS PARA SEU PRÓPRIO GANHO FINANCEIRO	Conteúdo que tenta deliberadamente enganar os usuários para obter ganhos financeiros ou acessar PII. Exemplos incluem a compra de visualizações, layouts enganosos, assinaturas artificiais, distribuição de pop-unders e redirecionamentos, manipulação de votos (para aumentar/diminuir) ou falsificação de logotipos de marcas.
SPAM	Conteúdo direcionado, indesejado ou repetitivo em vídeos, comentários, mensagens privadas ou redirecionamentos fora do domínio. Pode ter a intenção de aumentar artificialmente as visualizações ou diminuir as pontuações e outras métricas através de campanhas coordenadas (ou seja, equipes de trollagem). Também pode incluir conteúdo ou comportamento enganoso, como elementos de design enganosos ou pop-ups suspeitos.
SPAM DE TRÁFEGO ARTIFICIAL: INCENTIVA ARTIFICIALMENTE OS TELESPECTADORES AO ENGAJAMENTO	Mensagens direcionadas para incentivar as visualizações, chamadas de "manipulação de contagem de visualizações", que tentam transformar uma não visualização em uma visualização para obter ganho financeiro.
CONTAS FRAUDULENTAS	Contas geridas por bots em vez de humanos com a intenção de espalhar desinformação e distorcer o debate. Existe alguma sobreposição com "Desinformação" e "Personificação"/"Usurpação".

Critérios B - Base Normativa

Um desafio importante na elaboração e aplicação da legislação nacional, bem como das diretrizes de comunidade para as empresas[5], é a necessidade de conciliar direitos concorrentes, nomeadamente a liberdade de expressão e a prevenção de danos.

1. Reconciliação de diversas bases normativas

A pluralidade de fontes forma uma paisagem normativa cada vez mais elaborada, combinando:

a. Princípios gerais de direitos humanos internacionais ou regionais, em particular:
   i. A Declaração Universal dos Direitos Humanos (DUDH);
   ii. O Pacto Internacional sobre os Direitos Civis e Políticos (PIDCP), em especial os artigos 6º; 17, 18, 19, 20, 24, 26.
   iii. A Convenção Internacional sobre a Eliminação de Todas as Formas de Discriminação Racial (ICERD)
   iv. A Declaração dos Direitos da Criança
b. A diversidade de leis nacionais e regionais aplicáveis, existentes[6] ou recentemente elaboradas para o contexto digital devido às crescentes preocupações com conteúdos abusivos online.
c. A crescente importância dos Termos de Serviço (ToS) e das Diretrizes de Comunidade das empresas.

2. Consistência normativa internacional

As seguintes categorias podem ser utilizadas para determinar o grau de convergência normativa internacional sobre as diversas questões:

a. EXISTE um consenso universal de que o conteúdo/comportamento é ilegal E existe uma forte convergência material em todo o mundo sobre os critérios de limiar correspondentes (exemplo: material contendo abuso sexual de crianças);
b. EXISTE um consenso universal de que o conteúdo/comportamento é ilegal, MAS existem variações nacionais significativas nos critérios que determinam a ilegalidade (exemplo: difamação);
c. O conteúdo/comportamento NÃO É universalmente considerado ilegal, MAS a aplicação de leis internas específicas no território local

5 Foi salientado que o objetivo principal e fundamental dos Termos de Serviço (ToS, na sigla em inglês) e das Diretrizes de Comunidade das empresas é manter a natureza e os benefícios do serviço para a comunidade de usuários.

6 Isso pode incluir leis relevantes relacionadas à mídia, conforme aplicável.

é considerada aceitável por outros países, em particular por razões históricas (exemplo: criminalização da negação do Holocausto);

d. O conteúdo/comportamento NÃO É universalmente considerado censurável E alguns países até consideram que não deve ser permitido torná-lo ilegal (exemplo: leis que discriminam ou criminalizam certas orientações sexuais).

No entanto, as fronteiras entre estas diferentes categorias não são rígidas. Existem debates sobre onde alguns tópicos se inserem.

3. Tipos de regulação

Alguns provedores objetivam diretrizes de comunidade tão uniformes quanto possível para todos os seus usuários. Isto produz uma harmonização global de fato das regras aplicáveis nos seus respectivos espaços. Outros, no entanto, dependem da moderação orientada pela comunidade, por exemplo, organizada por tópico (Reddit) ou por idioma (Wikipedia).

Alguns provedores privados começaram a elaborar regras para novas questões, por exemplo, a publicação não consensual de conteúdos adultos (também conhecida por "pornografia de vingança"), com o consequente aparecimento de algumas iniciativas legislativas.

Poder-se-ia contemplar um quadro conceitual que permitisse distinguir mais claramente entre:

a. Regulação/moderação EM uma plataforma: sob a responsabilidade dos administradores dos subfóruns e grupos, as regras do grupo podem ser mais restritivas do que as regras da plataforma global.

b. Regulação PELA plataforma: As diretrizes de comunidade e as regras de decisão estabelecem o arcabouço geral para todos os conteúdos no espaço correspondente, incluindo, potencialmente, a latitude dada aos administradores de grupo.

c. Regulação DAS plataformas: leis nacionais, legislação regional ou acordos internacionais que definem as obrigações gerais dos provedores em termos de moderação de conteúdo, incluindo a forma de conciliar sua capacidade comercial para determinar seus ToS e as obrigações que podem resultar de uma abrangente posição de mercado.

Critérios C - Avisos de Terceiros

1. Emitidos por autoridades públicas:

a. Ordens formais com base em leis nacionais. No entanto, devido a limitações de volume e conveniência dos prazos para a ação, isto é por vezes feito sem a validação por um tribunal local que poderia estabelecer claramente a ilegalidade do conteúdo com todas as garantias processuais adequadas. Isto confere às entidades privadas a responsabilidade de determinar a legalidade ou não, com incentivos para restringir excessivamente os conteúdos em situações de incerteza. Podem ser desenvolvidos procedimentos adicionais (com proteções adequadas) para uma avaliação interna célere.

b. Pedidos mais informais com base nos ToS ou nas diretrizes de comunidade, por exemplo, através das chamadas unidades de consulta na Internet. São necessários procedimentos mais claros para garantir a transparência e a accountability no que tange à utilização desse canal pelas autoridades públicas.

2. Os avisos privados podem vir de:

a. Notificadores especializados, por exemplo, em direitos de autor ou material de abuso infantil. No entanto, é necessária uma maior clareza no que tange, principalmente, aos seus procedimentos, critérios de tomada de decisão, requisitos de diligência e vias de recurso para que as notificações possam ser feitas à *prima facie*.

b. Os meios de comunicação social, nomeadamente para efeitos de verificação de fatos (por exemplo, durante períodos eleitorais) ou de denúncia de ciberassédio contra jornalistas visados em função das suas atividades profissionais.

c. Sinalizadores individuais (incluindo "sinalizadores confiáveis") através de ferramentas da plataforma. O papel das denúncias de usuários deve ser visto em paralelo com o papel crescente dos meios de detecção automatizados para os meios de identificação e eliminação de conteúdos violentos. No entanto, continuam a ser necessárias ferramentas de sinalização fáceis de utilizar.

Critérios D - Detecção pelos provedores

Em resposta à pressão, os principais provedores implementam cada vez mais a detecção proativa e isso só pode ser feito através do uso intensivo de ferramentas algorítmicas, incluindo a Inteligência Artificial. A utilização de bases de dados *hash* para impedir o recarregamento de conteúdos anteriormente detectados como justificativa para a restrição de conteúdos ilegais já detectados também está sendo disseminada.

O desempenho de tais ferramentas, no entanto, varia fortemente de acordo com os diferentes tipos de conteúdo problemático: para imagens com elementos facilmente reconhecíveis, o desempenho das ferramentas é bom, ao passo que permanece muito menos preciso para qualquer conteúdo que exija uma melhor avaliação do contexto.

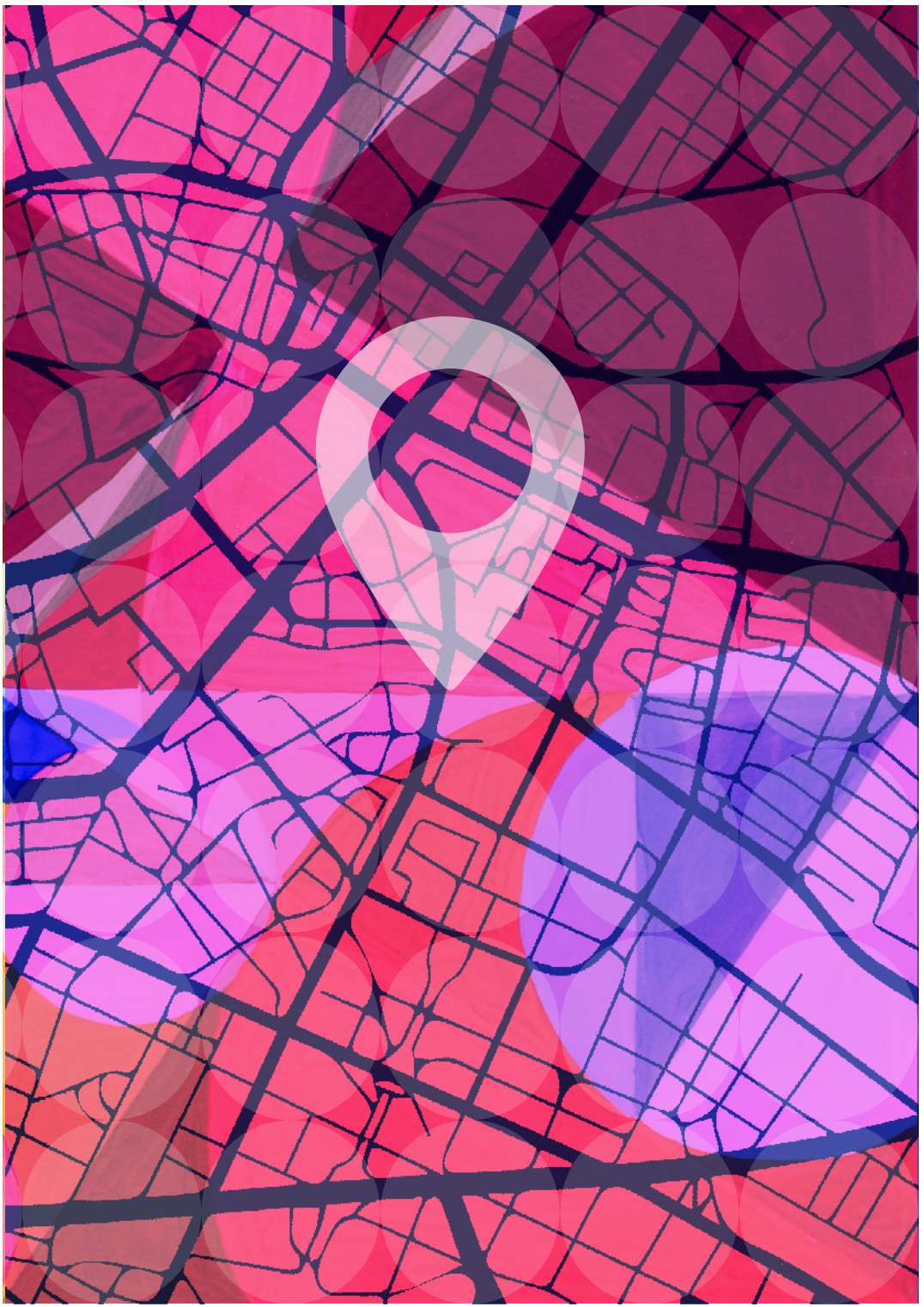
Apesar dos progressos significativos, os principais desafios devem ser enfrentados, uma vez que as ferramentas automatizadas:

1. Ainda não têm a precisão necessária para detectar todo o conteúdo infrator ou identificar corretamente o conteúdo questionável, correndo-se o risco de se aplicar medidas restritivas insuficientes ou excessivas.
2. Ignoram amplamente considerações contextuais, incluindo contexto externo, cultura e intenção.
3. Tomam decisões de risco sem um equilíbrio adequado entre interesses concorrentes, ignorando regulamentos legais, interpretações legais, nuances na plataforma ToS, etc.
4. Levantam sérias questões de transparência: a remoção ou restrição automatizada pode fornecer informações insuficientes sobre a sua fundamentação, dificultando a compreensão da decisão de restrição ou a sua contestação.
5. Ainda podem ser enganadas através de meios técnicos, por exemplo, mediante a alteração de metadados ou criptografia de conteúdo, permitindo assim que certos conteúdos nocivos permaneçam online ou sejam viralizados ainda mais através de canais criptografados.
6. Pode exibir vieses não detectados devido aos conjuntos de dados nos quais foram treinados.

A análise humana continua sendo necessária no processo de tomada de decisões sobre restrições individuais e é necessário um esforço de colaboração significativo, de um modo mais geral, para permitir avaliação e supervisão adequadas dos instrumentos algorítmicos.

A seguinte Tipologia de Modalidades de Detecção é uma lista de ações reconhecidas disponíveis aos provedores de serviços e intermediários de rede/hospedagem para identificar conteúdo supostamente nocivo ou ilegal. Esta lista foi desenvolvida para ilustrar e mapear um espectro de respostas possíveis e não se destina a apoiar quaisquer ações específicas.

AÇÕES	DESCRIÇÃO/FERRAMENTAS TÉCNICAS
PLATAFORMA/PROVEDOR DE CONTEÚDO E MOTORES DE BUSCA	
AUTENTICAÇÃO/ VERIFICAÇÃO DE CONTA	A autenticação destina-se a assegurar que a pessoa é quem afirma ser e a verificar os dados de identidade. Pode incluir a confirmação do endereço de e-mail, a data em que a conta foi criada, se o perfil está completo, etc. A autenticação refere-se mais a um processo interno, ao passo que a verificação se refere a dados externos.
MONITORAMENTO DE CONTEÚDO	O monitoramento de conteúdo envolve o processo de implementação de procedimentos e filtros para identificar conteúdo ou comportamentos online que possam violar os ToS, as Diretrizes da Comunidade ou as leis locais. Alguns monitoramentos são conduzidos por humanos, mas grande parte deles é feita automaticamente através de algoritmos ou Inteligência Artificial. Isso pode incluir a avaliação do comportamento dos usuários (por exemplo, quem eles seguem ou o que eles compartilham), de que maneira outras contas interagem com eles (por exemplo, quem silencia, segue, compartilha ou bloqueia o sujeito), ou se há ações coordenadas tomadas por grupos ou entre plataformas com a intenção de causar danos. Uma vez que forem identificados conteúdos/comportamentos potencialmente prejudiciais, estes podem ser assinalados para análise.
HASHING (E BANCOS DE DADOS DE HASH)	Esta tecnologia cria uma assinatura digital única (ou "hash") de uma imagem ou vídeo, que pode então ser comparada com hashes de outras fotos ou vídeos. Isso pode ajudar a detectar e remover ou impedir o upload de uma nova imagem ou vídeo se seu hash corresponder ao hash armazenado em um banco de dados de itens previamente identificados como restrições justificadas. As bases de dados de hash têm sido utilizadas, por exemplo, em relação a material de abuso sexual de crianças, extremismo violento, divulgação não autorizada de imagens íntimas ("pornografia de vingança") ou direitos autorais.
NOTIFICAÇÃO E RETIRADA: REMOÇÃO TEMPORÁRIA OU PERMANENTE	Mecanismo pelo qual um indivíduo pode emitir um pedido legal para um provedor de conteúdo, exigindo que remova, exclua ou restrinja o acesso a conteúdo supostamente nocivo. Exemplos incluem as políticas do "Direito ao Esquecimento" da UE e o regime de notificação e retirada de direitos de autor do Digital Millennium Copyright Act, dos Estados Unidos.
INTERMEDIÁRIOS DE REDE/HOSPEDAGEM	
NOTIFICAÇÃO E RETIRADA: REMOÇÃO TEMPORÁRIA OU PERMANENTE	Os intermediários de hospedagem podem tornar o conteúdo offline, com base nas políticas e procedimentos da empresa, ordens judiciais ou regulamentos estatais.



Critérios E - Tempestividade

Os recentes esforços legislativos têm colocado ênfase cada vez maior nos tempos de resposta curtos1 para eliminar tipos específicos de conteúdos, em especial no que diz respeito ao terrorismo e ao extremismo violento.

1. Tensões

a. O tempo de resposta pode ser medido por referência a diferentes eventos operacionais, incluindo: tempo de upload, notificação à plataforma ou notificação ao usuário. Qualquer regra que estabeleça um prazo de resposta obrigatório deve ser clara.
b. A tensão entre tempos de resposta curtos, a precisão da medida e a necessidade de garantir a proteção dos direitos pode ser resumida nas declarações a seguir:
   i. Algumas decisões sobre restrições de conteúdo precisam ser tomadas rapidamente para evitar danos;
   ii. Quanto mais rápida for a decisão, tanto maior será o risco de erros ou imprecisões nas decisões de restrição ou o seu impacto nos direitos dos usuários;
   iii. Garantir a exatidão da decisão e o pleno respeito aos direitos e interesses dos usuários exige uma avaliação cuidadosa e, por conseguinte, tempo.

2. Fundamentação para apoiar decisões rápidas

Há uma série de razões para incentivar decisões rápidas:

a. Incentivos normativos, incluindo o respeito às legislações nacionais, a limitação da responsabilidade legal do provedor de serviços e a perspectiva de multas.
b. Incentivos econômicos, incluindo o volume de conteúdos e pedidos a serem considerados (em termos de recursos), a satisfação dos usuários e de outras partes interessadas (como os anunciantes).
c. Considerações operacionais, incluindo a natureza e o volume dos conteúdos e dos pedidos de restrição, a distinção entre casos óbvios e casos mais graves e a consideração dos danos causados por restrições versus danos causados por manter os conteúdos acessíveis.

d. Considerações de interesse, incluindo para quem as razões para as restrições são mais prementes: o respeito pelas leis nacionais, ou segurança nacional, pode ser mais premente como um interesse para os governos do que para os usuários.

3. Riscos potenciais de decisões rápidas

a. Tomada de decisão incorreta:
   i. Falsos positivos, levando a restrições excessivas. Estes incluem conteúdos infratores incorretamente identificados com base em valores concorrentes (por exemplo, nudez artística vs. regras contra nudez), análise contextual (ou seja, situações externas em que não há ofensa de determinados conteúdos, por exemplo, amamentação), erros analíticos (ou seja, o conteúdo foi incorretamente identificado).
   ii. Falsos negativos, fazendo com que o conteúdo permaneça indevidamente acessível, materializando assim danos, em contrapartida aos falsos positivos.
b. Equidade processual:
   i. Capacidade limitada dos usuários para contestar uma decisão antes da entrada em vigor da restrição. A capacidade de recorrer *ex ante* é urgente em termos de tempo. Estes riscos diferem em função do tipo de conteúdo e dos danos conexos.
   ii. Transparência limitada para contestar decisões de restrição antes ou depois de terem sido tomadas, quando são utilizados sistemas de detecção automatizados e se verifica uma falta de informação sobre o processo de detecção ou a causa da restrição.
c. Danos materiais: riscos em função dos danos que decisões demasiado rápidas podem produzir, por exemplo:
   i. Sobre os direitos fundamentais, como a liberdade de expressão ou a privacidade.
   ii. Sobre os interesses dos usuários no correto funcionamento da plataforma, tais como colaboração e discussão.
   iii. Sobre interesses públicos maiores, como a democracia e o debate público.
d. Diferentes tipos de conteúdo (por exemplo, material de pornografia infantil vs. conteúdo político) têm diferentes riscos de danos causados por falsos positivos ou falsos negativos nas decisões de restrição.

e. As consequências derivadas de decisões erradas também devem ser tidas em conta como possíveis danos. Uma decisão errada de restrição pode impactar o usuário que gerou o conteúdo, mas também pode impactar o público, os ambientes de informação e as decisões políticas. A pressão para agir rapidamente pode ter um impacto desproporcional em determinados grupos de usuários com base na linguagem ou no tipo de conteúdo.
f. A necessidade de decisões rápidas, mesmo quando justificadas, pode ter outros efeitos negativos com relação às pessoas que analisam os conteúdos, ao seu preparo quanto às decisões sobre restrições e à sua proteção contra os danos causados pela exposição a conteúdos nocivos.

4. Os critérios que afetam a rapidez com que uma decisão pode ser tomada incluem:

a. Se o caso em questão é claro ou difícil/discutível.
b. Se a restrição está de acordo com a lei internacional de direitos humanos, a lei nacional local, ou com os ToS e as diretrizes de comunidade, e se existem alguns conflitos potenciais entre essas normas.
c. Qual o tipo de conteúdo, tanto em termos de formato (texto, imagem, vídeo) quanto de assunto.
d. Qual seria o tipo e o montante do prejuízo em caso de restrição ou não, relacionado com o impacto que o atraso pode ter.
e. Quais podem ser os diferentes efeitos em relação aos usuários em geral e aos alegadamente afetados por determinados conteúdos.
f. Qual será a ação implementada, entre a diversidade de medidas que poderiam ser utilizadas para restringir o acesso ao material. Por exemplo, a remoção de conteúdos restringe o acesso a todos os usuários, ao passo que a colocação de conteúdos atrás de um sistema de login restringe o seu acesso a usuários que não tenham se registrado em um determinado website. Estas e outras medidas têm impactos variáveis na exatidão e nos efeitos da restrição sobre os direitos dos usuários, sendo que a definição da menos restritiva em casos difíceis exige mais tempo.

Critérios F - Avaliação

A informação disponível nas notificações deve ser suficiente para que os tomadores de decisão compreendam, principalmente, a proibição a que se refere, o conteúdo específico que alegadamente a viola e se o conteúdo de fato viola a proibição. Quando se avalia que o conteúdo viola a proibição, a ação implementada deve respeitar o padrão de proporcionalidade. Para garantir uma ação proporcional em relação a cada um dos conteúdos, é necessário avaliar a diversidade dos fatores e proceder a uma apreciação mais ampla do impacto potencial da medida.

1. **Avaliação multifatorial**

a. **Qual é o contexto do conteúdo em questão?**
O conteúdo postado online está, por padrão, disponível globalmente. No entanto, o usuário que disponibiliza o conteúdo e quem o acessa o interpreta em contextos específicos (histórico, referências, orientação, comunidade linguística, etc.). A fim de ter em conta esta tensão fundamental, os tomadores de decisão podem identificar de onde e de quem provém o conteúdo específico. Uma discussão mais ampla sobre os métodos e as dificuldades em identificar a origem seria útil para compreender plenamente os desafios por trás da identificação do contexto. Este problema é agravado quando se consideram situações em que o próprio conteúdo é "espelhado" em vários websites/plataformas diferentes.
Além disso, para entender completamente o contexto, os tomadores de decisão podem primeiro tentar determinar onde o conteúdo é hospedado e exibido. Em outras palavras, é crucial descompactar as diferenças potenciais entre onde o domínio do site está registrado, o país de incorporação do proprietário do site/plataforma, onde o conteúdo está hospedado/codificado (*hashed*) e onde ele está disponível. Finalmente, a avaliação do contexto deve ser realizada por pessoas com capacidade de compreender a língua e o ambiente cultural correspondente.

b. **Qual a motivação daqueles que postaram/repostaram este conteúdo?**
É importante considerar a motivação dos usuários que postaram ou repostaram o conteúdo. Os tomadores de decisão devem ter em mente que pode haver mais do que

um motivo, entre eles: econômico, político, humor, sátira, comentário social. Esses motivos precisam ser avaliados em seu ambiente linguístico e cultural. Quando o motivo pode ser (ou já foi) determinado, isto pode ajudar os tomadores de decisão na sua reflexão sobre as várias opções disponíveis para restrição.

c. **Que motivos podem ter outros atores para "receber" ou ter acesso a este conteúdo?**
   Os tomadores de decisão podem considerar os motivos que outros atores podem ter para "receber" ou ter acesso a este conteúdo. Tais motivos podem estar alinhados com, ou ser independentes da intenção do(s) usuário(s) de publicá-lo(s). Também é importante abordar o risco associado ao conteúdo, incluindo a iminência de perigo associado a ele.

d. **Existem jurisdições/atores específicos que possam ter interesse e/ou ser afetados por esta decisão e, em caso afirmativo, o que dizem as suas leis/regras sobre este tipo de conteúdo?**
   Outras jurisdições/atores podem ter interesse na decisão, ou ser afetados por ela. Se os tomadores de decisão identificarem que essa é uma possibilidade, é importante considerar quais são esses interesses e, em particular, quais das suas leis ou regras específicas podem ser aplicadas. Os pontos acima relativos ao contexto e motivos dos usuários que enviam e recebem conteúdo podem informar a identificação de outras jurisdições relevantes cujos interesses podem ser considerados em uma potencial análise de cortesia ou conflito de leis.

e. **As proibições desse tipo de conteúdo são universais/amplamente compartilhadas/inconsistentes entre jurisdições?**
   O tomador de decisão pode determinar o nível de consistência normativa internacional, entendida como uma avaliação básica do grau de consenso global sobre a inaceitabilidade/ilegalidade de tais conteúdos. Como questão geral, pode ser útil considerar se o conteúdo se encontra em uma das quatro categorias descritas acima na Base Normativa.

f. **Qual é o formato do conteúdo em questão? Como o formato do conteúdo em questão impacta sua potencial viralidade?**
   O formato do conteúdo em questão (por exemplo, texto, imagem, vídeo, hiperlink, etc.) pode muitas vezes deter-

minar a viralidade do conteúdo e é um critério importante a se analisar no que diz respeito à capacidade do conteúdo ser compartilhado entre páginas, plataformas e dispositivos. Além disso, o formato do conteúdo é uma característica importante (mas não única) na determinação do tamanho do arquivo e das suas implicações em termos de acessibilidade e armazenamento.

2. Análise de impacto

A avaliação inclui a consideração de uma série de impactos potenciais, incluindo (mas não se limitando a):

a. Impactos na liberdade de expressão

As leis que restringem a liberdade de expressão devem atender aos testes de legalidade, legitimidade e necessidade extraídos dos artigos 19 da Declaração Universal dos Direitos Humanos (DUDH) e do Pacto Internacional sobre Direitos Civis e Políticos (PIDCP). No entanto, as leis sobre expressão variam entre jurisdições e, consequentemente, as decisões sobre como restringir o conteúdo digital devem prestar especial atenção aos potenciais conflitos de leis.

Em especial, é importante que os tomadores de decisão identifiquem, sempre que possível, que outras jurisdições podem ter ligações ao conteúdo em questão. Isto pode incluir, por exemplo, a identificação do:

i. local onde se situa(m) o(s) usuário(s) responsável(eis) pelo conteúdo;
ii. local onde a plataforma que hospeda o conteúdo está sediada; e/ou
iii. local onde estão localizados os públicos significativos para o conteúdo.

Quanto mais fortes forem as conexões identificáveis com países cujas leis possam ser aplicáveis para proteger o conteúdo em questão, mais cautelosos devem ser os tomadores de decisão antes de ordenar restrições que possam ter impactos nessas jurisdições.

b. Impactos na privacidade

O cumprimento de leis que restringem a expressão online é imperfeito e nunca completo. A dimensão com que as autoridades procuram limitar esta imperfeição tende a corresponder à dimensão com que ela frustra os legítimos

interesses de uma autoridade e/ou resulta em danos para outros indivíduos em sua jurisdição.

Permitir que um conteúdo que viole as leis de um país permaneça disponível online em outro lugar abre a possibilidade para que indivíduos no país censurador possam continuar a acessá-lo contornando restrições técnicas. No entanto, é importante reconhecer que a maioria dos usuários da Internet não usa ferramentas de evasão, e aqueles que as usam tendem a usá-las episodicamente. Como resultado, o "dano" que pode decorrer da possibilidade de evasão deve ser examinado cuidadosamente e caso a caso.

Os esforços para eliminar o conteúdo digital, incluindo os esforços para evitar a "repostagem", tendem a ter impactos extraterritoriais amplos que vão além da liberdade de expressão. Em particular, os esforços para identificar proativamente conteúdos susceptíveis de violar a privacidade criam frequentemente condições que podem conduzir a violações da privacidade. Os tomadores de decisão que ordenam restrições de conteúdo devem estar cientes de que as suas ordens podem ter impacto nos direitos de privacidade e proteção de dados dos indivíduos, tanto dentro quanto fora de sua jurisdição, e devem tomar medidas para garantir que essas ordens evitem ou minimizem a violação desses direitos.

c. **Impactos econômicos**

A hospedagem, exibição e transmissão de conteúdo digital pode envolver uma ampla gama de empresas privadas, incluindo web hosts, registros de Internet, provedores de serviços de Internet, operadoras de redes móveis, redes de entrega de conteúdo, plataformas de mídia social e intermediários financeiros. Ordens para restringir conteúdo, dependendo de sua formulação, muitas vezes impactam várias dessas entidades direta ou indiretamente.

Os tomadores de decisão que ordenem restrições de conteúdo devem considerar em que medida os operadores privados que recebem essas ordens dispõem dos meios tecnológicos e econômicos para executá-las. Dada a importância de promover a concorrência e a inovação no setor das TIC, deve-se dar especial atenção ao impacto que essas restrições podem ter nos pequenos operadores ou startups.

d. Definição de precedente

As decisões de restringir um determinado conteúdo raramente são tomadas isoladamente. Tais decisões tendem a basear-se em ações anteriormente tomadas em relação a conteúdos semelhantes e terão impacto em decisões futuras. Os tomadores de decisão devem estar cientes da possibilidade de que uma determinada restrição possa ser citada como precedente para futuras decisões de outros tomadores de decisão em outros contextos.

Na medida em que as decisões de restrição revelam cumulativamente padrões, elas também podem afetar as decisões dos indivíduos de publicar ou não conteúdo. Embora isso possa constituir uma "dissuasão" eficaz contra violações futuras, quando os padrões de restrição são vagos e as proteções de expressão não são claras, isso também pode levar ao "arrefecimento" da expressão legítima. A maneira como as decisões podem ser contextualizadas e aplicadas de forma restrita ajudará a mitigar a leitura ou aplicação errôneas por indivíduos ou outros tomadores de decisão.

Critérios G - Ação Geograficamente Proporcional

1. Base normativa diferente

As decisões de restrição de conteúdo baseiam-se cada vez mais em dois conjuntos distintos de regras: (1) legislação nacional e (2) Termos de Serviço (ToS) dos provedores e diretrizes de comunidade.

a. Legislação nacional

As leis nacionais relativas a conteúdos ilegais variam muito de país para país. Como consequência, conteúdos que são legais em um país podem ser ilegais em outro. Além disso, alguns países podem ter leis nacionais que proíbem a expressão protegida por normas internacionais de direitos humanos. Em reconhecimento à natureza exclusivamente antiterritorial do conteúdo digital, e por respeito às leis de outras nações soberanas (cortesia), como regra geral, quando se determina que o conteúdo digital viola as leis de uma jurisdição específica, qualquer decisão ou ação relacionada para restringir esse conteúdo deve ser limitada - na medida do possível - a essa jurisdição. Uma avaliação do nível de consistência normativa internacio-

nal (ver Critérios Operacionais B - Base Normativa) pode ajudar a garantir que as restrições com base nas leis nacionais sejam geograficamente proporcionais.

b. **ToS dos Provedores / Diretrizes de Comunidade**
Por natureza, as normas de ToS / Diretrizes de Comunidade[7] dos provedores aplicam-se geralmente à totalidade dos seus serviços, independentemente da nacionalidade ou localização dos usuários. As decisões de restrição de conteúdo com base nestas normas são, portanto, geralmente globais por padrão. Garantir o respeito às normas de proporcionalidade nesses casos continua sendo crucial para preservar a mais ampla disponibilidade de conteúdos legítimos. Um determinado ato ou forma de expressão pode violar as regras pertinentes em um determinado momento e em um determinado local. No entanto, pode não ser proibido em outro lugar ou tempo, ou ainda no mesmo lugar e tempo em circunstâncias diferentes. As Diretrizes de Comunidade devem permitir essa análise diferenciada.

2. Abordagem padrão e exceções

A base normativa invocada para uma restrição de conteúdo tem uma relação direta com a sua extensão geográfica, conforme ilustrado na tabela abaixo, que pode ajudar a identificar a ação padrão associada em cada caso:

	RESTRIÇÃO GEOGRAFICAMENTE LIMITADA	RESTRIÇÃO GLOBAL
ILEGAL SEGUNDO AS LEIS LOCAIS	A menos que a justificativa para o pedido seja claramente contrária aos padrões internacionais de direitos humanos (sem restrição pelo provedor), por padrão, o item de conteúdo é restringido localmente pelo provedor (por exemplo, por meio de filtragem geo-IP).	Uma restrição global pode, excepcionalmente, ser implementada pelo provedor em resposta a um pedido/ordem, se esta for fornecida com uma justificativa adequada (por exemplo, elevada coerência normativa internacional).
CONTEÚDO CONTRÁRIO ÀS NORMAS DE TOS/ DIRETRIZES DE COMUNIDADE	De acordo com a diversidade das circunstâncias locais, o conteúdo é restringido da forma geograficamente mais proporcional.	O conteúdo é geralmente restringido globalmente quando viola claramente o ToS / Diretrizes de Comunidade, salvo quando um tribunal emitiu uma ordem local de permanência.

7 Foi salientado que o objetivo principal e fundamental dos ToS e das diretrizes de comunidade das empresas é manter a natureza e os benefícios do serviço para a comunidade de usuários.

Critérios H - Escolha da Ação

As ações que podem ser implementadas para lidar com conteúdos que são ilegais, nocivos ou contrários aos ToS/Diretrizes de Comunidade são cada vez mais diversificadas. A escolha da medida adequada em cada caso é um componente importante para alcançar o efeito menos restritivo.

A Tipologia de Ações a seguir é uma lista de ações reconhecidas disponíveis para plataformas, intermediários ou Estados para bloquear conteúdo supostamente nocivo ou ilegal. Esta lista foi desenvolvida para ilustrar e mapear um espectro de respostas possíveis e não deve ser entendida como um índice normativo de ações que devem ser consideradas igualmente válidas.

AÇÕES	DESCRIÇÃO
PLATAFORMA/PROVEDOR DE CONTEÚDO E MOTORES DE BUSCA	
CONTEXTO ADICIONAL	Pode ser necessário um contexto adicional para a publicação de determinados tipos de conteúdo, bem como informações explicativas ou URLS para fontes adicionais de informação e perspectivas alternativas. Por exemplo, imagens gráficas de significado histórico, artístico ou científico podem requerer contexto para que os usuários entendam ou apreciem a imagem. O contexto adicional também pode ser utilizado em situações em que o contexto é considerado extremista ou uma forma de desinformação.
ROTULAGEM	Rotulagem com um alerta para um tipo específico de conteúdo (por exemplo, conteúdo violento).
VERIFICAÇÃO DE IDADE / CONTROLE ETÁRIO	A verificação de idade é realizada por plataformas para garantir que o conteúdo seja acessado apenas por usuários com a idade apropriada. O controle etário impede o acesso a conteúdos e serviços por parte de usuários menores de idade, de acordo com as leis nacionais, regionais ou internacionais.
DIREITO DE RESPOSTA	Resposta por suposto conteúdo difamatório, quando a pessoa que o publicou/postou tem a oportunidade de postar uma resposta, contra-argumento, ou declaração de isenção de responsabilidade.
SUSPENSÃO DE CONTA	As contas podem ser desativadas ou suspensas por um determinado período de tempo devido a violações de políticas ou tráfego inválido. Durante esse período, a conta pode não estar acessível (ou seja, a mensagem de erro será exibida), ou visível para o público, ou a funcionalidade chave pode ser desativada (capacidade de publicar, comentar, ler dados). Podem ser enviados alertas para que o titular da conta tenha tempo de solucionar o problema. Se o problema não for resolvido, a conta pode ser desativada.

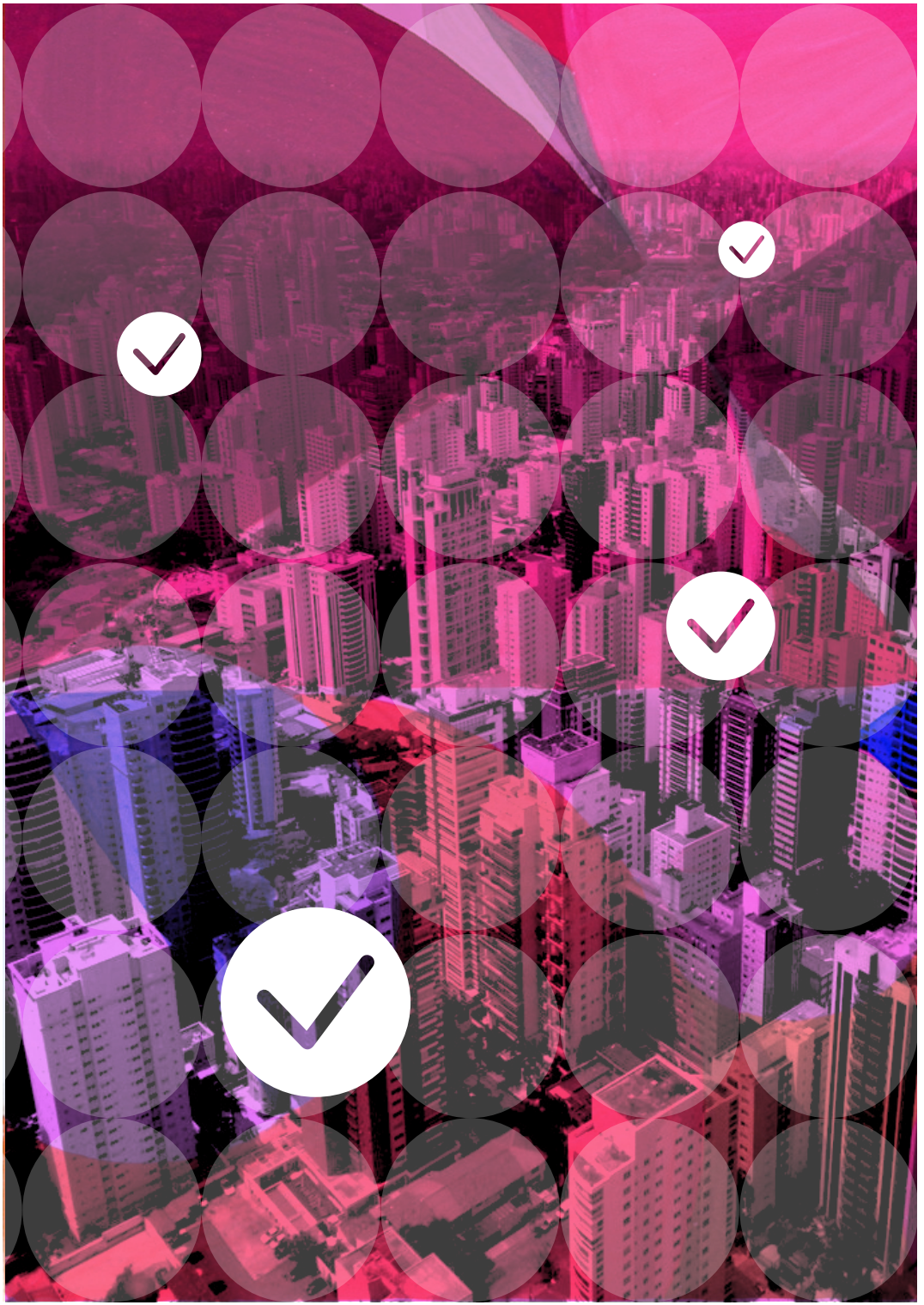
DESATIVAÇÃO DE CONTA	Os usuários ou provedores de conteúdos que não estejam em conformidade com a política vigente pertinente podem ter a sua conta desativada permanentemente para que esta deixe de ser visível ou ativa. Algumas plataformas podem impedir que o usuário crie uma nova conta na mesma plataforma.
ANONIMIZAÇÃO DE DOCUMENTOS DA FONTE	Nos casos que envolvem informações alegadamente difamatórias (por ex., "Direito ao esquecimento"), os nomes podem ser retirados de documentos originais, como artigos de jornal ou documentos públicos e substituídos por iniciais ou uma letra aleatória (ou seja, X ou Y).
BLOQUEAR A INDEXAÇÃO DA PESQUISA	Nos casos que envolvem informação alegadamente difamatória, o conteúdo de páginas individuais pode ser desindexado/desreferenciado, de maneira que o conteúdo não possa ser encontrado através de motores de busca internos (ou seja, arquivo de notícias) ou externos. Isto é feito através da inclusão de um metamarcador no código HTML da página, ou retornando um cabeçalho "noindex" na solicitação HTTP.
BLOQUEIO DE PALAVRAS-CHAVE	Provedores de conteúdo e mecanismos de busca podem bloquear termos específicos de busca por palavra-chave para evitar que o conteúdo associado seja encontrado por meio de resultados de pesquisa. Por exemplo, no Tumblr, pesquisas por palavras-chave associadas a conteúdo adulto voltarão sem resultados, mesmo se houver correspondências.
RETIRADA: REMOÇÃO TEMPORÁRIA OU PERMANENTE	Mecanismo pelo qual um indivíduo pode emitir um pedido legal para que um provedor de conteúdo remova, exclua ou restrinja o acesso a conteúdo supostamente nocivo. Exemplos incluem as políticas de "Direito ao Esquecimento" na UE e o regime de notificação e retirada de direitos de autor do Digital Millennium Copyright Act, dos EUA.
SUBCLASSIFICAÇÃO / VOTAÇÃO (ALTERAR A VISIBILIDADE DO CONTEÚDO)	A subclassificação é usada para rebaixar a visibilidade do conteúdo (como a pesquisa web no Google tem feito nos termos da DMCA) para conteúdos publicados por atores de comprovada má-fé que pretendem manipular ou causar cisões no discurso.
QUARENTENA	Os conteúdos potencialmente nocivos podem ser colocados em quarentena para evitar que sejam vistos pelos usuários. O conteúdo em quarentena geralmente exibe um aviso aos usuários que podem não desejar visualizá-lo ou exigir que os usuários aceitem visualizá-lo.
GEO-BLOQUEIO/ FILTRAGEM GEO-IP/ RETENÇÃO DE CONTEÚDO	As plataformas podem "reter conteúdo" ou bloquear conteúdo de destino, ou bloquear usuários e conteúdo de uma só vez. Isso pode ser feito bloqueando todos os usuários de uma região geográfica, endereços IP específicos ou outras aplicações. Um exemplo de bloqueio geográfico é o "conteúdo retido em país" (CWC, na sigla em inglês) que pode acontecer, por exemplo, se um tuíte violar as leis locais ou se for bloqueado devido a uma ordem judicial.

BANIMENTO "SILENCIOSO" (SHADOW BANNING)	O banimento "silencioso" restringe a visibilidade e o alcance do conteúdo de um usuário sem o seu conhecimento. Esta proibição discreta permite ao usuário realizar todas as atividades normais de um site, mas pode impedir que o seu perfil ou conteúdo publicado fique visível para terceiros ou restringir o alcance do conteúdo, impedindo-o de aparecer em murais ou em resultados de pesquisa. Isto pode ser feito para permitir que os conteúdos problemáticos ou possivelmente nocivos permaneçam no ar, impedindo que aqueles que não os procuram os encontrem. Pode impedir que os maus atores simplesmente iniciem uma nova conta se souberem da proibição ou, alternativamente, pode incentivar os atores de má fé a abandonar uma plataforma devido à falta de engajamento. É também uma técnica comum para combater bots e trolls. Outros termos usados são banimento invisível, banimento fantasma, conversão em fantasma.
BLOQUEIO BASEADO EM PLATAFORMA	Em cooperação com a plataforma, o conteúdo ou os resultados de pesquisa especificados são impedidos de retornar do motor de busca. Isto é frequentemente feito por autoridades nacionais para bloquear conteúdos "ilegais" em uma região geográfica, evitando, assim, bloquear toda uma plataforma. Em alguns casos, pode ser feito por plataformas para bloquear indivíduos que violem os seus ToS ou indiquem ameaça de malware.

AÇÕES	DESCRIÇÃO
INTERMEDIÁRIOS DE REDE / HOSPEDAGEM	
BLOQUEIO BASEADO EM INSPEÇÃO PROFUNDA DE PACOTES	Um dispositivo que bloqueia com base em palavras-chave e/ou outro conteúdo (por exemplo, nome do arquivo) é inserido na rede. Esta técnica é frequentemente utilizada para proteção de dados, AntiSpam e anti-malware (anti-vírus) e priorização de tráfego.
LISTAS DE BLOQUEIO POR PALAVRAS-CHAVE	A lista de bloqueio por palavras-chave é uma ferramenta usada por intermediários de hospedagem para filtrar palavras-chave e outras formas de ID para vídeo ou áudio. A filtragem pode ser automatizada ou feita em combinação com o monitoramento humano. Os Estados também empregam o bloqueio de palavras-chave para censurar conteúdos.
BLOQUEIO BASEADO EM URL OU CABEÇALHO HTTP	Um dispositivo que intercepta solicitações da web e procura URLs em uma lista de bloqueio é inserido na rede.
BLOQUEIO BASEADO EM IP E PROTOCOLO	Um dispositivo que bloqueia o tráfego, com base em endereço IP e/ou aplicação (por exemplo, VPN), entre o usuário final e o conteúdo é inserido na rede.
PROVEDORES DE SERVIÇOS DE INTERNET (ISPS) [PONTO DE CONTROLE]	Os ISPs são pontos de controle muito eficazes, uma vez que são facilmente identificáveis e podem identificar prontamente o tráfego regional e internacional de todos os usuários. Os mecanismos de filtragem podem ser colocados em um ISP através de ordens governamentais, de propriedade ou influência voluntária/coercitiva. Os ISPs podem impedir que todos os seus usuários acessem um site ou usem um aplicativo. O bloqueio pode ser feito com base em uma URL, endereço IP (todo o conteúdo associado ao IP ou parcial); especificações técnicas (tais como bloqueio de uma porta para impedir o uso de VOIP).

FILTRAGEM GEOGRÁFICA IP	Um site pode bloquear parcial ou totalmente usuários com endereços IP de um determinado país ou com base em GPS, identificação de rede Wi-Fi ou outras informações técnicas.
DEGRADAÇÃO DO DESEMPENHO	A degradação do desempenho envolve a diminuição intencional da conectividade e da velocidade de resposta em uma determinada rede. O "estrangulamento da largura de banda", por exemplo, pode ser feito para gerir o congestionamento da rede ou para bloquear parcialmente uma porcentagem do tráfego de determinados endereços IP ou outras aplicações.
DESCARTE DE PACOTES	O descarte de pacotes interrompe o fluxo de tráfego ao não encaminhar adequadamente os pacotes associados ao conteúdo prejudicial. Essa técnica é mais eficaz quando o pacote contém identificadores transparentes vinculados ao conteúdo especificado, como o IP de destino. Muitas vezes resulta em bloqueio excessivo.
BLOQUEIO BASEADO EM DNS / BLOQUEIO DE TLDS GEOGRÁFICOS	No nível da rede ou do ISP, o tráfego do Sistema de Nomes de Domínio (DNS) é encaminhado para um servidor DNS modificado que pode bloquear pesquisas de certos nomes de domínio.
INTERFERÊNCIA DE DNS	A interferência de DNS resulta no retorno de um endereço IP incorreto em resposta a uma consulta DNS a um destino censurado. Os usuários podem receber uma mensagem de erro.
REALOCAÇÃO/ APREENSÃO DO NOME DE DOMÍNIO	Os nomes de domínio podem ser reatribuídos ou apreendidos legalmente (p. ex., em casos de violações criminais de direitos autorais) ou extrajudicialmente quando um domínio de primeiro nível (TLD) anula o registro de um nome de domínio para impedir que os servidores DNS encaminhem e armazenem o site em cache.
DESCONEXÃO DE REDE OU ANÚNCIO DE ROTA ADVERSÁRIA	Esta é uma forma de interferência técnica em que toda uma rede pode ser cortada numa região específica, quando um organismo de censura retira todos os prefixos do BGP (Border Gateway Protocol) que passam pelo país do censor. Esta é uma forma extrema e extensa de bloqueio, geralmente realizada apenas por curtos períodos de tempo em circunstâncias adversas.
DERRUBAR O SERVIDOR	Se o conteúdo indesejável for hospedado no país de censura, os servidores podem ser fisicamente apreendidos ou pode-se exigir que o provedor de hospedagem impeça o acesso.

AÇÕES	DESCRIÇÃO
BLOQUEIO EXTRALEGAL	
BLOQUEIO/ INTERFERÊNCIA/ INJEÇÃO DE PACOTES RST	Um tipo específico de ataque de injeção de pacote, usado para interromper um fluxo estabelecido mediante a emissão de pacotes RST a ambos os lados de uma conexão TCP; como cada receptor pensa que o outro lado deixou cair a conexão, a sessão é terminada. Isto também é conhecido como ataque *"man in the middle"*.



PARTE IV - NOTIFICAÇÃO / RECURSO

Critérios I - Notificação Ao Usuário

1. **Cronologia da notificação**

a. **Notificação ao usuário antes da ação**
Quando uma decisão de restringir conteúdos com base na legislação nacional ou nas especificações técnicas do fornecedor ou nas Diretrizes de Comunidade tiver sido tomada, o usuário deverá ser notificado antes da aplicação da decisão. Isto pode permitir ao usuário modificar o conteúdo de modo a não infringir a base normativa relevante e/ou contestar a decisão.

b. **Notificação ao usuário simultaneamente ou após a ação**
Em algumas situações, pode não ser possível, aconselhável ou permissível que a notificação ocorra antes da implementação da decisão de restrição de conteúdo. Tais situações incluem, entre outras, a melhor avaliação dos provedores de serviços sobre a forma de minimizar potenciais danos.

c. **Exceções à notificação ao usuário**
Excepcionalmente, uma situação pode justificar uma exceção ao princípio geral da notificação ao usuário. Tal situação pode incluir, principalmente, casos em que o usuário não pode ser identificado, requisitos legais locais de confidencialidade e a necessidade de evitar entraves a investigações em curso.

2. **Conteúdo da notificação**

A notificação deve conter informações relativas à base normativa e à justificativa para a restrição, bem como os respectivos canais, informações e prazos para os recursos aplicáveis. Nos casos de conteúdos restritos com base nas orientações ToS/Diretrizes de Comunidade dos provedores, a notificação também deve conter informações relativas à cláusula/diretriz específica que foi violada.

Critérios J - Recurso

O recurso e a apelação surgiram como questões importantes em relação às restrições de conteúdo online. Duas das abordagens atualmente consideradas são abordadas a seguir: os organismos de análise independentes estabelecidos pela empresa e os conselhos de autorregulação nacionais. As discussões

sobre estas abordagens podem ser organizadas em torno das questões estruturantes nas duas notas conceituais abaixo. No entanto, estas notas conceituais não abordam nem prejudicam o nível de apoio a nenhuma destas abordagens.

I. Órgãos de Revisão Instituídos pela Empresa

A nota que se segue explora elementos relacionados com a potencial criação, pelas empresas, de mecanismos que permitam um recurso independente das suas decisões de restrição de conteúdo tomadas com base nas suas Diretrizes de Comunidade. É entendido como um instrumento específico da empresa[8] com autoridade vinculativa no terceiro nível de um processo gradual de tomada de decisões, na sequência de decisões iniciais em uma primeira instância e de uma etapa de reconsideração[9].

Tal como se explica mais adiante, as analogias com os Supremos Tribunais nacionais (ou equivalentes) têm alguma validade, mas só podem ser utilizadas até este ponto, dadas as diferenças muito significativas entre situações. Outras fontes de inspiração também podem ser relevantes e a criatividade é necessária neste ambiente transnacional radicalmente novo.

As seguintes perguntas preliminares poderão ajudar a estruturar os debates "e se" sobre a criação desse mecanismo:

COMPETÊNCIA	DEVIDO PROCESSO	ORGANISMO	OUTROS
▪ Tópicos abordados ▪ Referência normativa ▪ Fonte inicial (IA/notificações) ▪ Filtragem de casos ("cert") ▪ Foco/limitação do mandato ▪ Requerentes ▪ Recursos	▪ Etapas/duração limitadas ▪ Procedimento escrito/oral ▪ Princípio do contraditório ▪ Papel de terceiros ▪ Tomada de decisões ▪ Fundamentação ▪ Opiniões dissidentes ▪ Mecanismos céleres ▪ Transparência ▪ Regime suspensivo	▪ Tamanho ▪ Composição ▪ Perfis dos membros ▪ Designação ▪ Duração do mandato ▪ Frequência das reuniões ▪ Independência ▪ Apoio de secretariado ▪ Financiamento	▪ Estatuto ▪ Denominação ▪ Função(ões) consultiva(s) ▪ Abrangência geográfica ▪ Câmaras temáticas ▪ Mutualização ▪ Ferramentas eletrônicas ▪ Proteção de responsabilidade legal ▪ Coerência da jurisprudência

8 Um órgão específico em oposição a algo que seria estabelecido em nível nacional (como os Conselhos de Mídias Sociais) ou um grupo diversificado de empresas.

9 Ver Anexo 2, infográfico relativo às três etapas.

Os elementos da tabela acima são brevemente detalhados abaixo:

1. **Competência**

a. **Tópicos abordados:** As Diretrizes de Comunidade abrangem diversos tópicos com diferentes volumes de restrições de conteúdo[10] e níveis de detecção automática. Para manter o volume de pedidos de recurso esperados administrável, esse mecanismo deveria estar inicialmente aberto apenas para determinados tópicos? Seria uma opção centrar-se em questões (por exemplo, incitação ao ódio e intimidação) em que o impacto na liberdade de expressão e a necessidade de nuances são máximos, enquanto o número de ações iniciais é relativamente menor (ver anexo 1)?

b. **Referência normativa:** As Diretrizes de Comunidade constituiriam claramente a principal fonte normativa. No entanto, o Estatuto de um organismo deste tipo deveria fazer referência igualmente a outras fontes, como o direito internacional (por exemplo, princípios de direitos humanos e convenções específicas) ou mesmo a leis nacionais (especialmente se o mandato do organismo abranger também, em determinado momento, pedidos de autoridades públicas com base no direito nacional)?

c. **Detecção inicial:** As decisões de restrição de conteúdo são tomadas com base em 1) detecção de Inteligência Artificial, ou 2) sinalização de usuários ou avisos de autoridades públicas. Os recursos, no primeiro caso, envolvem apenas o usuário e a empresa, enquanto o segundo caso cria uma interação tripartite, com potencial impacto no procedimento. O mecanismo previsto deve aplicar-se apenas ao primeiro caso, por uma questão de simplicidade, ou abranger ambas as situações? Isto pode ser estabelecido por fases?

d. **Filtragem de casos ("cert"):** Prevenir a sobrecarga de burocracia que aflige muitos tribunais superiores em todo o mundo é um fator de sucesso fundamental. A Suprema Corte dos EUA concede "cert" apenas a 1,4% dos pedidos que recebe por ano (100 de 7.000) e outras jurisdições adotam uma prática semelhante. A filtragem de casos é pro-

10 Ver, por exemplo, os dados relevantes no relatório de transparência do Facebook, no anexo 1.

vavelmente necessária aqui, mas há incerteza quanto ao número real de casos a serem tratados. Além de eliminar casos claramente frívolos, isso requer um mecanismo de seleção rápida e precoce? Qual a latitude que o organismo deve ter na seleção dos casos que deve analisar? Deve haver disposições específicas e de celeridade para priorizar questões com base em um fator de prazo, como urgência ou situações locais tensas?

e. **Concentração/limitação do mandato:** A maioria dos Supremos Tribunais adota ou está sujeita a uma abordagem restritiva na sua seleção de casos, a fim de, por exemplo, se concentrar em: conflitos entre jurisdições inferiores; conflitos claros de interpretação da lei ou de uma Constituição; ou dimensões processuais de uma instância inferior. Deve ser aplicada aqui uma abordagem semelhante e documentada no Estatuto do organismo e nos formulários de apresentação online? No entanto, é importante notar que, nos exemplos acima, o mecanismo de revisão final se situa dois níveis acima de tribunais independentes inferiores e de um grande corpo de jurisprudência pública, enquanto o exercício aqui começa "de novo", e espera-se que intervenha diretamente como um acompanhamento de um simples processo interno de reapreciação.
f. **Requerentes:** Uma revisão independente final só é prevista contra decisões de restrição tomadas em fase de recurso/reapreciação existente e não contra uma decisão inicial (regra do esgotamento das vias de recurso anteriores). Destina-se claramente a ser iniciado por um usuário cujo conteúdo tenha sido restringido. Deverá este recurso ser igualmente iniciado - e, em caso afirmativo, quando - para notificadores cujos pedidos de afastamento tenham sido recusados? Nesse caso, devem ser feitas distinções entre autoridades públicas e sinalizadores individuais? E entre estes últimos, entre as pessoas diretamente visadas pelas postagens e os sinalizadores mais generalistas? A abertura do recurso para os notificadores aumenta as complexidades processuais.
g. **Recursos:** Que gama de soluções podem ser ordenadas: a simples inversão da decisão relativa à plataforma ou também alternativas mais granulares e matizadas (por exemplo, âmbito técnico, geográfico, advertências, etc.)?

O organismo pode ordenar à empresa que apresente uma correção pública?

2. Devido Processo

Para respeitar plenamente os direitos humanos, um órgão de revisão independente deve se inspirar em elaborados requisitos de devido processo desenvolvidos em várias nações para tribunais que lidam com a liberdade de expressão. No entanto, o grande volume de casos esperados e a necessidade de manter o processo gerenciável exigem alguma adaptação. Isto significa, nomeadamente, fazer escolhas sobre os seguintes elementos:

a. **Etapas/duração limitadas:** Em vez de diversas fases iterativas, o processo deve ter um número limitado de etapas e/ou duração? Os formatos online dedicados ao recurso podem ajudar nesse sentido?
b. **Procedimento escrito/oral:** O procedimento basear-se-á exclusivamente em resumos escritos ou também em alegações orais? Isso variaria de alguma forma, dependendo dos casos?
c. **Princípio do contraditório:** Este procedimento pode ser visto de duas maneiras diferentes. Seja como arbitragem de uma disputa entre a empresa e o usuário, seja como revisão de uma decisão de uma instância inferior. Os representantes das empresas seriam partes no processo ou apenas fundamentariam a decisão inicial? Os notificadores individuais diretamente afetados pela postagem em questão (se aplicável) devem fazer parte do processo?
d. **Terceiros:** Qual é a possibilidade da intervenção de terceiros no procedimento (por exemplo, representação legal, como "amicus" apresentado por uma ONG de apoio ou outras partes) e quais as condições destes?
e. **Tomada de decisões:** Quais seriam as regras majoritárias para as decisões do organismo e de quaisquer subconjuntos deste?
f. **Fundamentação:** Apresentar uma justificativa para cada decisão é potencialmente oneroso, mas constitui uma contribuição importante para a criação de uma jurisprudência coerente, na medida em que estabelece um precedente. Isto deve ser implementado e, em caso afirmativo, para todas ou apenas algumas decisões (por exemplo, em formações maiores)?

g. **Opiniões dissidentes:** Podem ser previstas e, em caso afirmativo, em que condições?
h. **Mecanismos céleres:** Independentemente do tamanho geral do organismo, a maioria das decisões pode ser tomada por um número limitado de membros, mantendo formações maiores para casos mais delicados? Do mesmo modo, as garantias processuais podem variar em função da importância ou complexidade do caso como, por exemplo, um mero procedimento escrito em uma só etapa para os mais simples?
i. **Transparência:** Qual seria o nível de publicidade das deliberações e decisões? Deverá ser criado um repositório de tais decisões e, em caso afirmativo, por quem? Devem ser tomadas algumas precauções para preservar os direitos dos usuários, tais como a anonimização das decisões?

3. Organismo

a. **Tamanho:** Se for formado um único órgão de recurso por empresa, a determinação da sua dimensão adequada pode ser informada por uma análise das práticas em tribunais superiores ou equivalentes não só nos EUA, mas também na Europa (por exemplo, França, Reino Unido, Alemanha, ...), Índia, Brasil e outros países, bem como em alguns tribunais regionais (por exemplo, Corte Europeia de Direitos Humanos – CEDH). Estes organismos variam significativamente de tamanho: 9 para o Supremo Tribunal dos EUA, 30 na Índia, 47 para a CEDH, com diferentes tamanhos de formações. À luz do grande número de casos esperados, do tamanho e diversidade das comunidades de usuários e da ausência de uma vasta rede de tribunais inferiores, um pequeno número de membros seria viável? Com base nas práticas de arbitragem e de mecanismos alternativos de resolução de conflitos (ADR), a possibilidade de estabelecer uma vasta lista de árbitros ou mediadores disponíveis para a composição de painéis ad hoc deve ser contemplada?
b. **Composição equilibrada:** As Diretrizes de Comunidade abrangem vários tópicos, exigindo competências diversificadas. Além disso, o alcance geográfico global de uma empresa significa uma diversidade de escritas4, idiomas, contextos culturais e políticos locais, que exigem conhe-

cimentos linguísticos e locais. Como garantir os equilíbrios geográficos, de atores, de gênero, de idade, culturas e de competências que serão fundamentais para permitir decisões diferenciadas e estabelecer a legitimidade de tal organismo? A composição deve ser organizada em torno de grupos específicos? Como os interesses da comunidade de usuários podem ser representados?

c. **Perfis dos membros:** Um impulso espontâneo seria o de recorrer principalmente aos conhecimentos especializados de antigos juízes ou advogados. No entanto, a maioria é proficiente num determinado organismo de legislação nacional e pode manter um viés específico nesse sentido, enquanto o principal corpo de normas a ser aplicado aqui será provavelmente o das Diretrizes de Comunidade. Como garantir uma ampla diversidade de perfis e experiências profissionais, privilegiando pessoas com exposição a uma variedade de ambientes?
d. **Designação:** Esta pode ser uma das questões mais delicadas. As modalidades de designação dos juízes dos tribunais superiores nos países são difíceis de transpor. Uma designação feita apenas pela administração da empresa - seja qual for o nível - provavelmente não seria entendida como plenamente legítima. No entanto, uma seleção completa pela própria comunidade levanta muitos desafios conceituais e operacionais. Que mecanismos inovadores podem ser projetados para permitir a seleção de pessoas de alta integridade, competência e dedicação que serão vistas pela comunidade e pelo público em geral como um colegiado legítimo e confiável? Devem ser combinadas diversas fontes de designação? Grupos específicos devem desempenhar algum papel e, em caso afirmativo, como formá-los se for global?
e. **Duração do mandato:** O mandato vitalício dos juízes do Supremo Tribunal dos EUA é um caso isolado e um mandato limitado parece mais adequado. Qual seria a sua duração adequada (2, 4, mais anos)? Deve haver um número limitado de renovações (1, 2, mais)? A rotatividade parcial ajudaria a evitar mudanças brutais na composição do grupo? Um grande grupo pode ser constituído progressivamente (por exemplo, com 1/3 dos membros de 2 em 2 anos nos primeiros 6 anos, se essa duração for mantida)?

f. **Frequência das reuniões:** Com que frequência o Organismo deve se reunir? A frequência deverá ter em conta o número de casos previstos em função das respostas às questões de abrangência (na parte 1) e procedimento (na parte 2) acima referidas.
g. **Independência:** Este é um fator crítico, qualquer que seja o papel que a empresa possa desempenhar na designação dos membros. Dado o volume de atividade previsto, deve-se esperar que os membros se dediquem plenamente a esta missão durante o período do seu mandato ou não? Em qualquer caso, quais devem ser as políticas de conflito de interesses que limitam suas atividades passadas ou atuais, incluindo suas potenciais relações com a empresa?
h. **Apoio de Secretariado:** Esse organismo necessitará de apoio de secretariado para gerir o processo e realizar investigação. A automatização será capaz de reduzir a carga global em comparação com os processos judiciais existentes?
i. **Financiamento:** O financiamento de tal organismo será de exclusiva responsabilidade da empresa? Ou deveria haver outras fontes?

4. Outros

a. **Estatuto:** Será necessária a criação de um Estatuto específico para esta instância de recurso independente, que especifique, entre outros, o seu mandato, a base de referência normativa, os procedimentos, a composição e o modo de designação. Como deve ser desenvolvido e qual o papel que a comunidade de usuários correspondente pode desempenhar neste contexto?
b. **Denominação:** Esta nota utiliza a expressão "Organismo de Revisão Independente" ("Independent Review Body") por padrão. Outros nomes podem ser considerados, tais como Painel, Conselho, Comitê ou equivalente. Qual poderia ser a denominação apropriada, uma vez que o termo "Revisão Independente" tem uma forte vantagem em termos de clareza.
c. **Função(ões) consultiva(s):** Além do papel de recurso sobre as decisões individuais acima, as seguintes funções consultivas adicionais poderiam ser contempladas para esse organismo:

- Análise caso-a-caso, em uma fase precoce, mediante pedido espontâneo da empresa em situações difíceis ou sensíveis, mesmo antes da tomada de uma decisão ou da notificação do usuário,
- De forma mais geral, fornecer orientações sobre as melhores práticas e o aperfeiçoamento das Diretrizes de Comunidade, com base nos casos em análise ou em alguns casos que seriam compartilhados pela empresa.

No primeiro caso, e talvez também no segundo, a empresa teria a opção de seguir/obedecer ao parecer/recomendação (sem qualquer outra justificativa), ou não (em cujo caso seria necessário apresentar uma explicação ao organismo para auxiliá-lo no aperfeiçoamento da sua jurisprudência)?

d. Câmaras temáticas: Muitas jurisdições ao redor do mundo dispõem de câmaras especializadas para diferentes tópicos. No devido tempo, diferentes subgrupos deverão ser criados, de acordo com as competências ou preferências pessoais dos membros, especializados em determinados tipos de casos?

e. Abrangência geográfica: Do mesmo modo, a fim de assegurar a máxima compreensão do contexto local, das culturas e dos arcabouços jurídicos, os subgrupos de membros deverão – oportunamente - compor câmaras especializadas, por exemplo, com base em um roteiro ou em uma base linguística (e não numa base puramente geográfica ou nacional)? Como manter a diversidade cultural em tais agrupamentos para preservar alguma coerência jurisprudencial? Essas instâncias de recurso independentes podem, alternativamente, ser criadas a nível nacional?

f. Mutualização: A implementação de um Órgão de Revisão Independente por parte de cada empresa pode ser difícil, especialmente para as pequenas empresas. Poderia haver alguns agrupamentos entre várias empresas?

g. Ferramentas eletrônicas: Como na moderação geral, uma automação significativa deste processo de revisão independente pode ser obtida para gerenciar o fluxo de trabalho de um grande número de casos. Poderiam ser explorados mecanismos inovadores para permitir a tomada de decisões colegiadas entre pessoas que possam estar distribuídas em vários locais do mundo?

h. **Proteção de responsabilidade civil:** A criação de um órgão de fiscalização independente teria impacto no regime de responsabilização da empresa em questão?
i. **Coerência da jurisprudência:** Como garantir a compatibilidade entre as decisões de uma diversidade de Órgãos de Revisão Independentes de diferentes empresas?

NOTA: Esta nota se concentra essencialmente nas decisões tomadas com base na detecção por IA. A análise independente das decisões tomadas com base na notificação suscita desafios processuais adicionais e deve também ser considerada, em especial, em dois casos: os alertas enviados por pessoas diretamente visadas ou afetadas por determinadas postagens e as notificações de autoridades públicas. Tais casos exigiriam etapas processuais adicionais e uma análise mais aprofundada.

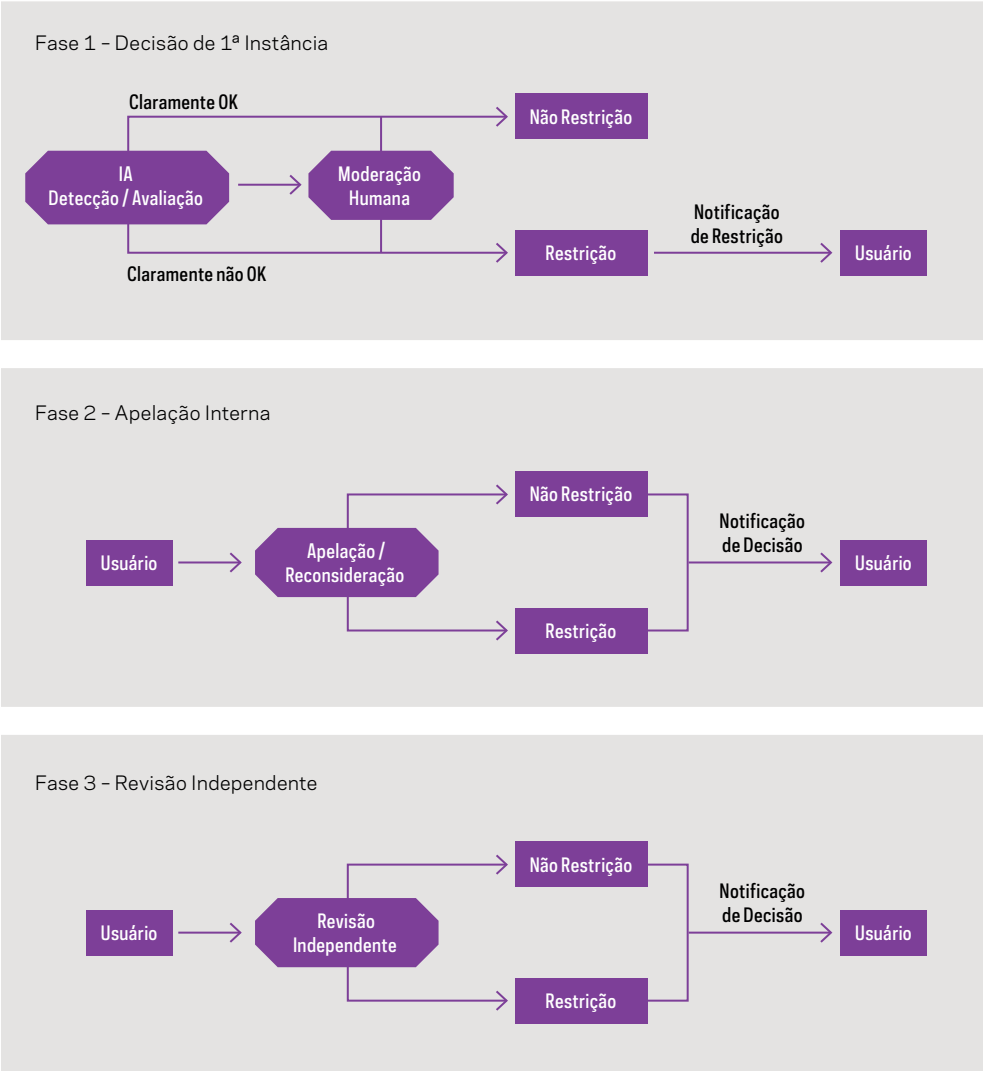
Anexo 1: Tipologia de ações por tema

Um recente relatório de transparência do Facebook mostra que as medidas tomadas podem ser agrupadas em três grupos diferentes:

VOLUMES ANUAIS MUITO ELEVADOS, COM UM FORTE COMPONENTE DE SEGURANÇA E QUASE 100% DE DETECÇÃO PELO FACEBOOK	VOLUMES ANUAIS SIGNIFICATIVOS, COM UM FORTE COMPONENTE VISUAL E QUASE 100% DE DETECÇÃO PELO FACEBOOK	VOLUMES ANUAIS MAIS LIMITADOS, COM UM FORTE COMPONENTE DE LIBERDADE DE EXPRESSÃO E NÍVEIS DE DETECÇÃO MAIS BAIXOS PELO FACEBOOK
▪ Spam (cerca de 4 bilhões de ações /ano) ▪ Contas falsas (cerca de 2,4 bilhões/ano)	▪ Nudez (100 M de ações /ano) ▪ Exploração infantil (36 M de ações /ano) ▪ Violência explícita (25 M de ações /ano) ▪ Terrorismo (15 M de ações /ano)	▪ Discurso de ódio (9,5 M de ações /ano, com 50 % de detecção automática) ▪ Bullying (8 M de ações /ano, com 20 % de detecção automática)

Talvez faça sentido centrar o âmbito deste sistema de revisão independente, pelo menos inicialmente, nas terceiras categorias (discurso de ódio e bullying), onde o impacto sobre a liberdade de expressão e a necessidade de nuances são maiores, enquanto que o número de ações iniciais é - relativamente - menor.

Anexo 2: Análise Independente como terceira etapa do Processo Decisório Gradual



O fluxo de trabalho do processo correspondente a situações em que foram tomadas decisões após a notificação (por usuários ou autoridades públicas) não está descrito aqui e envolve interações adicionais.

II. Conselhos de Autorregulação Baseados em Países

A presente nota identifica elementos para ajudar a discutir o conceito dos Conselhos de Mídias Sociais (CMSs). Propõe-se a criação de CMSs como organismos nacionais independentes de autorregulação que estabelecerão, entre outros, mecanismos de recurso contra decisões de moderação de conteúdos tomadas por Plataformas de Mídias Sociais (PMS).

Esta abordagem surgiu por analogia às práticas de autorregulação existentes na imprensa escrita, em particular nos Conselhos de Imprensa, mas deve levar em conta diferenças significativas. Outras referências também podem ser relevantes e é necessário originalidade neste ambiente transnacional radicalmente novo.

As seguintes perguntas podem ajudar a estruturar as discussões "e se" sobre a criação de tais CMSs. Estas adaptam e expandem as perguntas propostas neste documento para discutir outro tipo potencial de recurso: os órgãos de revisão independentes instituídos pela empresa. As perguntas podem ser categorizadas nos seguintes grupos:

COMPETÊNCIA	DEVIDO PROCESSO	ORGANISMO	OUTROS
▪ Empresas abrangidas ▪ Temas abordados (âmbito) ▪ Referência normativa ▪ Fonte inicial (IA/notificações) ▪ Filtragem de Casos ("cert") ▪ Foco/limitação do mandato ▪ Requerente ▪ Autoridade ▪ Recursos ▪ Sanções	▪ Etapas/duração limitadas ▪ Procedimento escrito/oral ▪ Princípio do contraditório ▪ Papel de terceiros ▪ Tomada de decisões ▪ Fundamentação ▪ Opiniões dissidentes ▪ Mecanismos Céleres ▪ Transparência ▪ Procedimento suspensivo	▪ Tamanho ▪ Composição ▪ Perfis dos membros ▪ Designação ▪ Duração do mandato ▪ Frequência das reuniões ▪ Independência ▪ Apoio de Secretariado ▪ Financiamento	▪ Criação ▪ Estatuto ▪ Denominação ▪ Função(ões) consultiva(s) ▪ Abrangência geográfica ▪ Câmaras temáticas ▪ Mutualização ▪ Ferramentas eletrônicas ▪ Proteção de Responsabilização ▪ Coerência jurisprudencial

Os elementos da tabela acima são brevemente detalhados abaixo:

1. **Competência**

a. **Empresas abrangidas:** Um CMS só aceitaria recurso contra decisões de empresas que tivessem voluntariamente

aceitado sua autoridade ou poderia também ser encarregado de supervisionar qualquer empresa que "prestasse serviços no país"?

b. **Tópicos abordados:** A moderação de conteúdo por PMSs cobre uma ampla gama de tópicos com diferentes volumes de restrições e níveis de detecção automática. Esse mecanismo deveria inicialmente estar aberto apenas para determinados tópicos, a fim de manter viável o volume de pedidos de recurso esperados? Seria uma opção centrar-se em questões (por exemplo, discurso de ódio e bullying) em que o impacto na liberdade de expressão e a necessidade de nuances são máximos, enquanto o número de ações iniciais é relativamente menor?
c. **Referência normativa:** Em que documentos se baseariam as decisões do CMS? Fontes das autoridades públicas existentes, tais como legislação(ões) nacional(is), convenções específicas, princípios internacionais de direitos humanos? As Diretrizes de Comunidade das empresas devem ser levadas em conta? Devem ser desenvolvidos novos documentos ad hoc (por exemplo, um "Código de Ética" ou equivalente)? Em caso afirmativo, devem ser específicos para cada CMS ou devem ser mais amplos (regionais ou mesmo globais)? E como devem ser desenvolvidos? Nota: a expressão "Código de Ética" pode ser um rótulo errado se se tratar de normas materiais (harmonização) e não dos procedimentos internos do Conselho.
d. **Detecção inicial:** As decisões de restrição de conteúdo são tomadas pelas PMSs com base em 1) Inteligência Artificial, 2) alertas do usuário ou 3) avisos das autoridades públicas nacionais, incluindo decisões judiciais. No primeiro caso, os recursos apenas envolvem o usuário que fez a postagem e a empresa, enquanto os outros dois criam uma interação tripartite com consequências no procedimento de recurso. Podem surgir tensões com as autoridades públicas no terceiro caso. O mecanismo previsto deverá abranger apenas o primeiro caso, por uma questão de simplicidade, ou abranger uma ou ambas das outras situações? Isto pode ser estabelecido por fases?
e. **Filtragem de casos ("cert"):** Dados os vastos volumes de conteúdos postados e as numerosas decisões tomadas pelas

PMSs, manter o número de processos de recurso gerenciáveis para um CMS pode ser um grande desafio. Que critérios e mecanismos de filtragem podem ajudar a eliminar casos claramente frívolos, abordar rapidamente situações repetidas em que existem precedentes e concentrar-se nas questões difíceis e potencialmente criadoras de precedentes?

f. **Foco/limitação do mandato:** A competência do órgão deverá ser explicitamente definida de forma limitativa, por exemplo, no seu Estatuto? A competência poderia abranger, por exemplo, além dos tópicos mencionados acima, requisitos relativos a: reapreciação prévia obrigatória dentro da empresa (por exemplo, pela ouvidoria), ou uma ligação substancial do caso com o país em questão (com ou sem critérios enumerativos). As decisões devem abordar apenas os aspectos processuais da decisão da empresa ou a parte material do processo?
g. **Requerentes:** Deve ser considerada a nacionalidade ou a residência do requerente, em especial para evitar a escolha de foro ("forum shopping")? Além disso, tal recurso é claramente contemplado como uma via de recurso para um usuário cujo conteúdo tenha sido restringido. A abertura de recursos aos notificadores acrescenta algumas complexidades processuais. A revisão das decisões tomadas com base no pedido/ordem das autoridades públicas pode levantar questões de hierarquia das normas. O processo também deve ser aberto - e, em caso afirmativo, em que condições – para os notificadores cujos pedidos de retirada tenham sido recusados? Nesse caso, devem ser feitas distinções entre autoridades públicas e notificadores individuais e, entre estes últimos, entre as pessoas diretamente visadas por uma postagem e os notificadores em geral?
h. **Autoridade:** Em que medida seriam vinculativas as decisões desse Conselho para as plataformas participantes? A este respeito, podem existir diferentes modelos em diferentes países e/ou para diferentes provedores no mesmo país? Pode haver duas situações: autoridade vinculativa para aqueles que aderiram formalmente ao Estatuto e não vinculativa para os outros, mesmo que isso crie desincentivos?
i. **Recursos:** Que gama de soluções podem ser ordenadas: a simples inversão da decisão relativa à plataforma ou

também alternativas mais granulares e matizadas (por exemplo, âmbito técnico, geográfico, advertências, etc.)?

j. **Penalidades:** Em determinadas circunstâncias, um CMS poderia impor sanções (monetárias ou não, por exemplo, desculpas públicas) às plataformas como parte da sua decisão?

2. Devido processo

Para respeitar plenamente os direitos humanos, um mecanismo de recurso como o CMS poderia inspirar-se nas práticas dos Conselhos de Imprensa, mas também nos elaborados requisitos de devido processo desenvolvidos em várias nações para tribunais que lidam com a liberdade de expressão. No entanto, o grande volume de casos esperados e a necessidade de manter o processo gerenciável exigem alguma adaptação.

Isto significa, entre outros, fazer escolhas sobre os seguintes elementos:

a. **Etapas/duração limitadas:** Em vez de diversas fases iterativas, o processo deve ter um número limitado de etapas e/ou duração? Os formatos online dedicados ao recurso podem ajudar nesse sentido?

b. **Procedimento escrito/oral:** O procedimento basear-se-á exclusivamente em resumos escritos ou também em alegações orais? Isso variaria de alguma forma, dependendo dos casos?

c. **Princípio do contraditório:** Este procedimento pode ser visto de duas maneiras diferentes. Seja como arbitragem de uma disputa entre a empresa e o usuário, seja como revisão de uma decisão de uma instância inferior. As autoridades públicas ou notificadores individuais seriam partes no processo ou apenas fundamentariam a decisão inicial? Os notificadores individuais diretamente afetados pela postagem em questão (se aplicável) devem fazer parte do processo?

d. **Terceiros:** Qual é a possibilidade da intervenção de terceiros no procedimento (por exemplo, representação legal, como "amicus" apresentado por uma ONG de apoio ou outras partes) e quais as condições destes?

e. **Tomada de decisões:** Quais seriam as regras majoritárias para as decisões do CMS e quaisquer subconjuntos deste?

f. **Fundamentação:** Apresentar uma justificativa para cada decisão é potencialmente oneroso, mas constitui uma contribuição importante para a criação de uma jurisprudência coerente, na

medida em que estabelece um precedente. Isto deve ser implementado e, em caso afirmativo, para todas ou apenas algumas decisões (por exemplo, em estruturas maiores)?

g. **Opiniões dissidentes:** Podem ser contempladas e, em caso afirmativo, em que condições?
h. **Mecanismos céleres:** Independentemente do tamanho geral do organismo, a maioria das decisões pode ser tomada por um número limitado de membros, mantendo formações maiores para casos mais delicados? Do mesmo modo, as garantias processuais podem variar em função da importância ou complexidade do caso, com, por exemplo, um mero procedimento escrito em uma só etapa para os mais simples?
i. **Transparência:** Qual seria o nível de publicidade das decisões? E das deliberações?
j. **Procedimento suspensivo:** Se a ação da empresa permanecer em vigor durante o recurso, deve um procedimento específico permitir que o conteúdo seja restabelecido enquanto se aguarda a decisão? Em caso afirmativo, em que circunstâncias?

3. Estrutura

a. **Tamanho:** Os organismos menores são mais fáceis de gerir, mas as limitações de uma composição equilibrada (ver acima) vão na direção oposta. O tamanho de um CMS deveria variar em relação ao tamanho do país e ao número de casos que é provável que ele aborde, à luz das respostas às perguntas acima sobre o escopo e o mandato?
b. **Composição:** O conceito de Conselhos de Redes Sociais baseia-se na representação de diferentes categorias de atores, em particular empresas e diferentes tipos de organizações da sociedade civil. Como identificar os grupos relevantes e definir o equilíbrio entre os diferentes grupos? As autoridades locais devem ter uma representação e, em caso afirmativo, de que natureza: papel de decisão pleno ou não? Como a composição deveria variar em relação às circunstâncias locais e existiriam algumas diretrizes mínimas comuns?
c. **Perfis dos membros:** A moderação de conteúdo abrange vários tópicos, exigindo competências diversificadas.

Além disso, a abordagem nacional exige capacidade linguística e conhecimento do contexto local e do sistema jurídico. Como garantir o equilíbrio de gênero, de idade, culturais e de competências entre atores, que serão fundamentais para permitir decisões diferenciadas e estabelecer a legitimidade de tal organismo? Como podem ser representados os interesses da comunidade de usuários?

d. **Designação:** Para a sua formação, os conselhos de imprensa recorrem geralmente a associações profissionais preexistentes (por exemplo, meios de comunicação social, jornalistas, etc.) que podem designar, por meio de eleições, os ocupantes dos respectivos lugares. O novo campo das Redes Sociais pode, no entanto, não ser tão estruturado quanto os meios de comunicação tradicionais. Como as circunscrições devem ser determinadas? Quão diversificados podem ser os modos de designação? Podem ser concebidos mecanismos inovadores para permitir a seleção de pessoas de elevada integridade, competência e dedicação? Devem ser combinados diversos modos de designação?
e. **Duração do mandato:** Qual é a duração adequada do mandato dos membros do Conselho? Deve haver limites para as renovações? A renovação deve ser rotativa para garantir a continuidade?
f. **Frequência das reuniões:** Com que frequência o Conselho deve se reunir? A frequência deverá levar em conta a quantidade de casos prevista, em função das respostas às perguntas sobre o escopo (na parte 1) e procedimento (na parte 2) acima referidas. Será que reuniões muito infrequentes colocariam uma responsabilidade grande e potencialmente desproporcional sobre um Secretariado?
g. **Independência:** Que grau de independência deve ser estabelecido, 1) para a instituição no seu conjunto, em especial em relação ao governo nacional, e 2) para cada membro do Conselho? No segundo caso, deve-se esperar que os membros se dediquem plenamente a esta missão durante o seu mandato ou não? Em ambos os casos, quais devem ser as políticas de conflito de interesses que limitam suas atividades passadas ou atuais? Os membros devem ser remunerados?
h. **Apoio de Secretariado:** Esse organismo necessitará de apoio de secretariado para gerir o processo e realizar inves-

tigação. A automatização será capaz de reduzir a carga global em comparação com os processos judiciais existentes?

i. **Financiamento:** O financiamento de um organismo desse tipo basear-se-ia apenas nas contribuições das PMS participantes? De acordo com que critérios (várias métricas de tamanho, atividade relacionada no país, ...)? Os critérios e níveis serão estabelecidos pelo próprio Conselho? Deve haver outras fontes de financiamento, inclusive do governo em questão?

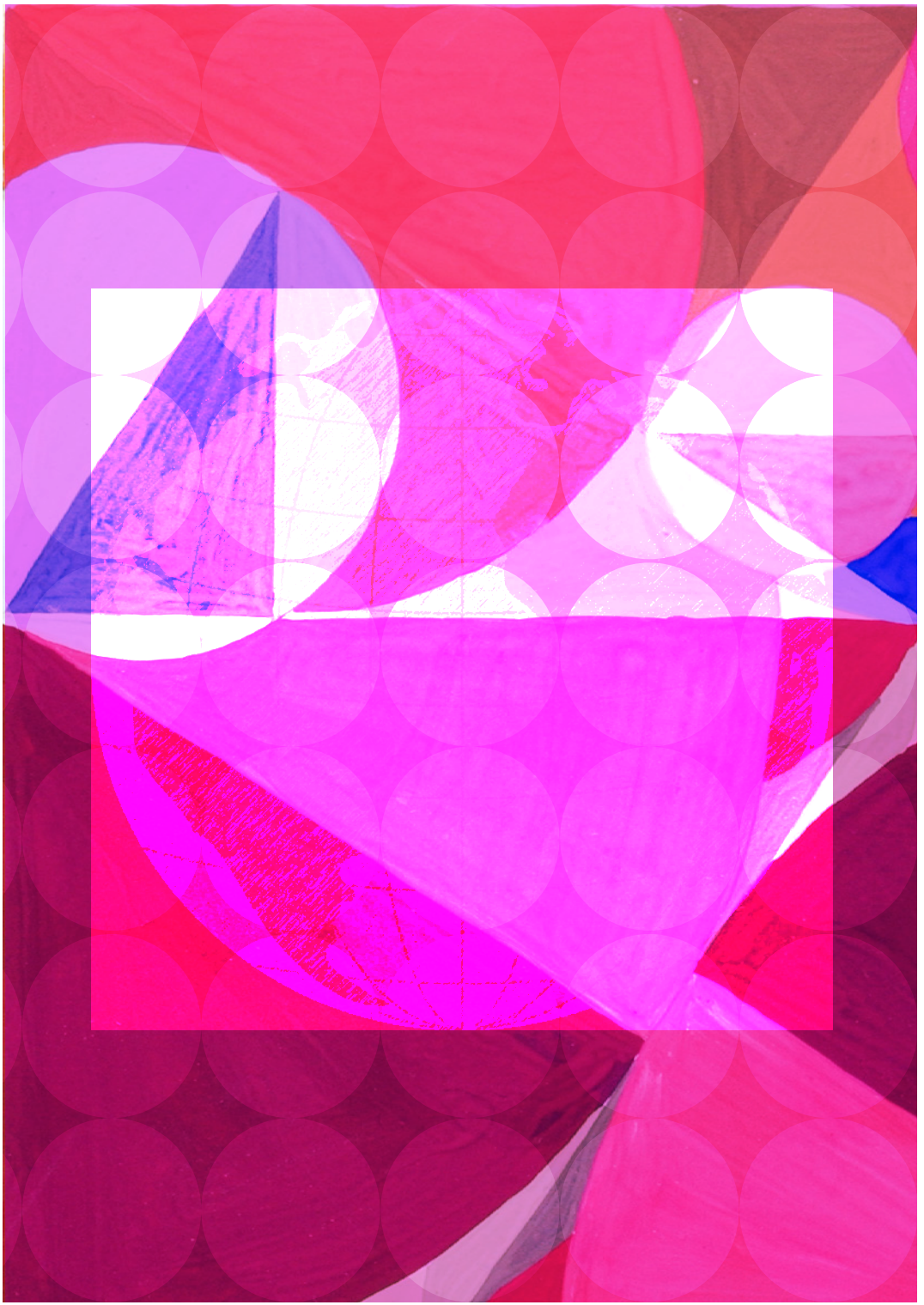
4. Outros

a. **Criação:** Quem cria um CMS: uma coligação espontânea de empresas e atores da sociedade civil? O mesmo, mas incentivado pelo governo local? O governo local, embora uma legislação formal ainda garanta a independência (ou não)? Isso pode variar de país para país (ver analogia com os diferentes regimes de ccTLDs)?
b. **Estatuto:** Será necessário um Estatuto específico para esta instância de recurso independente, que especifique, entre outros, o seu mandato, a base de referência normativa, os procedimentos, a composição e o modo de designação. Como deve ser desenvolvido? Qual seria a forma do compromisso das PMSs participantes de implementar as decisões?
c. **Denominação:** Esta nota usa a expressão "Conselho de Mídias Sociais" por padrão. Podem ser previstos nomes alternativos, correspondendo a potenciais diferenças de abordagens entre os países?
d. **Função(ões) consultiva(s):** Além do papel de recurso sobre as decisões individuais acima, as seguintes funções consultivas adicionais poderiam ser contempladas para esse organismo:
   - Análise caso-a-caso, em uma fase precoce, mediante pedido espontâneo da empresa em situações difíceis ou sensíveis, mesmo antes da tomada de uma decisão ou da notificação do usuário,
   - De forma mais geral, fornecer orientações sobre as melhores práticas e o aperfeiçoamento das Diretrizes de Comunidade, com base nos casos em análise ou em alguns casos que seriam compartilhados pela empresa.

No primeiro caso, e talvez também no segundo, a empresa teria a opção de seguir/obedecer o parecer/recomendação (sem qualquer outra justificativa), ou não (em cujo caso seria necessário apresentar uma explicação ao organismo para auxiliá-lo no aperfeiçoamento da sua jurisprudência)?

e. **Câmaras temáticas:** Muitas jurisdições ao redor do mundo dispõem de câmaras especializadas para diferentes tópicos. No devido tempo, diferentes subgrupos deverão ser criados, de acordo com as competências ou preferências pessoais dos membros, especializados em determinados tipos de casos?
f. **Mutualização:** A implementação dos Conselhos de Mídias Sociais em todos os países pode ser difícil, especialmente para os países menores. Alguns agrupamentos podem ser organizados, numa base geográfica (por exemplo, regional), linguística ou cultural? Isto exigiria a existência de algum quadro de referência harmonizado (por exemplo, a Carta Europeia dos Direitos do Homem)?
g. **Ferramentas eletrônicas:** Como na moderação geral, uma automação significativa deste processo de revisão independente pode ser alcançada para gerenciar o fluxo de trabalho de um grande número de casos. Poderiam ser explorados mecanismos inovadores que permitam uma tomada de decisão colegiada?
h. **Proteção de responsabilidade civil:** O compromisso com um regime voluntário de autorregulação, como um CMS, teria impacto no regime de responsabilização das empresas participantes?
i. **Coerência da jurisprudência:** Como garantir a compatibilidade entre as decisões de uma diversidade de Conselhos de Mídias Sociais de diferentes países, especialmente quando dizem respeito a casos transnacionais?

Nota: Esta nota aborda principalmente os recursos contra as restrições de conteúdo. São igualmente necessários mecanismos de recurso contra as suspensões de contas, que podem suscitar questões adicionais.



PARTE V - ESCALABILIDADE

Critérios K - Capacidade dos pequenos provedores/países

1. **Provedores pequenos ou atípicos** são confrontados com desafios específicos em um cenário em rápida evolução relativo à moderação e restrição de conteúdo, inclusive:
    a. Regras jurídicas frequentemente estabelecidas em referência a grandes atores mundiais bem conhecidos, sem critérios ou limiares suficientes para um tratamento diferenciado dos pequenos atores ou de diferentes tipos de serviços,
    b. Disponibilidade limitada de recursos humanos e financeiros para lidar com o aumento de obrigações na avaliação de conteúdo,
    c. Dificuldades em desenvolver por conta própria ou mesmo ter acesso a ferramentas algorítmicas e de IA para atender às crescentes obrigações de detecção e tempos de resposta curtos,
    d. Dependência de banco de dados hash externo para evitar o recarregamento do conteúdo,
    e. Capacidade limitada para criar mecanismos de recurso próprios.

Deve-se levar em conta esforços diferenciados de tratamento e mutualização como parte do ecossistema geral de moderação e restrição de conteúdo.

MECANISMO OPERACIONAL

NOVAS ABORDAGENS RELATIVAS AO RECURSO APÓS RESTRIÇÃO DO CONTEÚDO

Contexto

Todos os dias, centenas de milhões de mensagens e centenas de milhares de horas de vídeos são carregados nas principais plataformas da Internet e tornados globalmente acessíveis, facilitando grandemente a liberdade de expressão. Ao mesmo tempo, preocupações legítimas são levantadas em relação ao aumento de comportamentos nocivos. Abordar os abusos e ao mesmo tempo proteger os direitos humanos tornou-se uma questão central da sociedade digital global.

Os provedores de serviços têm um papel importante a desempenhar na identificação e moderação de conteúdos que sejam ilegais ou não estejam em conformidade com os seus Termos de Serviço (ToS) e Diretrizes de Comunidade. Isto foi traduzido em vários arcabouços normativos, incluindo a autorregulação, códigos de conduta ou regulamentação rígida. Além disso, espera-se que as numerosas decisões dos provedores sobre restrição de conteúdos sejam tomadas em prazos curtos para limitar potenciais danos.

A utilização de ferramentas automatizadas permite cada vez mais a detecção de conteúdos potencialmente infratores, mas implica riscos de restrições de conteúdo tendenciosas e falsos positivos de negativos. A crescente dependência das ToS / Diretrizes de Comunidade como base para as decisões de restrição de conteúdo, paralelamente, fez crescer os papéis de definição de normas e de tomada de decisões dos provedores.

A fim de garantir que a moderação e as restrições dos conteúdos sejam proporcionais e conduzidas de forma responsável, especial atenção está sendo dispensada aos mecanismos de recurso que permitem aos usuários contestar uma decisão de restrição dos seus conteúdos. Nos últimos anos, surgiram novas abordagens em vários graus de desenvolvimento, nomeadamente:

- **Revisão independente estabelecida pela empresa** [Conforme detalhado nos Critérios Operacionais J - Recurso] - Algumas empresas exploram mecanismos para fornecer um recurso independente às suas decisões de restrição de conteúdo tomadas com base nas suas Diretrizes de Comunidade.

É entendido como um instrumento específico da empresa com autoridade vinculativa no terceiro nível de um processo gradual de tomada de decisões, na sequência de decisões em primeira instância e de uma etapa de reconsideração.

- **Revisão por conselhos nacionais de autorregulação** [Conforme detalhado nos Critérios Operacionais J - Recurso] Propõe-se a criação de organismos independentes de autorregulação (Conselhos de Mídias Sociais) nacionais para fornecer, entre outros, mecanismos de revisão das decisões de moderação de conteúdos tomadas pelos provedores.
- **Reexame por autoridades nacionais** - Alguns atores propuseram que determinadas autoridades públicas nacionais possam ter um papel formal na revisão das decisões de restrição de conteúdos tomadas pelos provedores. O parecer desses organismos seria vinculativo para a empresa e limitado geograficamente ao país.
- **Conselho Consultivo Global** - Finalmente, surgiram propostas para um conselho global com poder consultivo sobre os Termos de Serviço (ToS) e as Diretrizes de Comunidade das empresas, para aumentar a transparência e a accountability em relação a esta importante base normativa.

Nota: A lista acima não é exaustiva e não aborda nem prejulga o grau de apoio a nenhuma dessas propostas.

Interoperabilidade dos mecanismos de recurso

A recente multiplicação de iniciativas e abordagens aos mecanismos de recurso ilustra que os atores identificaram esta questão como importante e expressaram o desejo de abordá-la. Por outro lado, esta proliferação levanta grandes questões de interoperabilidade, a saber:

1. **Coerência da jurisprudência:** Como podem ser tratadas as situações em que uma decisão tomada no âmbito de um mecanismo de recurso contradiz as conclusões de outro? Os casos decididos desta forma devem ter impacto nos ToS /diretrizes de comunidade?
2. **Sobreposição:** Como evitar a duplicação de esforços? Em particular, se vários mecanismos separados considerarem a mesma decisão de restrição de conteúdo, qual a melhor forma de promover a coordenação?

3. **Responsabilidade civil:** De que forma uma decisão potencialmente concorrente ou complementar de vários mecanismos de recurso teria impacto na responsabilização dos provedores de serviços? Quais as consequências para a responsabilização dos provedores de serviços que decorrem de decisões contraditórias?
4. **Relações com os tribunais nacionais:** Como os mecanismos de recurso múltiplos podem interagir com os tribunais nacionais? Em especial, as decisões de mecanismos de recurso independentes poderão ser objeto de recurso junto aos tribunais nacionais?
5. **Respectivas responsabilidades dos atores:** Que papéis cada tipo de ator pode desempenhar nos vários mecanismos de recurso, para garantir que os direitos dos usuários sejam respeitados, que os processos permaneçam eficientes e que não serão criados encargos excessivos?

Todos os mecanismos de recurso que forem implementados abordarão parcialmente estas questões. No entanto, a menos que sejam estabelecidos arcabouços de coordenação e cooperação entre os atores, existem riscos significativos de que ações descoordenadas conduzam a consequências indesejadas, incluindo uma menor proteção dos direitos dos usuários, duplicação de esforços e custos elevados. Normas e critérios desenvolvidos em conjunto podem ajudar a estruturar as interações entre os vários mecanismos e garantir que a interoperabilidade seja incluída por padrão nas abordagens implementadas.

Benefícios esperados

A criação de um grupo específico no âmbito da Rede de Políticas Internet & Jurisdição, que reúna os diversos atores que abordam a questão dos mecanismos de recurso, poderá proporcionar os seguintes benefícios:

- Permitir que os atores que desenvolvem propostas de mecanismos de recurso aperfeiçoem seu projeto para garantir sua máxima utilidade. Atores relevantes podem dar e recolher avaliações em um espaço seguro e neutro, para garantir que as normas de accountability e transparência sejam respeitadas.
- Desenvolver normas e critérios sobre temas transversais que precisam ser abordados coletivamente. Estes podem ser introduzidos em iniciativas individuais para promover a interoperabilidade.

Próximos passos

A 3ª Conferência Global da Rede de Políticas Internet & Jurisdição, em Berlim, poderá discutir a validade desta proposta, o mandato potencial e a cronologia deste grupo, bem como formas de assegurar o envolvimento dos atores mais relevantes.


http://www

03.
Domínios e Jurisdição

Abordagens Operacionais
Normas, critérios, mecanismos

CONTEXTO

Lidar com o abuso no nível do DNS - o desafio

O sistema de endereçamento na Internet é essencial para o bom funcionamento da rede global que atualmente está na base da maior parte das atividades humanas. Os nomes de domínio asseguram uma conversão fácil entre as cadeias de identificação legíveis pelo ser humano e os longos e numéricos endereços IP (Protocolo de Internet) que indicam a localização de um determinado servidor na rede. O Sistema de Nomes de Domínio (DNS) é gerenciado[1] por um conjunto distribuído de operadores técnicos, formado principalmente por: Registros responsáveis pelos domínios de primeiro nível (ccTLDs e gTLDs[2]) e Registradores que distribuem domínios de segundo nível aos registrantes. A Corporação da Internet para Atribuição de Nomes e Números (ICANN) tem a missão[3] de "assegurar o funcionamento estável e seguro dos sistemas de identificadores únicos da Internet" e, em especial, de "coordenar o desenvolvimento e a implementação de políticas relativas ao registro de nomes de domínio de segundo nível em domínios genéricos de primeiro nível ("gTLD")".

Preservar a neutralidade da camada técnica é importante para garantir a confiança no DNS. Ao lidar com potenciais abusos, há uma distinção tradicional[4] entre abuso de registro e abuso de uso. O primeiro está "relacionado às atividades relacionadas a nomes de domínio básicos, executadas por registradores e registros", ao passo que o segundo "refere-se ao que um registrante faz com seu nome de domínio após a criação do domínio - a finalidade para a qual o registrante coloca o domínio e/ou os serviços que o registrante opera nele". Embora o primeiro seja inteiramente da competência da ICANN, o seu

---

1 Uma explicação mais detalhada desta arquitetura pode ser encontrada em: <https://whois.icann.org/en/domain-name-registration- process>

2 Os domínios de primeiro nível de código de país (ccTLDs) são extensões de duas letras, como .uk, .br ou .fr, correspondentes a países, de acordo com uma lista ISO; os domínios de primeiro nível genéricos (gTLDs) incluem os originais .com, .net, .org e agora mais de mil novos domínios introduzidos mais recentemente. Para mais informações sobre esta importante distinção, ver: <https://websapiens.eu/site/artile.php?aid=31&cid=26>

3 Ver: <https://www.icann.org/resources/pages/governance/bylaws-en/#article1>

4 Ver o relatório do grupo de trabalho sobre políticas de abuso de registro da gNSO da ICANN: <https://gnso.icann.org/sites/default/files/filefield>

estatuto indica que "a ICANN não regulamentará (ou seja, não imporá regras e restrições) os serviços que utilizam os identificadores únicos da Internet ou o conteúdo que esses serviços transportam ou fornecem".

No entanto, a pressão está aumentando para que se aproveite os nomes de domínio para mitigar atividades ou conteúdos ilegais em sites subjacentes. O abuso de utilização abrange duas dimensões: abuso técnico (por exemplo, phishing, distribuição de malware, etc.), que está estreitamente relacionado com a segurança e a estabilidade do DNS, e conteúdo abusivo (por exemplo, material de pornografia infantil, violações da propriedade intelectual, etc.). Os Registros e Registradores (Operadores de DNS) são muito diversos em termos de dimensão, atividades ou estruturas de governança. Além disso, a distinção fundamental entre código de país e TLD genéricos, em termos de relação com a legislação e as autoridades nacionais, conduz a abordagens e restrições muito diferentes ao receber pedidos diretos ou ordens para ação no nível do DNS relativamente ao abuso de utilização, especialmente quando têm origem transfronteiriça. Na ausência de um arcabouço geralmente aceito para lidar com o abuso de utilização, as práticas dos operadores de DNS variam consideravelmente.

Esta situação levanta duas questões fundamentais: 1) Quando pode ser adequado agir no DNS para resolver abusos? e 2) Quem deve ser responsável por tomar essa decisão?

Pertinência da ação no nível do DNS

Em princípio, dada a função neutra do DNS e a norma geral de proporcionalidade, o fato de uma suspensão de um domínio ter um impacto global por natureza exige um limiar elevado de atividade ou conteúdo abusivo para justificar tal medida. Um critério fundamental a ter em conta também é o envolvimento e a intenção reais do registrante no comportamento ou conteúdo infrator. Por último, independentemente dos tipos de danos, o bloqueio no DNS é uma ferramenta grosseira que não permite limitar o acesso a conteúdos específicos. Pode até mesmo ter uma eficiência limitada para impedir que os usuários tenham acesso ao recurso que pretendem alcançar (por exemplo, diretamente através do endereço IP). Outros atores, como os provedores de serviços de hospedagem, muitas vezes são mais capazes de dar uma resposta proporcional.

Tendo em vista o que foi exposto acima, os operadores de DNS estão mais inclinados a tomar medidas no DNS em resposta a abusos técnicos do que quando lidam com conteúdos abusivos, os quais normalmente não têm competência para avaliar adequadamente, dada a diversidade das legislações nacionais aplicáveis, a menos que o conteúdo tenha atingido um limiar claro de abuso.

Tomada de decisões

Por uma questão de segurança jurídica e de limitação da responsabilidade legal, os operadores de DNS preferem simplesmente cumprir decisões oficiais.

A este respeito, as decisões judiciais podem proporcionar garantias processuais e clareza da lei aplicável. Os operadores de DNS geralmente apenas obedecem – e normalmente até mesmo exigem - ordens de entidades jurídicas do país em que estão localizados, receando que a aceitação de ordens de tribunais estrangeiros incentive os governos a exercer autoridade extraterritorial de forma imprevisível. No entanto, as decisões judiciais nacionais relativas a um nome de domínio podem significar a imposição da legislação de um determinado país sobre os registrantes, atividades e usuários em todo o mundo, algo que pode conferir forte poder aos países onde muitos operadores estão localizados.

Neste contexto, os "notificadores" especializados autoestabelecidos, de vários tipos e estruturas, documentam os abusos percebidos e propõem acordos formais aos operadores de DNS. No entanto, não existe nenhum mecanismo externo de "credenciamento" para atestar a sua credibilidade e, atualmente, só detêm a autoridade que os operadores aceitam conferir-lhes. Os operadores de DNS podem utilizar vários fatores para decidir se devem celebrar um acordo com um notificador ou aceitar os seus pedidos, incluindo a sua estrutura e arcabouço de governança, os critérios explícitos e a base jurídica (nacional ou mais geral) em que se baseiam as suas avaliações, a sua neutralidade e potenciais conflitos de interesses e as garantias processuais que oferece. No entanto, o critério fundamental é a reputação ao longo do tempo: há quanto tempo o notificador tem estado ativo, sua trajetória no mercado e, mais importante ainda, se está disposto a defender suas notificações e apoiar o operador em caso de litígio.

Arcabouço de cooperação

Os diferentes atores reconhecem a dificuldade de abordar essas questões. Manifestaram interesse em trabalhar em conjunto para definir que condições estritas de atuação no DNS podem ser adequadas para lidar com abusos de uso, bem como regras e garantias processuais que possam ajudar a estabelecer a credibilidade dos notificadores especializados.

O trabalho do Grupo de Contato dedicado da Rede de Políticas Internet & Jurisdição, tal como apresentado neste documento "Abordagens Operacionais", visa a contribuir para esta discussão, abordando os elementos-chave de um arcabouço voluntário sobre as responsabilidades mútuas dos diferentes atores no que diz respeito às ações no nível do DNS.

Secretariado da Rede de Políticas Internet & Jurisdição

Mensagem do coordenador

A Internet nunca foi construída para tudo aquilo que é atualmente usada. Ela cresceu até se tornar uma rede de redes que facilita a interação econômica, social e científica em todo o mundo, sem fronteiras e praticamente independente de grandes distâncias. Essa rápida expansão nos desafia a adaptar a forma como nós e nossas sociedades trabalhamos, interagimos e nos organizamos.

A Rede de Políticas Internet & Jurisdição aborda uma das "consequências não intencionais" da Internet: como lidar com interações entre jurisdições, incluindo possíveis atividades criminosas ou prejudiciais transfronteiriças. É do interesse de todos os atores legítimos manter a Internet não só segura e estável, mas também segura e fidedigna para todos os seus usuários. É necessário encontrar um equilíbrio para permitir que as pessoas utilizem a Internet livremente e reconhecer e combater os abusos de uma forma proporcional e eficaz.

Isso vai além da missão de um ator ou de um setor isolado. O papel que os operadores do Sistema de Nomes de Domínio (DNS) podem e não podem razoavelmente desempenhar a esse respeito é de particular importância.

Em Paris, em 2016, a 1ª Conferência Global da Rede de Políticas Internet & Jurisdição iniciou um processo estruturado, reforçado após a 2ª Conferência Global, realizada em Ottawa, em fevereiro de 2018. Muitos debates frutíferos foram conduzidos em Grupos de Contato dedicados através de reuniões vir-

tuais e físicas ao redor do mundo. Estas discussões conduziram ao presente documento *Abordagens Operacionais*. Baseado na experiência prática real, ele fornece informações reais sobre o que faria sentido fazer, hoje, em caráter voluntário, para lidar com diferentes tipos de abusos.

Ao longo destes anos, todos os atores participaram em pé de igualdade e contribuíram generosamente com o seu tempo e experiência, em pleno respeito às opiniões e perspectivas de cada um. Foi um prazer e uma honra trabalhar com o Secretariado da Internet & Jurisdiction e com os Membros do Grupo de Contato, naquilo que eu acredito ser uma contribuição útil para a nossa compreensão do que podemos fazer juntos: soluções legais, escaláveis e razoáveis para usuários e provedores de serviços.

Penso que é justo dizer que todos aprendemos uns com os outros e que conseguimos dar um passo a diante. Os problemas estão longe de estarem resolvidos. No entanto, este passo, e mais passos como este, ajudarão a Internet - que não é boa nem má em si mesma - a ser utilizada da forma mais eficaz e segura para todos nós.

Maarten Botterman
Coordenador
Grupo de Contato do Programa Domínios e Jurisdição

Membros do Grupo de Contato do Programa Domínios e Jurisdição

O Secretariado nomeou um Coordenador neutro para facilitar o trabalho do Grupo de Contato:

Maarten Botterman
Diretor
Consultoria GNKS e Membro do Conselho Diretor da ICANN

As discussões nos Grupos de Trabalho, que ajudaram a realizar trabalhos concentrados em tópicos específicos, foram moderadas por Facilitadores neutros:

Susan Chalmers
Especialista em Políticas de Internet
Estados Unidos
Departamento de Comércio, NTIA

Brian Cimbolic
Vice-Presidente e Advogado Geral
Public Interest Registry

MEMBROS DO GRUPO DE CONTATO

Benedict Addis
Presidente, Registrar of Last Resort (RoLR)

Fiona Alexander
Administradora Associada
Estados Unidos,
Departamento de Comércio NTIA

Tijani Ben Jemaaa
Diretor Executivo
Mediterranean Federation of Internet Associations

James Bladel
Vice-Presidente de Políticas
GoDaddy

Maarten Botterman
Membro do Conselho Direto
ICANN

Jordan Carter
Diretor Executivo
InternetNZ

Mishi Choudhary
Diretora Jurídica, Software
Freedom Law Centre

Brian Cimbolic
Vice-Presidente e Advogado Geral
Public Interest Registry

Keith Drazek
Vice-Presidente
Políticas Públicas e Relações Governamentais
VeriSign

Heather Dryden
Assessora Sênior
Canadá
Departamento de Inovação
Ciência e Desenvolvimento Econômico

Rita Forsi
Diretora-Geral
Instituto Superior de Comunicações e Tecnologia da Informação
Itália
Ministério do Desenvolvimento Econômico

Jothan Frakes
Diretor Executivo
Domain Name Association (DNA)

Grace Githaiga
Co-convener
Kenya ICT Action Network (KICTANET)

Hartmut Glaser
Secretário-Executivo
Comitê Gestor da Internet no Brasil (CGI.br)

Rahul Gosain
Diretor
IRSME
Índia
Ministério de Eletrônica e Tecnologia da Informação

Rudolf Gridl
Chefe de Divisão
Governança da Internet
Alemanha
Ministério Federal para Assuntos de Economia e Energia

Rob Hall
CEO Momentous

Statton Hammock
Vice-Presidente de Política Global e Desenvolvimento Industrial
MarkMonitor

Byron Holland
Presidente e CEO
Canadian Internet Registry Authority (CIRA)

Will Hudson
Assessor Sênior de Políticas Internacionais
Google

Manal Ismail
Diretora Executivo
Coordenação Técnica Internacional
Egito
Autoridade Reguladora Nacional das Telecomunicações

Konstantinos Komaitis
Diretor Sênior
Estratégia e Desenvolvimento de Políticas
Internet Society

Marilia Maciel
Pesquisadora Sênior em Políticas Digitais
Diplo Foundation

Desiree Miloshevic
Assessora Sênior
Relações Internacionais e Políticas Públicas
Afilias

Paul Mitchell
Diretor Sênior
Políticas de Tecnologia
Microsoft

Cristina Monti
Assessora de Políticas
Fluxos e Proteção de Dados Internacionais
Comissão Europeia
DG JUST

Michele Neylon
CEO
Blacknight Internet Solutions

Seun Ojedeji
Engenheiro Chefe de Rede
Universidade Federal de Oye-Ekiti

Crystal Ondo
Vice-Presidente
Assuntos Corporativos
Donuts

Rod Rasmussen
Presidente
R2 Cyber

Bryan Schilling
Diretor de Proteção ao Consumidor
ICANN

Jorg Schweiger
CEO
DENIC

Geo Van Langenhove
Gerente Jurídico e Encarregado de Proteção de Dados
European Registry of Internet Domain Names (EURid)

Peter Van Roste
Diretor-Geral
Council of European National Top-Level Domain Registries (CENTR)

Chris Wilson
Gerente Sênior de Políticas Públicas (Governança da Internet)
Amazon Web Services

Além dos membros do Grupo de Contato, o Secretariado gostaria de agradecer aos seguintes atores pelo seu empenho nos debates realizados no âmbito do Grupo de Contato e dos seus Grupos de Trabalho.

Mohit Batra
Analista de Tecnologia
National Internet Exchange of India (NIXI)

Elizabeth Behsudi
Ex-Vice-Presidente e Advogada Geral
Registro de Interesse Público

Diego Canabarro
Assessor Especialista ao Conselho
Comitê Gestor da Internet no Brasil (CGI.br)

Brent Carey
Comissário para Nome de Domínio
New Zealand Domain Name Commission

Susan Chalmers
Especialista em Políticas de Internet
Estados Unidos
Departamento de Comércio NTIA

Gunther Grathwohl
Conselheiro
Alemanha
Ministério Federal para Assuntos de Economia e Energia

Allan Macgillivray
Assessor Sênior de Políticas ao Presidente
Canadian Internet Registration Authority (CIRA)

Polina Malaja
Assessora de Políticas
Council of European National Top-Level Domain Registries (CENTR)

Julie Michel
Consultora Jurídica
European Registry of Internet Domain Names (EURid)

David Payne
Vice-Presidente
Compliance, Afilias

Mathieu Potter
Analista de Políticas
Canadá
Departamento de Inovação, Ciência e Desenvolvimento Econômico

SÍNTESE DAS ABORDAGENS OPERACIONAIS

O documento *Abordagens Operacionais* a seguir é o resultado dos melhores esforços dos Membros do Grupo de Contato do Programa Domínios e Jurisdição para abordar as importantes questões identificadas no *Roteiro de Ottawa* da 2ª Conferência Global da Rede de Políticas Internet & Jurisdição, de 26 a 28 de fevereiro de 2018. O Plano de Trabalho que lá foi aprimorado identificou 11 importantes Questões Estruturantes para orientar ainda mais as interações do Programa Domínios e Jurisdição. As atuais *Abordagens Operacionais* são uma contribuição conjunta de alguns dos especialistas mais engajados nesse campo para o debate em andamento sobre as complexas questões de quando e como pode ser apropriado tomar medidas no nível do DNS para lidar com abusos. **No entanto, não devem ser entendidas como o resultado de uma negociação formal validada pelas organizações desses Membros**.

Assim sendo, os Membros do Grupo de Contato do Programa, com a ajuda do Secretariado, produziram o conjunto de Normas, Critérios e Mecanismos Operacionais propostos em anexo para fornecer um arcabouço comum de referência para os vários atores ao implementar ou desenvolver práticas voluntárias para lidar com abusos. Estas *Abordagens Operacionais* pretendem ajudar a educar o público em geral sobre as condições em que pode ser adequado agir no nível do DNS para resolver abusos técnicos e de conteúdos de websites, no pleno respeito aos princípios internacionais dos direitos humanos. Este documento também pode ajudar os tomadores de decisão públicos e privados a ter em conta toda a gama de parâmetros relevantes ao desenvolver e implementar arcabouços, regras e práticas responsáveis a este respeito.

Tendo em conta o pouco tempo disponível para abordar estas questões complexas, o trabalho dos Membros do Grupo de Contato do Programa foi distribuído em quatro Grupos de Trabalho temáticos, para propor, redigir e aperfeiçoar elementos que estão documentados de acordo com a estrutura tripartite apresentada na página 16.

Estas *Abordagens Operacionais* irão alimentar a 3ª Conferência Global da Rede de Políticas Internet & Jurisdição, a ser realizada entre 3-5 de junho de 2019 em Berlim, organizada em parceria com o Governo da República Federal da Alemanha, e institucio-

nalmente apoiada pelo Conselho da Europa, Comissão Europeia, ICANN, OCDE, CEPAL das Nações Unidas e UNESCO.

ESTRUTURA DAS ABORDAGENS OPERACIONAIS

O documento *Abordagens Operacionais* está organizado de acordo com a seguinte estrutura tripartite.

Normas operacionais

Esta seção identifica um conjunto de normas que podem ajudar a organizar o comportamento dos atores em suas próprias ações e interações mútuas. Concentram-se no nível operacional, no contexto dos princípios de alto nível existentes.

As Normas Operacionais de Domínios e Jurisdição identificam especificamente elementos relativos à pertinência da atuação no nível do DNS, mecanismos de notificação para Registros e Registradores (Operadores de DNS), ações adequadas e garantias processuais.

Critérios operacionais

Esta seção contém listas de elementos ou critérios que podem ser usados por todas as categorias de tomadores de decisão ao desenvolver, avaliar e implementar soluções. O objetivo é que todos os atores sejam capazes de discutir ideias, avaliar iniciativas e debater propostas usando arcabouços comuns de referência e questões estruturantes.

Os Critérios Operacionais de Domínios e Jurisdição abordam quatro temas importantes relacionados à pertinência da atuação no nível do DNS: (I) Nível de ação, incluindo os tipos de abusos relativamente aos quais poderá ser apropriado atuar no nível do DNS e os limiares correspondentes; (II) Avisos adequados, incluindo os componentes de um pedido completo, os tipos de notificadores e a devida diligência esperada dos notificadores; (III) Ações solicitadas, incluindo os possíveis tipos de ação que são disponíveis/aplicáveis no nível dos operadores de DNS; e (IV) Garantias processuais, incluindo transparência, critérios de orientação relativos à notificação dos registrantes e modalidades de recurso, se quiserem contestar as denúncias ou ações contra os seus nomes de domínio.

Mecanismo operacional

Esta terceira seção apresenta uma proposta para a qual os esforços de operacionalização poderão ser iniciados após a 3ª Conferência Global da Rede de Políticas Internet & Jurisdição, em Berlim.

A nota conceitual explora como uma interface para a comunicação de abuso, fácil de usar, poderia ser contemplada para enviar notificações devidamente documentadas aos destinatários certos, e como organizar melhor os próximos passos durante a 3ª Conferência Global e o trabalho de acompanhamento.

NORMAS OPERACIONAIS

Qualquer abordagem voluntária relativa a pedidos de ação no DNS para fazer face a abusos técnicos e de conteúdos deve abordar devidamente:

Nível de ação

Limiares - Critérios claros e limiares determinam quando a ação no DNS pode ser apropriada para lidar com abusos técnicos e de conteúdos.

Termos de Serviço (ToS) - Os ToS dos operadores de DNS descrevem claramente os tipos de abusos que estão dispostos a combater e os procedimentos aplicáveis para denunciá-los.

Avisos adequados

Destinatários - Quando se justifica uma ação no DNS, os Registradores devem ser os primeiros destinatários dos avisos de abusos, dado que a sua relação direta com o registrante permite uma ação eficaz.

Ponto(s) de Contato - Cada Operador de DNS indica de forma transparente e anuncia publicamente o(s) Ponto(s) de Contato para o qual os avisos devem ser endereçados.

Formatos - Componentes compartilhados para avisos facilitam a avaliação de sua completude, qualidade e relevância, auxiliando na estruturação de interações entre notificadores e operadores de DNS.

Substância - Os avisos individuais fornecem informações de apoio suficientes e prova de auditoria prévia para avaliar se o nível do alegado abuso justifica a ação solicitada.

Ações

Viabilidade técnica - As ações solicitadas devem ser tecnicamente implementáveis pelos Operadores de DNS, sendo fornecidas informações suficientes nos avisos para a sua execução, se consideradas justificadas.

Ação adequada - Entre todas as medidas possíveis, a ação aplicada é a mais razoável, em conformidade com as normas da necessidade e da proporcionalidade e tendo em conta potencial impacto colateral.

Reversibilidade - As ações implementadas são tão reversíveis quanto possível, para permitir a restauração do serviço DNS, se apropriado.

Garantias processuais

Devida diligência - Antes de alegar que um nome de domínio está associado a abuso, os notificadores conduzirão a devida diligência material e processual. Após o recebimento do aviso, os operadores de DNS procederão com devida diligência semelhante como parte de sua investigação.

Contrato do Notificador - Qualquer acordo contratual entre um Operador de DNS e um notificador especializado define suas respectivas responsabilidades e estabelece critérios claros para garantir o devido processo.

Respostas - Os Operadores de DNS acusam o recebimento de avisos e, quando emitidos por autoridades públicas, informam se alguma medida foi tomada.

Notificação - Os registrantes são notificados sobre os alegados abusos perante um Registrador ou um Registro que se mobiliza contra um nome de domínio. Para algumas alegações de abuso, quando isso não for possível, aconselhável ou mesmo permissível, a notificação é feita imediatamente após o fato, a menos que legalmente proibido.

Recurso - Os operadores de DNS e notificadores mantêm um processo publicamente identificável que permite que os registrantes contestem ou recorram de uma ação contra um nome de domínio após um aviso de abuso, fornecendo provas verificáveis que não exigem (ou pelo menos minimizam a necessidade de) que o operador de DNS interprete a lei.

CRITÉRIOS OPERACIONAIS

Os seguintes critérios representam os melhores esforços dos membros do Grupo de Contato do Programa Domínios e Jurisdição e seus Grupos de Trabalho, compilados pelo Secretariado I&J, na identificação de listas concisas de elementos que podem ser usados por todas as categorias de tomadores de decisão no desenvolvimento, avaliação e implementação de soluções. O objetivo é que todos os atores sejam capazes de discutir ideias, avaliar iniciativas e debater propostas usando arcabouços comuns de referência e questões estruturantes.

Os seguintes documentos devem ser entendidos como referência e base para futuros trabalhos na Rede de Políticas Internet & Jurisdição, após sua 3ª Conferência Global. Abaixo está a lista de Critérios Operacionais para o Programa Domínios e Jurisdição:

Parte I - Nível de Ação

- CRITÉRIOS A - Tipos de Abusos
- CRITÉRIOS B - Limiares

Parte II - Avisos adequados

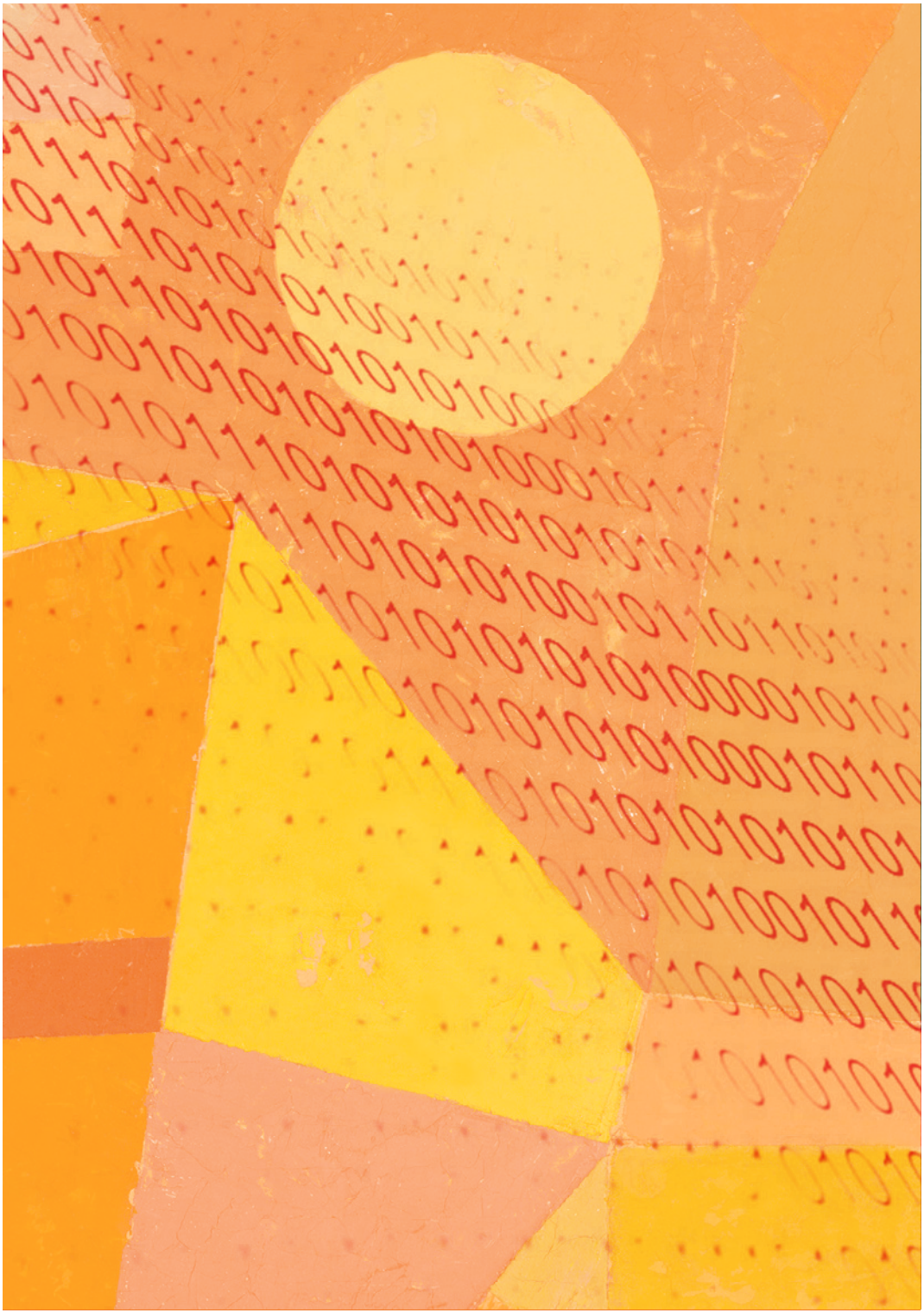
- CRITÉRIOS C - Componentes do Aviso
- CRITÉRIOS D - Tipos de Notificadores
- CRITÉRIOS E – Devida diligência dos Notificadores

Parte III - Ações

- CRITÉRIOS F - Tipos de Ações

Parte IV - Garantias processuais

- CRITÉRIOS G - Transparência
- CRITÉRIOS H - Notificação aos Registrantes
- CRITÉRIOS I - Recurso para os Registrantes



PARTE I - NÍVEL DE AÇÃO

Critérios A - Tipos de Abusos

Os operadores de DNS recebem pedidos transfronteiriços para tomarem medidas contra nomes de domínio alegadamente associados a abusos técnicos ou conteúdos problemáticos. Abaixo estão listadas descrições de diferentes tipos de abusos técnicos, bem como abusos de conteúdo de websites, para os quais os Registros e os Registradores frequentemente recebem tais pedidos[5].

1. Abusos técnicos

Os nomes de domínio podem ser indevidamente utilizados para propagar diferentes tipos de abuso técnico, incluindo, entre outros, os seguintes:

a. **Spam** é um e-mail em massa não solicitado e não autorizado pelo destinatário, cuja mensagem foi enviada como parte de uma coleção maior de mensagens, todas com conteúdo substancialmente idêntico[6]. O e-mail de spam pode conter malware e/ou ataques de phishing ou pharming.

b. **Malware** é um software malicioso, instalado em um dispositivo sem o consentimento do usuário, que interrompe as operações do dispositivo, coleta informações confidenciais e/ou obtém acesso a sistemas de computador privados. O malware inclui vírus, spyware, ransomware e outros softwares indesejados[7].

c. **Phishing** ocorre quando um agressor induz uma vítima a revelar informações pessoais, corporativas ou financeiras sensíveis (por exemplo, números de conta, IDs de login, senhas), seja enviando e-mails fraudulentos ou enganosos, de aparência "semelhante", ou atraindo usuários finais para sites mimetizados. Algumas campanhas de phishing visam a persuadir o usuário a instalar um software, que na verdade é um malware.

---

5 Estas listas são ilustrativas e não pretendem ser exaustivas.

6 Ver "The Definition of Spam" por The Spamhaus Project, em <https://www.spamhaus.org/consumer/definition/>

7 Ver M3AAWG & London Action Plan, Operation Safety-Net: best practices to Address Online Mobile and Telephony Threats (2015) ("Operation Safety-Net"), em <https://www.m3aawg.org/system/files/M3AAWG_LAP-79652_IC_Operation_Safety-Net_Brochure-web2-2015-06.pdf>; "Malware" page at the U.S. Federal Trade Commission website, at <https://www.consumer.ftc.gov/articles/0011-malware>

d. **Pharming** é o redirecionamento de usuários desavisados para sites ou serviços fraudulentos, normalmente através de sequestro (hijacking) ou envenenamento (poisoning) de DNS. O sequestro de DNS ocorre quando os agressores usam malware para redirecionar as vítimas para seu próprio site, em vez do inicialmente solicitado. O envenenamento do DNS faz com que um servidor DNS responda com um endereço IP falso contendo código malicioso[8]. O phishing é diferente do pharming porque o último envolve a modificação de entradas do DNS, enquanto o primeiro engana os usuários para inserir informações pessoais.
e. **Botnets** são conjuntos de computadores conectados à Internet que foram infectados por malware e instruídos a executar atividades sob o controle de um administrador remoto[9].
f. **Hospedagem de fluxo rápido** é usada para disfarçar a localização de sites ou outros serviços de Internet, ou para evitar esforços de detecção e mitigação, ou para hospedar atividades ilegais. As técnicas de fluxo rápido usam o DNS para mudar frequentemente a localização na Internet à qual o nome de domínio de um provedor de hospedagem ou servidor de nomes da Internet está relacionada[10].

2. Abusos de conteúdo de website

A maioria dos operadores de DNS lida com pedidos de tratamento de conteúdos problemáticos de sites da Internet de forma diferente dos abusos técnicos. Uma vez que os Registros e Registradores (quando não funcionam também como provedores de hospedagem) não podem eliminar partes ofensivas de conteúdos de um site, na maior parte dos casos não é adequado agir no nível do DNS. A reparação de conteúdos problemáticos deve ocorrer ao nível do registrante ou do provedor de hospedagem na Web.

---

8 Ver Política Antiabuso de Nomes de Domínio do Registro de Interesse Público, em <https://pir.org/policies/org-idn-policies/anti-abuse- policy/>; definições de DNS hijacking e DNS poisoning na Kaspersky Lab Encyclopedia, at <https://encyclopedia.kaspersky.com/glossary/dns-hijacking/>

9 Ver "A Glossary of Common Cybersecurity Terminology," National Initiative for Cybersecurity Careers and Studies, em: <https://niccs.us-cert.gov/about-niccs/glossary#B>

10 Ver a Política Antiabuso de Nomes de Domínio do Registro de Interesse Público, em <https://pir.org/policies/org-idn-policies/anti-abuse-policy/>

As descrições abaixo provêm de diversas fontes, inclusive dos comentários dos membros do Grupo de Contato. Elas não são nem pretendem ser interpretadas como descrições normativas. Alguns tipos de conteúdos problemáticos apresentam um grau mais elevado de acordo compartilhado entre jurisdições do que outros.

a. **Material de abuso infantil** consiste em fotografias ou vídeos feitos por um agressor, documentando o abuso sexual de uma criança[11].
b. **Substâncias controladas** e bens regulados para venda ou comércio incluem drogas ilegais, a venda ilegal de drogas legais, serviços ilegais, mercadorias roubadas e armas de fogo ou outras armas ilegais. A legalidade de uma determinada substância ou bem varia consoante às jurisdições.
c. **Conteúdo extremista violento** inclui conteúdo que retrata violência explícita, encoraja a ação violenta, endossa uma organização terrorista ou seus atos, ou encoraja as pessoas a se juntar a tais grupos.
d. **Discurso de ódio** inclui a defesa do ódio nacional, racial ou religioso que constitui incitação à discriminação, hostilidade ou violência[12].
e. Pedidos de suspensão de nomes de domínio relacionados com **propriedade intelectual** em resposta ao conteúdo do website (não relacionados com o próprio nome de domínio) foram emitidos com base em pretensas marcas registradas (por exemplo, venda de produtos falsificados), violação de patentes ou segredos comerciais ou pirataria de obras protegidas por direitos de autor. Como em todas as categorias acima, as leis relativas à propriedade intelectual diferem entre jurisdições.

---

11 Interpol, "Online child abuse material: Q&A" (Janeiro de 2017). <https://www.interpol.int/Media/Files/Crime-areas/Crimes- against-children/Online-Child-Abuse-%E2%80%93-Questions-and-Answers/>

12 O Pacto Internacional sobre os Direitos Civis e Políticos (adotado em 16 de Dezembro de 1966, entrou em vigor em 23 de Março de 1976) 999 UNTS 171 (ICCPR), Art. 20(2), disponível em <https://www.ohchr.org/EN/ProfessionalInterest/Pages/PIDCP.aspx>

Critérios B - Limiares

1. Abuso técnico

A ação no nível do DNS é geralmente justificada em situações de abuso técnico, a fim de proteger a estabilidade e a segurança da infraestrutura global da Internet. No entanto, justificam-se medidas adicionais específicas para ajudar o registrante se o domínio for obviamente comprometido por terceiros sem o seu conhecimento.

2. Conteúdo abusivo

Por outro lado, dado o impacto geograficamente global de uma ação no DNS, a ação em relação a conteúdos abusivos só se justifica se for atingido um limiar particularmente elevado de abuso/danos, no que se refere a, entre outros aspectos:

a. Grau de consistência normativa global[13] em relação ao alegado abuso: ou seja, se o conteúdo em questão é considerado ilegal em um número suficiente de jurisdições;
b. Proporção do site efetivamente dedicada ao conteúdo infrator;
c. Demonstrada intenção ou má-fé do registrante, e
d. Falta de medidas alternativas disponíveis para remediar a situação.

13 Ver documento Conteúdo e Jurisdição Abordagens Operacionais, Critérios Operacionais B - Base Normativa

PARTE II - AVISOS ADEQUADOS

Critérios C - Componentes do Aviso

Os operadores do DNS recebem frequentemente avisos de abuso numa grande diversidade de formatos que, muitas vezes, não contêm informações suficientes para investigação e ação. Por conseguinte, o quadro abaixo propõe uma lista de componentes que os bons avisos devem conter para facilitar as interações entre os emissores e os operadores do DNS.

IDENTIFICAÇÃO	
Número ID da solicitação	Referência fornecida pelo emissor do pedido.
Tempo	Data ou carimbo com data e hora precisos correspondente à emissão do pedido.
Entidade emissora	Natureza e identificação precisa do requerente: tribunal,autoridade judiciária, notificador, representante legal de um denunciante.
Registrador requerido	Nome do Ponto de Contato (POC) para abusos do Registrador que administra o registro.
Registro relevante	Registro que administra a extensão TLD correspondente (para informação).
CASO	
Elementos comprobatórios	Abuso de segurança e estabilidade ou conteúdo abusivo (da lista de taxonomia).
Proporcionalidade	Documentação factual do abuso alegado.
Base jurídica	Fundamento que justifica que o abuso alegado atinge o limiar de intervenção exigido.
DEVIDA DILIGÊNCIA	
Avaliação	Medidas tomadas pelo notificador privado – antes do envio da notificação ao operador de DNS - para determinar a realidade e a extensão do abuso, em relação às normas previamente acordadas e à(s) lei(s) aplicável(is).
Medidas prévias	Medidas tomadas pelo notificador privado - antes do envio da notificação ao operador de DNS - para contatar o registrante e solicitar a cessação do abuso (quando aplicável).

AÇÃO SOLICITADA	
Domínio(s) visado(s)	Nome(s) de domínio(s) específico(s) sobre o(s) qual(is) a ação é solicitada, identificado(s) através do(s) URL(s) específico(s) onde ocorre o alegado abuso.
Ação intentada	Indicação da ação específica solicitada (ver critérios F - Tipos de Ações) e fornecimento de informações relevantes para a sua execução técnica.
PRAZOS	
Prazo fixado	Quando as ações devem ser executadas (item especialmente importante no caso de ações combinadas ou de emergência).
Período	Duração da ação solicitada (se aplicável).
Emergência	Esta ação se justifica por uma emergência específica (natureza da emergência)?
Fundamentação para a emergência	Esclarecimento da relação entre a ação solicitada e a emergência e a forma como a emergência será evitada.
CONFIDENCIALIDADE	
Confidencialidade	Pedido para não notificar o registrante antes da ação ou potencialmente até mesmo "ex post" por um período de tempo (se aplicável).
Fundamentação para a confidencialidade	Justificativa adequada para tal confidencialidade.
Prazo da confidencialidade	Prazo para ausência de notificação.
AUTORIDADE	
Autenticação	Informações que permitam verificar a identidade da autoridade pública requerente e a autenticidade do aviso.
Certificação	Autocertificação por escrito, feita pelo notificador privado, atestando sua autoridade, a realização de devida diligência prévia e a exatidão das suas declarações.
CONTATOS	
Entidade emissora	Dados de Contato da entidade requerente, à qual deve ser enviada a notificação da ação (ou não ação).
ASSINATURA	

Critérios D - Tipos de Notificadores

1. Ordens da jurisdição do operador de DNS

Os operadores de DNS podem ser legalmente obrigados a cumprir ordens judiciais da sua jurisdição (incluindo ordens estrangeiras que tenham sido "internacionalizadas"). No entanto, as autoridades competentes devem exercer esta autoridade de forma responsável para evitar impor desproporcionalmente a sua legislação nacional aos conteúdos produzidos e alojados legalmente em outras partes do mundo (ver Critérios Operacionais B - Limiares).

2. Outras fontes de notificações

a. Os tribunais fora da jurisdição onde o operador de DNS está constituído podem emitir notificações transfronteiriças para ação no nível do DNS. Embora não sejam diretamente executáveis per se, os operadores de DNS podem, no âmbito dos seus termos de serviço, tomar medidas à luz dos procedimentos seguidos localmente e da sua própria investigação dos fatos de que dispõem.
b. Notificadores especializados representando interesses públicos ou específicos emitem notificações para Operadores de DNS. Estes últimos determinam, após investigação, se devem ou não tomar medidas, com base na demonstração do nível exigido de devido processo e da devida diligência realizada e da sua relação preexistente com o notificador (contratual ou outra).
c. As pessoas em causa enviam avisos através dos Pontos de Contato para abusos dos operadores de DNS, a fim de chamar sua atenção para os abusos que, em sua opinião, devem ser combatidos no nível do DNS.

Critérios E – Devida Diligência dos Notificadores

1. Princípio geral

As pessoas ou entidades que apresentarem queixas ou notificarem abusos (notificadores) aos Registradores e aos Registros de nomes de domínio devem garantir que procederam à devida diligência (tanto material quanto processual) antes de alegar que um nome de domínio é objeto de abusos, quer no DNS/abuso técnico (abusos de segurança e estabilidade), quer no contexto de queixas relativas a conteúdos (abusos de conteúdo de sites da Web).

2. Considerações operacionais

a. Devida diligência material

A devida diligência material deve garantir que qualquer reclamação contra

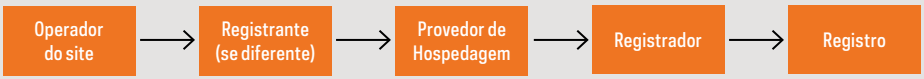
o conteúdo de qualquer domínio seja devidamente investigada, fundamentada e documentada (por exemplo, capturas de tela, listagem em qualquer lista negra, prova de propriedade em alegações de violação). Um notificador deve garantir que efetuou a devida diligência material antes de emitir um aviso.

b. Devida diligência processual

A devida diligência processual envolve uma hierarquia (ver Quadro 1 abaixo) na maneira como o aviso deve ser feito.

Em caso de abuso técnico, os avisos devem ser feitos diretamente ao Registrador e ao Registro. Nos casos de reclamações de conteúdo, a mitigação no DNS é uma reparação imperfeita. Por conseguinte, os avisos devem seguir a seguinte ordem:

QUADRO 1
Vias adequadas de encaminhamento de reclamações de conteúdo



Atualmente, alguns notificadores de queixas relativas a conteúdos apresentam as suas queixas diretamente ao Registro ou ao Registrador. Isto pode gerar problemas de proporcionalidade.

i. Utilizando o exemplo de um site de compartilhamento de arquivos, se um Registrador ou Registro suspender todo o domínio devido a uma alegação relativa a um número limitado de conteúdos infringentes ou ofensivos, milhares de outros conteúdos legítimos poderão ficar inacessíveis não só para o registrante, mas também para os usuários finais.
ii. O operador do website, o registrante ou o provedor de hospedagem, no entanto, podem impactar e provavelmente remover os casos limitados de conteúdos abusivos, deixando o conteúdo restante (bem como o nome de domínio) inalterado.

Assim, no caso de queixas relativas a conteúdos, o notificador deve primeiro tentar trabalhar com o operador do site, o registrante e o provedor de hospedagem para que os conteúdos específicos sejam removidos. Se nenhum desses atores agir ou retirar o conteúdo, o notificador poderá encaminhar a questão para o Registrador ou para o Registro (esse encaminhamento continuará sujeito à aplicabilidade de qualquer utilização aceitável ou política semelhante).

Critérios F - Tipos de Ações

A proteção do núcleo central da Internet é e deve ser uma prioridade fundamental. O DNS - parte do núcleo da Internet - é um sistema de endereçamento. Trata-se de uma camada neutra e técnica, vital para o bom funcionamento da Internet. A ação na camada do DNS não é uma forma totalmente eficaz - nem deve ser considerada como a ferramenta natural - para lidar com abusos técnicos ou conteúdos problemáticos.

A atuação no nível do DNS deve ser considerada apenas quando for possível determinar de forma confiável que o próprio domínio é usado com a intenção clara de conduta abusiva significativa. Além disso, uma vez que a suspensão de um domínio tem, por definição, um impacto global, a proporcionalidade exige que apenas um nível particularmente elevado de abuso e/ou dano possa potencialmente justificar recorrer a tal medida. É importante que o impacto de uma ação específica no nível do DNS seja bem compreendido.

Os pedidos de suspensão de nomes de domínio devem ser dirigidos, em primeira instância, às partes que estão mais próximas da atividade abusiva, inclusive por relação contratual (ver Quadro 1, Critérios E – Auditoria Jurídica dos Notificadores, para mais detalhes). Por exemplo, os solicitantes devem primeiro tentar contatar o registrante do nome de domínio e, em seguida, o provedor de hospedagem (um ou ambos podem ser o infrator), pois essas partes têm a relação mais direta com o conteúdo do site[14]. A ação direta dos registrantes ou provedores de hospedagem minimiza o impacto potencial no funcionamento do DNS. Se essas tentativas não forem bem-sucedidas, os solicitantes devem considerar as opções abaixo. A seguir enumeramos os diferentes

14 Ver CENTR, Domain name registries and online content (Jan 30, 2019), disponível em: <https://centr.org/library/library/centr- document/domain-name-registries-and-online-content.html> descreve relações entre os vários atores envolvidos com um website com conteúdo abusivo).

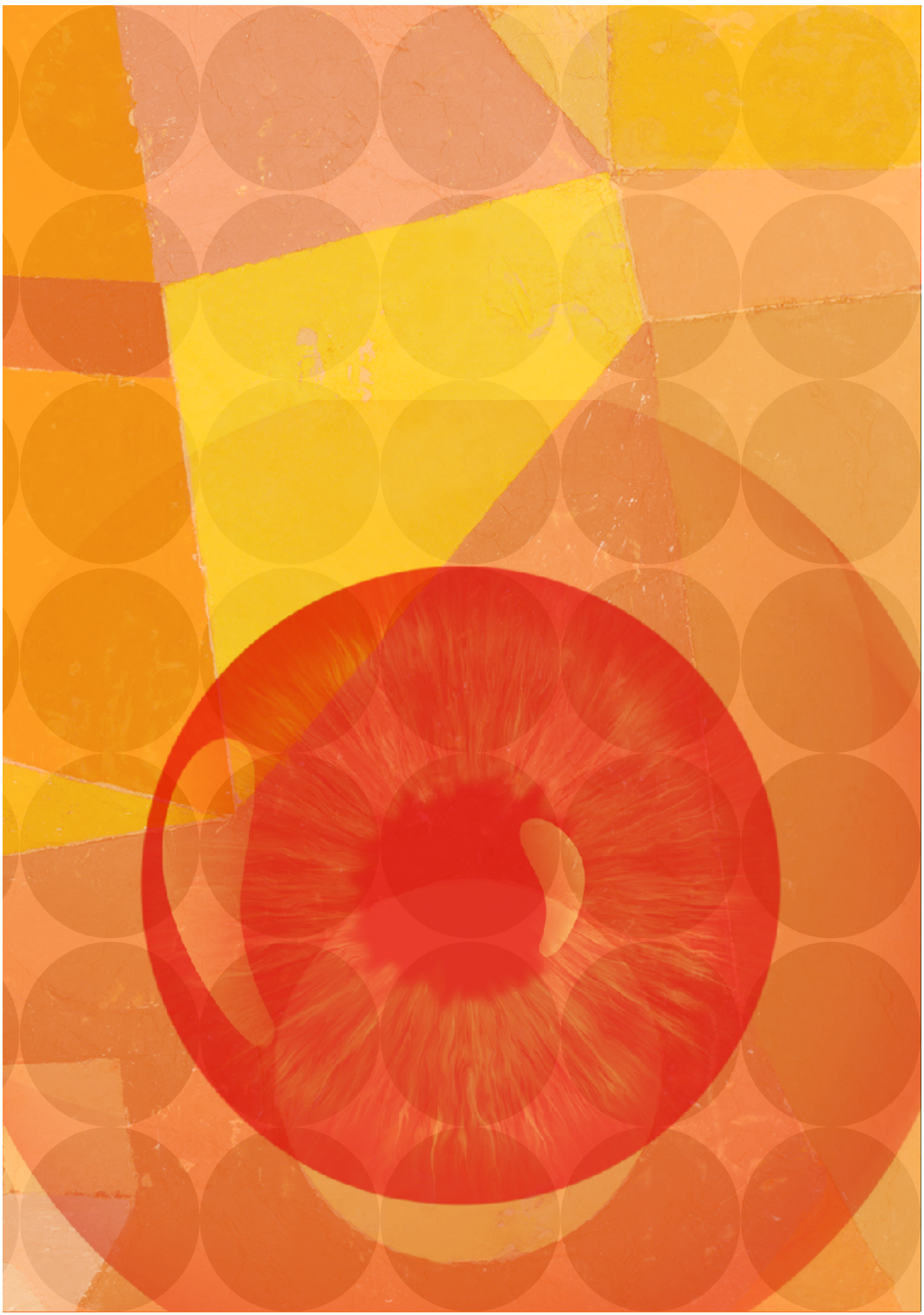
tipos de ações que os operadores de Registro e os Registradores podem empreender, conforme adequado, em resposta a pedidos de suspensão transfronteiriços[15].

Observe que a disponibilidade de qualquer ação abaixo pode variar de acordo com os provedores.

1. Para os Registros: **Remeter o pedido de suspensão ao Registrador** que tem a relação contratual com o Registrante do nome de domínio.
2. **Suspender** o nome de domínio para impedir a resolução do nome no DNS. Isso remove o nome de domínio do arquivo de zona do TLD, para que o nome de domínio não seja mais ativo na Internet pública. No caso de o pedido ter sido feito por engano, esta ação pode ser anulada.
3. **Bloquear** o nome do domínio para que ele não possa ser alterado. Um domínio bloqueado não pode ser transferido, excluído ou ter seus dados modificados, mas ainda assim estará ativo na Internet.
4. **Redirecionar** os serviços de nomes para o nome de domínio. Um registro tem a capacidade técnica de alterar os servidores de nomes de domínio. Ao alterar os servidores de nomes para o nome de domínio, os serviços associados ao nome de domínio podem ser redirecionados para "sink-holing" (registro de tráfego), para identificar vítimas para fins de compensação.
5. **Transferir** o nome de domínio para um Registrador devidamente qualificado pode impedir a exploração, permitindo simultaneamente a gestão do ciclo de vida, dos códigos de status EPP e da expiração.
6. **Eliminar** o nome de domínio. A supressão é uma ação extrema e não é geralmente recomendada sem a devida diligência e orientação das autoridades competentes. Restaurar um nome de domínio, se a supressão for considerada inadequada, pode envolver encargos adicionais que não se manifestam quando se suspende um nome de domínio. A exclusão geralmente não é tão eficaz na mitigação de abusos quanto a suspensão, pois um registrante é livre para registrar novamente o nome de domínio depois que ele for removido da zona.

---

15 Essas ações foram adaptadas de ICANN's Framework for Registry Operator to Respond to Security Threats, disponível em <https://www.icann.org/resources/pages/framework-registry-operator-respond-security-threats-2017-10-20-en>. (citações internas omitidas).



PARTE IV - GARANTIAS PROCESSUAIS

Critérios G - Transparência

Uma abordagem bidimensional pode ajudar a melhorar a transparência:

1. **Estatística**
   Além das métricas atualmente usadas para medição de desempenho, os operadores de DNS seriam encorajados a desenvolver métricas para a coleta e geração de relatórios, em formatos exportáveis e acessíveis, estatísticas coerentes referentes a notificações de abuso e ações implementadas. As autoridades públicas e os notificadores especializados devem igualmente desenvolver mecanismos para assegurar a rastreabilidade das suas notificações.

2. **Tomada de decisão**
   Os operadores de DNS documentam e disponibilizam ao público os critérios que determinam quando é adequada uma ação no nível do DNS, os tipos de conteúdos abusivos contra as quais estão dispostos a tomar medidas e o(s) seu(s) Ponto(s) de Contato para abuso(s). Também documentam e divulgam seus critérios internos de tomada de decisão e os canais de apelação/recurso. Os notificadores especializados também documentam e disponibilizam ao público os seus critérios de avaliação de abusos, bem como as suas regras para devida diligência e garantias processuais.

Critérios H - Notificação aos Registrantes

1. **Princípio geral**
   Os Registrantes devem, em geral, receber notificações de alegados abusos perante um Registrador ou um Registro que atue contra um nome de domínio. Há, no entanto, algumas alegações de abuso em que isso não é possível, aconselhável ou mesmo permissível e, nesses casos, a menos que legalmente proibido, deve ser feita notificação após o fato.

2. Considerações operacionais

a. Notificação ao Registrante antes da ação

Se um Registro ou Registrador receber alegações de violação de direitos de autor, alegações de difamação, casos em que se possa inferir que o conteúdo é ilegal ou fraudulento, mas que não podem ser comprovados sem uma investigação mais profunda[16] (geralmente, "queixas relativas ao conteúdo"), a notificação ao Registrante deve ocorrer antes que um operador de DNS tome medidas no domínio.

b. Notificação ao Registrante após a ação

Se um Registro ou Registrador receber alegações de abuso técnico do DNS ("abuso técnico"), ordens judiciais de jurisdição(ões) competente(s), ou alegações de abuso, de acordo com o estabelecido nas políticas ou procedimentos aplicáveis do Registrador ou do Registro, a notificação ao Registrante pode ocorrer após o fato[17].

c. Quem fornece a notificação?

Entre o Registrador e o Registro, os Registradores são o operador preferido para encaminhar as notificações aos Registrantes. Os Registradores geralmente têm uma relação contratual e comercial mais próxima com o Registrante, e o Registrador coleta as informações do Registrante. Muitos Registros de ccTLDs têm relações contratuais ou comerciais diretas com o Registrante e podem estar em posição semelhante para fornecer notificações.

Os Registros de gTLDs normalmente (mas nem sempre) fornecem notificações aos Registradores, que devem trabalhar com o Registrante para corrigir o alegado abuso. Em situações sem mandato judicial, as notificações de abuso são normalmente enviadas ao Registrador, o qual deverá, então, trabalhar com o Registrante em um prazo limitado (por exemplo, 48 horas) para corrigir o alegado abuso.

---

16 Isto pressupõe que as várias categorias de conteúdo estão dentro do escopo dos Termos de Serviço do Registro ou Registrador, das Políticas de Uso ou Anti Abuso ou outros termos ou políticas similares. Se o conteúdo estiver fora do escopo de tais termos, nenhuma notificação será normalmente fornecida e o domínio não será acionado.

17 Há também casos em que um operador de DNS não pode fornecer qualquer notificação (por exemplo, quando uma ordem judicial exige um tratamento confidencial ou após ponderar considerações relevantes em matéria de execução da lei).

d. Conteúdo do aviso

Na maioria dos casos, apenas as informações necessárias para informar a investigação e a reparação do alegado abuso por parte do Registrante devem constar da notificação. Em alguns casos, todo o encaminhamento pode ser transmitido (por exemplo, em casos de alegada infração aos direitos de autor, se tal se inserir no âmbito dos termos das partes relevantes).

Critérios I - Recursos Disponíveis aos Registrantes

1. Princípios gerais

Os Registradores e os Registros devem manter um processo publicamente disponível (mesmo que informal) para permitir que um Registrante conteste ou recorra de uma ação contra um nome de domínio por abuso técnico ou por queixa relativa a um conteúdo. Qualquer recurso deve incluir provas verificáveis de forma independente que não exijam (ou pelo menos minimizem a necessidade de) que o Operador de DNS interprete a lei, o que geralmente está fora da área de conhecimento do Operador de DNS.

2. Considerações operacionais

a. Processo

A Política Anti Abuso /Política de Uso Aceitável de Registros e Registradores deve esclarecer a forma como esse recurso pode ser interposto.

i. Pode ser algo como: "Para questões relativas a ações tomadas em conformidade com esta política, favor contatar [abuse@example.example ou review@example.example]".

O processo estará disponível para ações, salvo aquelas realizadas em virtude de uma ordem judicial da jurisdição do Operador de DNS. Se a ação foi tomada em conformidade com uma sentença de um tribunal com jurisdição sobre o operador de DNS, nenhum processo interno do operador de DNS poderá anular tal ordem.

O operador de DNS deve realizar a devida diligência adequada e completa antes que a ação no domínio seja efetivada. Isso deve evitar a necessidade de muitas idas e vindas com o Registrante ao longo do processo.

b. Provas apresentadas

Registros e Registradores não são tribunais de jurisdição

competente, nem especialistas na interpretação das várias leis aplicáveis. Assim, qualquer prova apresentada por um registrante/requerente deve ser verificável de forma independente e não deve exigir (ou pelo menos minimizar a necessidade de) que o Operador de DNS interprete a lei. Para que um operador de DNS possa reverter sua decisão em tal recurso, as provas devem ser irrefutáveis e objetivas. É importante dispor de um mecanismo desse tipo em caso, por exemplo, de erro do operador de DNS ou de provas irrefutáveis fornecidas contra a acusação do notificador.

c. **Ação de reversão em relação ao abuso técnico**
   Há menos "espaço de manobra" na avaliação de abuso técnico do que na avaliação de conteúdo abusivo. No caso de um domínio envolvido em phishing ou na distribuição de malware que tenha sido identificado como tal, a prova clara de um limiar elevado deve ser suficiente para permitir a reversão de uma suspensão, a menos que o domínio tenha sido comprometido.
   i. Se um registrante for capaz de demonstrar que o domínio foi comprometido sem o seu conhecimento, o operador do DNS poderá considerar tal prova.
   ii. Outro exemplo em que um operador de DNS reverte uma decisão por abuso técnico seria devido a um erro do operador de DNS, como a suspensão do nome de domínio errado (exemplo1.exemplo em vez de exemplo11.exemplo), ou se um domínio foi retirado de uma lista de bloqueio na qual se baseou antes da suspensão.

d. **Ação de reversão em relação ao abuso de conteúdo do website**

Neste caso há mais espaço para interpretação do operador de DNS sobre reclamações de conteúdo, mas qualquer prova apresentada deve ser passível de ser verificável de modo independente e não deve exigir, ou pelo menos minimizar, a necessidade de o operador de DNS interpretar a lei.

Se um registrante recorrer de uma ação que um operador de DNS tomou em virtude da sua confiança ou trabalho com terceiros (por exemplo, um notificador especializado), o operador e o notificador do DNS devem dispor de um processo através do qual o notificador possa avaliar de forma independente as provas compensatórias e estar disposto a reverter sua recomendação.

MECANISMO OPERACIONAL
INTERFACE PARA COMUNICAÇÃO DE ABUSOS AOS OPERADORES DE DNS

Contexto

Todos os atores têm um interesse comum de que os conteúdos efetivamente abusivos possam ser comunicados ao operador de DNS correto, com informações e justificativas suficientes para permitir a tomada de decisões e a adoção de medidas proporcionais, quando for justificado agir no nível do DNS. No entanto, existem dois desafios em termos de:

- Identificação do destinatário: Encontrar o Ponto de Contato para Abuso para enviar um aviso exige que se compreenda como funciona o sistema de nomes de domínio, incluindo as diferenças entre Registros e Registradores e entre domínios de primeiro nível genéricos e de códigos de país. Também é necessária uma conscientização da existência do WHOIS e de serviços equivalentes no espaço de ccTLDs.
- Ação legítima: Nem as condições em que é aceitável agir no nível do DNS nem o tipo de ações proporcionais são suficientemente compreendidas. Como resultado, frequentemente falta uma justificativa adequada e as ações solicitadas podem não ser tecnicamente viáveis.

Os avisos mal formulados, incompletos ou sem justificativa suficiente, enviados para o destinatário errado, são onerosos para os operadores de DNS e criam ineficiências. Além disso, medidas para combater abusos reais podem não ser tomadas. A educação é importante para abordar esta questão, mas exige um esforço maciço. Poder-se-ia discutir algo simples e este é o propósito desta nota conceitual.

Neste contexto, é importante notar que poderiam ser utilizados alguns elementos básicos para uma solução:

- Para gTLDs, o Contrato de Credenciamento de Registradores contém disposições específicas (RAA 3.18), que impõem a cada Registrador: "manter um Ponto de Contato para receber denúncias de abuso", cujo endereço de e-mail "deve ser publicado na página inicial do Registrador".
- O serviço WHOIS (independentemente das mudanças no seu nome e da implementação do GDPR) já contém cam-

pos correspondentes ao e-mail e número de telefone do Registrador em questão para denúncias de abuso.
- O trabalho no contexto do Grupo de Contato do Programa Domínios e Jurisdição joga alguma luz sobre quando a ação no nível do DNS pode ser apropriada e os formatos para avisos adequados.

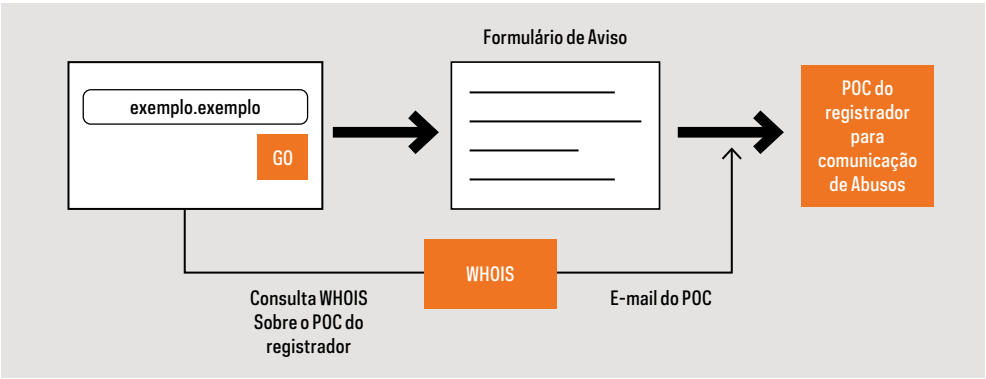
Ideia de uma interface para a comunicação de abusos

Uma "interface de comunicação de abusos" fácil de usar permitiria o envio de avisos devidamente documentados ao destinatário certo, por meio de:

- uma consulta WHOIS direcionada (para obter o campo "e-mail do ponto de contato para abuso"), e
- um formulário pormenorizado para introduzir os dados técnicos e a justificativa da notificação de abuso.

Um notificador introduziria o nome de domínio visado, preencheria o formulário pertinente e ordenaria o seu envio ao agente de registro, conforme ilustrado no infográfico (altamente simplificado) abaixo.

Isso parece tecnicamente simples de implementar para gTLDs. No entanto, isso exigiria trabalho adicional que fosse voluntariamente expandido no espaço de ccTLDs.



Utilizar as informações já recolhidas através do serviço WHOIS reduz o peso de manter a exatidão dos registros, comparado à criação de uma base de dados de Pontos de Contato inteiramente nova e dedicada.

Benefícios esperados

Esta abordagem poderá proporcionar os seguintes benefícios:

- Assegurar a simplicidade de utilização para uma gama de notificadores e um elevado nível de justificativa das notificações.
- Estabelecer algum "atrito" (por exemplo, através de campos obrigatórios num formulário) para evitar o abuso do próprio sistema de notificação e a correspondente sobrecarga.
- Esclarecer os canais de interação entre os notificadores e os operadores de DNS, de forma interoperável.
- Proporcionar a oportunidade para educar os notificadores sobre: os critérios que devem ser cumpridos para justificar uma ação no nível do DNS, qual o operador de DNS adequado para interagir com eles e as garantias processuais (incluindo a devida diligência prévia) que lhes são aplicáveis (ver Critérios E – Devida Diligência pelos Notificadores).

Serviços adicionais poderiam ser construídos em torno de tal interface, incluindo:

- Informar o registro relevante sobre uma notificação relativa a um dos seus domínios, se for caso
- Coletar estatísticas úteis para a elaboração de relatórios de transparência.

Esta abordagem também pode contribuir para um debate mais abrangente sobre o conceito de "acessibilidade", ou seja, as condições em que um Registrador pode potencialmente enviar uma notificação a um Registrante (sem revelar seus detalhes). Isso poderá permitir, principalmente, que um notificador efetue diligências prévias.

De modo geral, o anúncio da disposição de se contemplar esse serviço representaria uma comunicação pública positiva por parte da comunidade de Registros e Registradores - ou, pelo menos, da sua parte mais empenhada - sobre o seu compromisso de combater os abusos de um modo responsável, tendo simultaneamente presente a necessária proteção da neutralidade do DNS.

Próximos passos

A 3ª Conferência Global da Rede de Políticas Internet & Jurisdição, em Berlim, poderá discutir esta proposta, o mandato potencial e o cronograma de tal grupo, bem como formas de garantir o envolvimento dos atores mais relevantes.

04.
Anexo
Roteiro de Berlim

Resumo do Secretariado e Planos
de Trabalho dos programas da I&J

REDE DE POLÍTICAS INTERNET & JURISDIÇÃO

De 3 a 5 de junho de 2019, quase 300 participantes de alto nível, membros de governos, das principais empresas de Internet do mundo, operadores técnicos e representantes da sociedade civil, academia e organizações internacionais de mais de 50 países se reuniram em Berlim, Alemanha, durante a 3ª Conferência Global da Rede de Políticas Internet & Jurisdição[1]. Após a França (2016) e o Canadá (2018), a 3ª Conferência Global teve o Governo Federal da Alemanha como anfitrião, e apoio institucional de seis organizações internacionais: Conselho da Europa, Comissão Europeia, ICANN, OCDE, CEPAL das Nações Unidas e UNESCO.

A Conferência foi um marco importante na abordagem dos principais desafios jurídicos transfronteiriços do século XXI digital. As partes interessadas apreciaram os documentos *Abordagens Operacionais*[2] produzidos nos três Programas da Rede de Políticas Internet & Jurisdição: Dados e Jurisdição, Conteúdo e Jurisdição e Domínios e Jurisdição. Elaborados por Grupos de Contato multissetoriais dedicados, estes documentos contêm propostas concretas para Normas, Critérios e Mecanismos relativos, respectivamente, a: acesso transfronteiriço a provas eletrônicas, moderação e restrições de conteúdo online e suspensões de nomes de domínios. As propostas são o resultado do trabalho conduzido pelos 140 Membros dos três Programas, desde agosto de 2018, para implementar o *Roteiro de Ottawa*[3] adotado durante a 2ª Conferência Global, em fevereiro de 2018.

As partes interessadas reiteraram o seu forte apelo ao desenvolvimento conjunto, através da Rede de Políticas Internet & Jurisdição, de soluções operacionais e normas de políticas. Com base nas propostas concretas dos documentos *Abordagens*

1 A lista de participantes, programa, vídeos das Sessões Plenárias das Partes Interessadas e fotos da Conferência podem ser consultados em <https://conference.internetjurisdiction.net/>

2 Os documentos Abordagens Operacionais podem ser consultados em: <https://www.internetjurisdiction.net/news/operational-approaches-documents-with-concrete-proposals-for-norms-criteria-and-mechanisms-released>

3 O Documento de Resultados da 2ª Conferência Global da Rede de Políticas Internet & Jurisdição, que contém o Roteiro de Ottawa, pode ser consultado em <https://www.internetjurisdiction.net/news/outcomes-of-the-2nd-global-conference-of-the-internet-jurisdiction-policy-network>

Operacionais, os participantes da 3ª Conferência Global aperfeiçoaram o Roteiro de Berlim com Planos de Trabalho para estruturar novos esforços nos três Programas da Rede de Políticas até a sua 4ª Conferência Global, a ser realizada em 2021.

Por ocasião da Conferência, foram formalmente lançados os principais resultados do primeiro *Relatório de Status Global Internet & Jurisdição (Internet & Jurisdiction Global Status Report)*[4]. Essa importante publicação complementa o trabalho de desenvolvimento de políticas dos três Programas, promovendo a coerência das políticas e aumentando a capacitação em todo o mundo. 94% dos atores da Rede de Políticas que foram consultados sobre o assunto acreditam que os desafios jurisdicionais na Internet se tornarão cada vez mais agudos nos próximos três anos, enquanto 79% deles afirmam que ainda não dispomos de coordenação e instituições suficientes para enfrentar estes desafios. Com base em um esforço de coleta de dados em larga escala, o *Relatório de Status Global Internet & Jurisdição* visa a permitir a inovação de políticas baseadas em evidências nos níveis global e regional.

Após Paris, em 2016, e Ottawa, em 2018, esta 3ª Conferência Global demonstrou o compromisso de engajamento de um número crescente das principais partes interessadas no trabalho da Rede de Políticas Internet & Jurisdição, a fim de conciliar os objetivos de enfrentar abusos, proteger os direitos humanos e possibilitar o desenvolvimento da economia digital.

As discussões em Berlim contribuíram para fortalecer o espírito construtivo manifestado durante o trabalho dos Grupos de Contato dos Programas, tornando esta 3ª Conferência Global da Rede de Políticas Internet & Jurisdição um passo catalisador no processo de desenvolvimento conjunto de soluções operacionais para os desafios comuns das partes interessadas.

4 Mais informações sobre o primeiro Relatório de Status Global Internet & Jurisdição do mundo podem ser consultadas em <https://www.internetjurisdiction.net/publications/paper/internet-jurisdiction-global-status-report-key-findings>

RESUMO DO SECRETARIADO

Administrando a Interdependência Jurídica

O primeiro dia da 3ª Conferência Global em Berlim destacou a rápida evolução do ambiente jurisdicional desde a 2ª Conferência Global, realizada em Ottawa, em 2018. As partes interessadas salientaram a proliferação acelerada de iniciativas dos agentes públicos e privados. Embora isso ainda seja frequentemente feito de forma descoordenada e sob a pressão da urgência, esta tendência geral demonstra positivamente uma crescente conscientização entre os atores de todos os grupos de interesse sobre os desafios comuns que enfrentam e o seu crescente empenho em abordá-los.

A crescente interdependência econômica e social em nossa sociedade global conectada aumenta a interdependência jurídica: as decisões adotadas em um país para regular atividades online ou combater abusos têm cada vez mais impactos extraterritoriais, intencionalmente ou não; da mesma forma, ações ou inações por empresas de Internet têm consequências para usuários em todo o mundo.

Esta interdependência jurídica exige uma abordagem sistêmica. Compete a todos os atores desenvolverem soluções específicas para avaliar minuciosamente o seu impacto, as suas potenciais consequências não intencionais ou as externalidades negativas e a dinâmica que produzem no longo prazo. Idealmente, as soluções devem, em última análise, ser capazes de escalar para um grande número de atores e suficientemente adaptáveis para ter em conta as evoluções futuras.

Ainda que a cooperação internacional esteja sob pressão, os participantes da 3ª Conferência Global enfatizaram novamente que ela é mais necessária do que nunca. O trabalho realizado nos três Programas temáticos da Rede de Políticas Internet & Jurisdição que produziram os documentos *Abordagens Operacionais*, bem como as discussões durante a própria Conferência, foram considerados ilustrativos do que pode ser alcançado quando os atores trabalham em um espírito construtivo de respeito mútuo e comportamento responsável.

Construção da sociedade digital global

Ao longo da história, a humanidade tem se confrontado, às vezes de forma conflitante, com o desafio de se organizar em comunidades cada vez maiores. Como consequência de tremendas inovações técnicas, precisamos agora gerenciar as interações de bilhões de pessoas conectadas. Definir qual é a sociedade digital que queremos construir, ou seja, quais valores são suficientemente compartilhados para funcionar potencialmente em uma escala para toda a humanidade; e de que maneira e por quem as normas devem ser estabelecidas, implementadas e aplicadas não é nada menos que um desafio civilizacional. As decisões que tomamos hoje terão impactos duradouros nas gerações futuras.

A harmonização global e a uniformidade não são alcançáveis nem desejáveis: podem facilmente negar a diversidade que faz a riqueza das sociedades humanas. Ao mesmo tempo, uma corrida armamentista jurídica entre todos os atores para impor suas próprias normas ao máximo apenas exacerba os conflitos e, em última análise, recompensa os mais poderosos.

Para evitar estes cenários extremos, as partes interessadas salientaram o valor de uma terceira abordagem, mais equilibrada e escalável, baseada no princípio fundamental que permitiu o sucesso da Internet e da World Wide Web: a interoperabilidade. A interoperabilidade jurídica foi, portanto, o tema central nas discussões dos atores sobre soluções operacionais e normas de políticas durante o segundo dia da 3ª Conferência Global nas Reuniões dos três Programas da Rede de Políticas.

InteroperabilidadeJurídica: o caminho a seguir

Numerosos e diversos regimes de governança - públicos ou privados - definem as responsabilidades dos atores aos quais se aplicam. Possibilitar a interoperabilidade e a convivência entre esses arcabouços heterogêneos de governança pode conciliar a necessidade de soluções coletivas com o reconhecimento da autonomia dos atores, bem como a diversidade das suas referências culturais e autoridade normativa. A interoperabilidade pode fornecer soluções tão distribuídas e escaláveis quanto a própria internet.

Isso requer: comunicação entre todas as partes interessadas para ajudá-las a compreender a situação, as preocupações e as

intenções mútuas; normas de comportamento acordadas para fomentar a coordenação informal ou estruturada; e processos para o desenvolvimento de mecanismos práticos de cooperação. A Rede de Políticas Internet & Jurisdição se esforça para promover essa abordagem através de processos que envolvem uma ampla gama de atores em diferentes grupos e regiões.

Concretamente, em seus esforços para enfrentar adequadamente os abusos, as partes interessadas desenvolvem uma variedade de respostas normativas, incluindo leis nacionais ou acordos internacionais para atores públicos, ou Termos de Serviço e Diretrizes de Comunidade aprimorados para atores privados. Esses dois tipos de atores também elaboram, desenvolvem ou já implementaram diferentes sistemas técnicos, como plataformas e portais para notificações, ferramentas algorítmicas e sistemas técnicos para gerenciar e responder a avisos ou ordens. Assegurar a interoperabilidade exige, portanto, um esforço específico para abordar: 1) a interoperabilidade entre atores, tendo em conta as ferramentas técnicas que empregam, bem como 2) a interoperabilidade entre as diferentes normas aplicáveis.

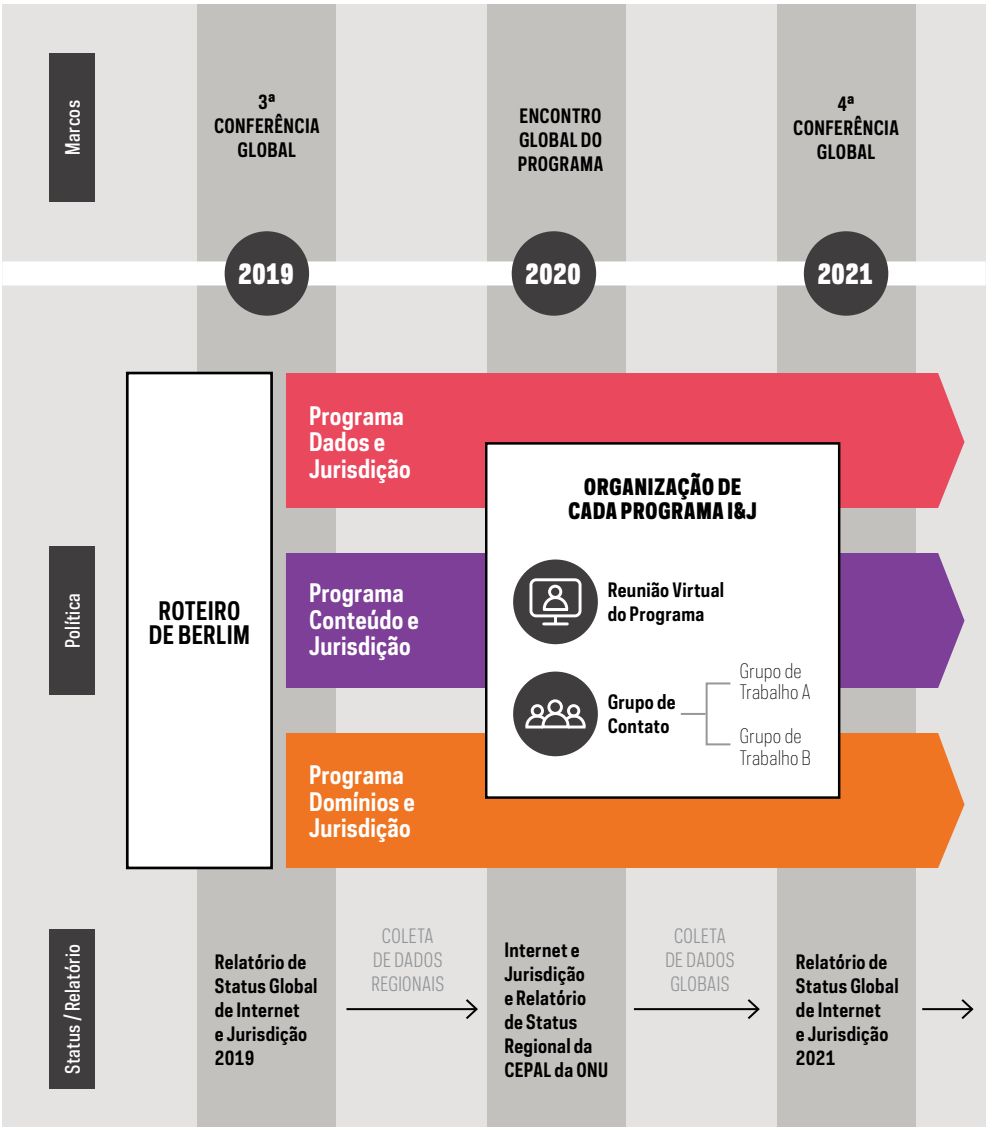
O roteiro de Berlim: rumo a soluções operacionais

Com base nas propostas concretas para as Normas, Critérios e Mecanismos contidos nos Documentos *Abordagens Operacionais*, os participantes da 3ª Conferência Global da Rede de Políticas de Internet & Jurisdição aperfeiçoaram os Planos de Trabalho abaixo para estruturar o trabalho futuro nos três Programas, com o intuito de promover o desenvolvimento das soluções operacionais e normas de políticas.

Assim sendo, serão criados dois novos Grupos de Trabalho específicos em cada um dos três Programas temáticos para abordar, respectivamente, a interoperabilidade entre atores (GT-A) e entre normas (GT-B). Replicando o processo estabelecido entre a 2ª e 3ª Conferências Globais, um Grupo de Contato para cada Programa orientará e revisará o trabalho desses dois Grupos de Trabalho.

Além disso, serão realizadas reuniões virtuais regulares do Programa para promover a comunicação entre os Membros da Rede de Políticas interessados nos respectivos Programas, para prover atualizações regulares sobre o progresso dos trabalhos e explorar e responder a questões emergentes ou subtópicos específicos de cada Programa.

Conforme descrito no cronograma abaixo, a 4ª Conferência Global da Rede de Políticas Internet & Jurisdição acontecerá em 2021, e cada Programa realizará um Encontro Global físico em 2020 para fazer um balanço dos avanços na implementação de soluções operacionais e de padrões de políticas.



PLANO DE TRABALHO
PROGRAMA DADOS E JURISDIÇÃO

Contexto

Conforme mencionado no Roteiro de Ottawa da 2ª Conferência Global da Rede de Políticas Internet & Jurisdição, realizada em Ottawa, Canadá, de 26 a 28 de fevereiro de 2018:

As investigações criminais exigem cada vez mais acesso a informações sobre usuários e provas digitais armazenadas em nuvem por empresas privadas em jurisdições fora do país requerente.

Os procedimentos existentes nos Tratados de Assistência Jurídica Mútua (MLATs, a sigla em inglês) são amplamente reconhecidos como lentos e mal-adaptados. Entretanto, garantias processuais limitadas aplicam-se a pedidos diretos enviados às empresas e esses pedidos diretos podem até mesmo ser proibidos por alguns estatutos nacionais impeditivos.

Esta situação de insegurança jurídica é insustentável. Em particular, a falta de estruturas de cooperação claras incentiva abordagens obrigatórias de localização de dados que são tecnicamente difíceis de implementar e podem ter impactos prejudiciais na economia de nuvem e nos direitos humanos.

Diferentes esforços para o desenvolvimento de soluções estão em curso e a coerência política entre elas é importante: ações descoordenadas podem ter consequências indesejadas ou aumentar os conflitos entre leis.

Todos os atores são confrontados com um desafio comum: desenvolver normas de políticas que respeitem a privacidade e processos legais que definam as condições em que as autoridades responsáveis pela aplicação da lei podem solicitar a entidades estrangeiras o acesso a dados armazenados de usuários, necessários para investigações lícitas.

Objetivo comum

Nessa perspectiva, os participantes da Reunião do Programa Dados e Jurisdição da 2ª Conferência Global da Rede de Políticas Internet & Jurisdição, realizada em Ottawa, Canadá, de 26 a 28 de fevereiro de 2018, identificaram como objetivo comum:

A definição de normas substantivas e processuais de alto nível

- Que permitam às autoridades competentes de países específicos,

- Em investigações sobre determinados tipos de crimes com conexão clara com o país requerente,
- Enviar diretamente pedidos estruturados e que respeitem o devido processo
- Para empresas privadas de outro país a fim de obter a divulgação voluntária
- Dos dados do usuário, onde quer que esses dados estejam armazenados.

Plano de trabalho de Berlim

Para atingir este objetivo e com base nas Questões Estruturantes identificadas no Roteiro de Ottawa, o Grupo de Contato do Programa Dados e Jurisdição desenvolveu as *Abordagens Operacionais*, propondo Normas, Critérios e Mecanismos para fornecer um arcabouço de referência comum a todos os atores que lidam com esta questão.

Com isso em mente, os participantes da Reunião do Programa Dados e Jurisdição da 3ª Conferência Global da Rede de Políticas Internet & Jurisdição, realizada em Berlim, Alemanha, de 3 a 5 de junho de 2019, analisaram e aperfeiçoaram a minuta de um Plano de Trabalho. Esse Plano de Trabalho poderá orientar atividades futuras do Programa Dados e Jurisdição, que continuam focadas no acesso transfronteiriço a provas eletrônicas em investigações criminais.

Os participantes da Conferência de Berlim destacaram a importância da ampla divulgação do documento *Abordagens Operacionais* após a 3ª Conferência Global. O documento, organizado em Normas, Critérios e Mecanismos Operacionais, traz muito conteúdo útil. Grande parte desse conteúdo reflete um amplo consenso que resultou de discussões intensas entre várias partes interessadas e, como tal, pode fornecer uma contribuição valiosa para muitos atores que lidam com questões de Dados e Jurisdição em vários fóruns e processos.

Ao mesmo tempo, identificou-se que alguns elementos do documento *Abordagens Operacionais* necessitam de maior atenção, em alguns casos para esclarecer ou definir melhor certos aspectos; em outros, para explorar mais amplamente.

Os participantes identificaram os seguintes componentes concretos para estruturar novos esforços do Programa através de dois Grupos de Trabalho dedicados a:

Interoperabilidade entre atores (grupo de trabalho A)

Este grupo de trabalho abordará a interface processual entre autoridades públicas requerentes, provedores de serviços e outras partes relevantes no que diz respeito à emissão, validação, transmissão e tratamento de pedidos/ordens de acesso a provas eletrônicas. Os participantes da 3ª Conferência Global identificaram temas que podem merecer mais discussão, tendo em conta o progresso documentado nas *Abordagens Operacionais*. Esses tópicos incluem:

- Componentes de pedido/ordem e formato *(Ref. Critérios J — Formatos de Pedidos; Critérios D-1b — Usuários e Mecanismo Operacional — Linguagem de Marcação e Tags de Interoperabilidade)*, em especial, os seguintes subtópicos:
  - Cronologia da notificação ao país destinatário (antes ou concomitantemente ao pedido? Considerações práticas de volume e carga de trabalho?) (Ver também o Grupo de Trabalho B — Interoperabilidade das Normas)
  - Transmissão de informações básicas sobre a investigação criminal
  - Suficiência de informações para operacionalizar as normas acordadas, tendo em conta a salvaguarda das investigações, a capacidade dos provedores para contestar os pedidos/ordens e a diferenciação dos componentes dos pedidos enviados às autoridades judiciais e aos provedores (ver também Critérios J-3 e Grupo de Trabalho B — Interoperabilidade das Normas)
  - Fundamentação para confidencialidade e condições e fundamentação para as exceções quanto à notificação ao usuário
  - Obrigações dos provedores no tocante à manutenção das normas de privacidade
- Autenticação das autoridades requerentes *(Ref. Critérios F-1,2,3 — Diversidade das Autoridades Públicas)*
- Autenticação de pedidos/ordens *(Ref. Critérios I-2,3 - Transmissão)*, nomeadamente o seguinte subtópico:
  - Possível papel da autoridade competente (legal ou judicial?) no país destinatário como ponto de contato (Consultar Critérios J-3 - Formatos de Pedido)
- Canais de transmissão para pedidos / ordens *(Ref. Critérios C - Provedores, Critérios I-1,4 - Transmissão e Crité-*

rios G-1 - Diversidade de Provedores), nomeadamente os seguintes subtópicos, tendo em conta considerações de escalabilidade:
  - Ações das autoridades competentes / empresas receptoras
  - Cronogramas para respostas a pedidos
  - Canais de transmissão criptografados e seguros entre autoridades públicas e agentes privados
- Relatório de transparência sobre regras e estatísticas *(Ref. Critérios E-1 - Transparência/Accountability)*.

Interoperabilidade entre normas (grupo de trabalho B)

Este grupo de trabalho abordará as interações substantivas entre as disposições da legislação penal nacional e os regimes que permitem o acesso transfronteiriço a provas eletrônicas, no âmbito dos direitos humanos internacionais. Os trabalhos do Grupo de Trabalho basear-se-ão na prática existente. Tal prática inclui as bases jurídicas nacionais para habilitar as autoridades competentes a ordenar a produção ou os dados, e para exigir ou permitir que o provedor de serviços divulgue os dados. Além disso, inclui a base jurídica internacional para a transferência de dados, incluindo aspectos como o idioma dos pedidos (ver também Critérios J-2 — Formatos de Pedidos).

Os participantes da 3ª Conferência Global identificaram temas que merecem mais discussão, tendo em conta o consenso entre as partes interessadas documentado em diversas partes das *Abordagens Operacionais*. Esses tópicos incluem:

- **Tipos de crimes abrangidos e respectivas sanções** *(ref. Critérios A-2 — Âmbito de Aplicação do Regime)*
- **Validação judicial/independente de pedidos/ordens individuais** *(Ref. Critérios B-1 - Autoridades Públicas e Critérios H-3 - Escalabilidade Geográfica)*, nomeadamente os seguintes subtópicos:
  - Responsabilidade pela avaliação de situações de emergência, tendo em conta as práticas existentes e em desenvolvimento (por exemplo, o MLAT e o projeto sobre emergências do Protocolo da Convenção de Budapeste)
  - Duração das situações de emergência
- **Normas nacionais para análise e aprovação de um pedido** *(Ref. Critérios B-2,3 - Autoridades Públicas)*

- Esclarecimentos e desafios relativos aos pedidos/ordens por provedores de serviços *(Ref. Critérios C-1,2,3 - Provedores)*, nomeadamente os seguintes subtópicos:
  - Possíveis sanções por descumprimento
  - Problemas de escalabilidade para pequenos provedores (por exemplo, recuperação de custos, capacidade)
  - Relações e distribuição de papéis entre atores públicos e privados nos processos de contestação
  - Resolução de conflitos de lei
- Salvaguarda dos interesses de outras partes que não a autoridade requerente *(Ref. Critérios K-3 - Nexo e Critérios E-2 - Transparência/Accountability)*, em particular o seguinte subtópico:
  - Disponibilidade/fontes de recursos para reforçar as capacidades do país destinatário (?)
- Regras de notificação para o usuário e acesso a recursos *(Ref. Critérios D - Usuários)*
- Elementos de um pedido/ordem a ser divulgado a um provedor no que diz respeito à descrição da infração alegada *(Ref. Critérios J - Formatos de Pedido, ver também Grupo de Trabalho 1 - Interoperabilidade dos Atores)*

PLANO DE TRABALHO
PROGRAMA CONTEÚDO E JURISDIÇÃO

Contexto

Conforme afirmado no Roteiro de Ottawa da 2ª Conferência Global da Rede de Políticas Internet & Jurisdição, realizada em Ottawa, Canadá, de 26 a 28 de fevereiro de 2018:

Todos os dias, centenas de milhões de posts e centenas de milhares de horas de vídeos são carregados nas principais plataformas de internet e tornados globalmente acessíveis, facilitando grandemente a liberdade de expressão. Ao mesmo tempo, são levantadas preocupações legítimas quanto ao aumento de comportamentos nocivos, incluindo o discurso de ódio, assédio, ameaças à segurança, incitamento à violência ou discriminação.

A proteção dos direitos humanos e da liberdade de expressão, quando se trata de tais abusos na Internet, constitui um grande desafio transnacional, diante da ausência de arcabouços substantivos e processuais claramente acordados para lidar com a disparidade das legislações nacionais: os conteúdos jurídicos num país podem ser ilegais noutro país.

Além disso, o número de decisões de restrições individuais a serem tomadas é sem precedentes, e as determinações caso a caso devem atentar cuidadosamente para o contexto e a intenção, mas dentro de recursos e tempos de resposta muito limitados, dada a propagação viral.

Neste contexto, são feitas exigências opostas em relação às expectativas dos intermediários: um pedindo-lhes que policiem minuciosamente os conteúdos postados em suas plataformas para garantir o respeito às leis nacionais e proteger seus usuários; e o outro se opõe a que eles façam determinações por conta própria, exercendo monitoramento proativo de conteúdo, por medo de implicações prejudiciais aos direitos humanos.

São necessárias diretrizes comuns claras e mecanismos processuais adequados para enfrentar este desafio comum de todos os atores: maximizar a necessária remediação de danos e minimizar as restrições à liberdade de expressão.

Objetivo comum

O objetivo fundamental é definir interfaces jurisdicionais viáveis entre diferentes normas jurídicas nacionais. Os parti-

cipantes da Reunião do Programa Conteúdo e Jurisdição da 2ª Conferência Global da Rede de Políticas Internet & Jurisdição, realizada em Ottawa, Canadá, de 26 a 28 de fevereiro de 2018, acordaram como seu objetivo comum a identificação do status atual, e a obtenção de esclarecimento e coerência com relação aos seguintes pontos:

Definição de normas substantivas e processuais elevadas

- Normas substantivas aplicáveis, incluindo a interação entre os direitos humanos internacionais e regionais acordados, leis nacionais e diretrizes de comunidade das empresas,
- Respectivas obrigações dos Estados e respetivas responsabilidades e proteções de outros atores, incluindo a identificação de conteúdos alegadamente ilegais,
- Decisão, normas e procedimentos, incluindo o processo gradual das decisões individuais e mecanismos de recurso;
- Finalidades legítimas, necessidade e proporcionalidade no que concerne o âmbito geográfico das restrições,
- O devido processo necessário e as normas de transparência que devem ser aplicadas além das fronteiras.

Plano de trabalho de Berlim

Para atingir esse objetivo e com base nas Questões Estruturantes identificadas no Roteiro de Ottawa, o Grupo de Contato do Programa Conteúdo e Jurisdição desenvolveu *Abordagens Operacionais* com Normas, Critérios e Mecanismos propostos para fornecer um quadro de referência comum para todos os atores que abordam esta questão. Assim sendo, os participantes da Reunião do Programa Conteúdo e Jurisdição, durante a 3ª Conferência Global da Rede de Políticas Internet & Jurisdição, realizada em Berlim, Alemanha, de 3 a 5 de junho de 2019, identificaram os seguintes componentes concretos para estruturar novos esforços do Programa através de dois Grupos de Trabalho dedicados a:

Interoperabilidade entre atores (grupo de trabalho A)

Este grupo de trabalho abordará as relações processuais entre autoridades públicas, notificadores, provedores de serviços e usuários, na medida em que se relacionam com a moderação de conteúdos e restrições, principalmente:

- **Formatos e componentes das queixas apresentadas por autoridades públicas e agentes privados** *(Ref. Critérios C-1,2 - Avisos de Terceiros e Critérios F - Avaliação),* incluindo mecanismos para requisitos de emergência/urgência.
- **Formatos e componentes da notificação ao usuário** *(Ref. Critérios I - Notificação ao Usuário)*
- **Canais e ferramentas de reclamações e notificações** *(Ref. Critérios C - Avisos de Terceiros),* incluindo um mecanismo para relatar abusos de sistemas de notificação, baseado na adjudicação pós-recurso.
- **Procedimentos de recurso** *(Ref. Critérios J - Recurso e Mecanismo Operacional - Abordagens relativas a recursos após restrição de conteúdo)*
- **Avaliação e supervisão da tomada de decisão algorítmica relativa aos procedimentos acima** *(Ref. Critérios D - Detecção do Provedor)*

Interoperabilidade entre normas (grupo de trabalho B)

Este Grupo de Trabalho abordará a interação entre os direitos humanos internacionais, as leis nacionais e os tratados internacionais aplicáveis, e os Termos de Serviço e Diretrizes de Comunidade dos provedores e suas implicações sobre o interesse e os direitos do usuário, considerando, em especial, a governança legítima, transparente e accountable. O âmbito do Grupo de Trabalho leva em consideração:

- **A coerência normativa internacional baseada nos direitos humanos** *(Ref. Critérios B-2 - Base Normativa e F-1e - Avaliação)*
- **Os avisos das autoridades públicas com base nas Diretrizes de Comunidade** *(Ref. Critérios C-1b - Avisos de terceiros)*
- **A ação geograficamente relevante e proporcional** (*Ref. Critérios G - Proporcionalidade geográfica)*
- **As relações entre os diferentes níveis de regulação das plataformas e a moderação nas e pelas plataforma**s *(Ref. Critérios B-3 - Base Normativa)*
- **Referências normativas e coerência jurisprudencial para mecanismos de recurso** *(Ref. Critérios J - Recurso e Mecanismo Operacional - Abordagens relativas ao recurso após restrição de conteúdo)*

PLANO DE TRABALHO
PROGRAMA DOMÍNIOS E JURISDIÇÃO

Contexto

Conforme afirmado no Roteiro de Ottawa da 2ª Conferência Global da Rede de Políticas Internet & Jurisdição, realizada em Ottawa, Canadá, de 26 a 28 de fevereiro de 2018:

Pedidos transfronteiriços de suspensão de nomes de domínio são enviados com uma frequência cada vez maior aos Operadores do Sistema de Nomes de Domínio (DNS) em relação a alegado conteúdo abusivo ou atividade em sites subjacentes.

No entanto, o DNS, como um sistema de endereçamento, é uma camada técnica neutra e vital para o bom funcionamento da Internet. Este nível não é uma forma totalmente eficaz - nem deve ser considerado a ferramenta natural - para abordar conteúdos abusivos. A proteção do núcleo da Internet é e deve ser uma prioridade fundamental.

A atuação no nível do DNS só deve ser considerada quando for possível determinar com segurança que um domínio é usado com a clara intenção de conduta abusiva significativa. Além disso, uma vez que uma suspensão do domínio tem, por definição, um impacto global, a proporcionalidade impõe que apenas um nível particularmente elevado de abuso e/ou prejuízo possa potencialmente justificar tal medida. É importante que o impacto de uma ação específica no nível do DNS seja bem compreendido.

Esta importante questão é geralmente reconhecida como fora do âmbito da ICANN. Além disso, a distinção fundamental entre Domínios de Primeiro Nível genéricos e de códigos de país em termos das relações com, respectivamente, a ICANN e as leis ou autoridades nacionais, leva a abordagens e restrições muito diferentes.

No entanto, todos os atores são confrontados com um desafio comum: definir quando é apropriado agir no nível do DNS em relação ao conteúdo ou comportamento sob um endereço de domínio, e qual o papel que os tribunais e os chamados "notificadores" devem ou poderiam desempenhar, respectivamente.

Objetivo comum

Nesta perspectiva, os participantes da Reunião do Programa Domínios e Jurisdição da 2ª Conferência Global da Internet & Jurisdição Policy Network, realizada em Ottawa, Canadá, de 26 a 28 de fevereiro de 2018, identificaram como objetivo comum a definição dos seguintes tópicos:

Normas substantivas e processuais elevadas que definam

- Em quais condições restritas a interrupção de um nome de domínio sem o consentimento do registrante pode ser contemplada/aceitável;
- Quais ações os operadores de nomes de domínio deveriam/estariam dispostos e aptos a exercer;
- Que regras e procedimentos podem ajudar a estabelecer ou reforçar a credibilidade das notificações dos notificadores (para fins de informação ou ação); e
- Quais mecanismos podem ajudar a melhorar a transparência em tais processos.

Plano de trabalho de Berlim

Para atingir esse objetivo e com base nas Questões Estruturantes identificadas no Roteiro de Ottawa, o Grupo de Contato do Programa Domínios e Jurisdição desenvolveu *Abordagens Operacionais*, propondo Normas, Critérios e Mecanismos para fornecer um arcabouço de referência comum a todos os atores que lidam com esta questão. Assim sendo, os participantes da Reunião do Programa Domínios e Jurisdição da 3ª Conferência Global da Rede de Políticas Internet & Jurisdição, realizada em Berlim, Alemanha, de 3 a 5 de junho de 2019, identificaram os seguintes componentes concretos para estruturar novos esforços no Programa através de dois Grupos de Trabalho dedicados a:

Interoperabilidade entre atores (grupo de trabalho A)

Este grupo de trabalho abordará a interface processual entre operadores de DNS, tribunais nacionais e estrangeiros, notificadores especializados, indivíduos e registrantes, e em especial:

- **Componentes do aviso e canais de notificação de abuso** *(Ref. Critérios C - Componentes do Aviso e Mecanismo Operacional - Interface para Notificações de Abusos a Operadores de DNS)*, incluindo os seguintes elementos:
  - Relações com a aplicação da lei

- Cronograma para respostas e documentos corroborativos
- Rotas de emergência
- Local claro para obtenção de informações
- Informações de contato
- Avaliação/Análise de pedidos
- Padrão aceito globalmente para formatos de solicitação (e interface de idioma)

- **Mecanismos de notificação aos registrantes** *(Ref. Critérios H - Notificação aos Registrantes)*, incluindo:
  - Procedimento aplicável a atores específicos (por exemplo, aplicação da lei) para justificar uma exceção aos princípios da notificação do registrante
- **Devida diligência processual por notificadores especializados e tipos de notificadores** *(Ref. Critérios E-2b – Devida Diligência por Notificadores)*, incluindo os seguintes elementos:
  - Estruturas para identificar a responsabilidade legal
  - Canais de indenização para registros
  - Papel dos notificadores confiáveis
- **Aspectos processuais dos mecanismos de recurso para registrantes** *(Ref. Critérios I - Recurso para Registrantes)*
- Rastreabilidade de notificações e coleta de estatísticas *(Ref. Critérios G-1 - Transparência)*, incluindo os seguintes elementos:
  - Transparência do processo
  - Dados relevantes à transparência do processo
- **Expectativas das partes em um sistema de notificação de abusos** *(Ref. Critérios C - Componentes de Aviso e Mecanismo Operacional - Interface para Notificações de Abusos a Operadores de DNS)*

Interoperabilidade entre normas (grupo de trabalho B)

Este Grupo de Trabalho abordará a interação entre as leis nacionais, políticas dos Operadores de DNS e regras dos notificadores especializados, em particular:

- **Limites que justifiquem a ação, de acordo com diferentes tipos de abuso** *(Ref. Critérios A - Tipos de Abuso e Critérios B - Limiares)*, incluindo os seguintes elementos:
  - Mapeamento da fonte normativa dos danos e dos limiares atuais para ação dos Operadores de DNS

- Princípio da proporcionalidade e esgotamento de medidas alternativas
- Interesse coletivo dos consumidores
- Gravidade do abuso/dano e respectivos canais de notificação e escalonamento
- Verificação do conhecimento do abuso pelo registrante

- **Alcance geográfico das ordens judiciais do país de incorporação do Operador de DNS** *(Ref. Critérios D-1 - Tipos de notificadores)*, incluindo:
  - Risco de que uma ação local tenha efeitos globais
- **Tratamento de ordens judiciais de fora da jurisdição do Operador de DNS** *(Ref. Critérios D-2a - Tipos de notificadores)*, incluindo:
  - Consistência normativa internacional (incluindo diferenças de consistência entre abuso técnico e abuso de conteúdo)
- **Devida diligência substantiva pelos Notificadores** *(Ref. Critérios E-2a – Devida Diligência pelos notificadores)*, incluindo os seguintes elementos:
  - Impacto potencial sobre outros atores devido à natureza específica do DNS
  - Funções e descrições dos notificadores confiáveis
  - Potencial papel da Inteligência Artificial na tomada de decisões
  - Identificação do operador de DNS pelo notificador

nic.br

Núcleo de Informação
e Coordenação do
Ponto BR