

# QUAL É A ESTRUTURA DE INTERVENÇÃO IDEAL PARA CONTER AS *FAKE NEWS* E REFORÇAR A DEMOCRACIA?



*Sascha Meinrath, Steven Mansour, Humza Jilani*

Este artigo visa ajudar a forjar um caminho unificado no esforço criticamente importante para conter a informação falsa e reforçar a democracia. Primeiro, são discutidas as ações regulatórias necessárias para lidar com os danos das plataformas de mídia digital. Em seguida, são descritos tais danos, bem como os potenciais espaços para a ação regulatória e legislativa. O capítulo conclui com uma proposta de estrutura de intervenção em cinco níveis, exigindo divulgação e transparência, auditorias algorítmicas, multas por não cumprimento intencional, diminuição da proteção de responsabilidade e processo criminal.

## **AÇÕES REGULATÓRIAS NECESSÁRIAS PARA LIDAR COM OS DANOS DAS PLATAFORMAS DE MÍDIA DIGITAL**

Os reguladores da União Europeia já começaram a averiguar como estabelecer um regime para examinar, auditar e fazer cumprir as violações da privacidade das plataformas de mídia digital<sup>1</sup>. Poderes semelhantes também foram instituídos para permitir a supervisão de outros danos relacionados a essas plataformas. Da mesma forma, as capacidades tecnológicas necessárias para identificar, documentar, rastrear e analisar desinformações estão amplamente disponíveis. As empresas de mídia digital têm usado tais ferramentas para rastrear materiais protegidos por direitos autorais e identificar trabalhos deles derivados por décadas.

***Em essência, a funcionalidade necessária para impedir a desinformação já está incorporada aos principais modelos de negócios de muitas empresas de mídia.***

Portanto, os esforços regulatórios para conter a desinformação e a informação errada nas mídias sociais deveriam se concentrar em determinar o nível de acesso aos dados e à tecnologia – e o empoderamento legal – necessário para avaliar e informar sobre a natureza, a amplitude e o escopo dos danos observados em todo o cenário das mídias sociais e das plataformas digitais.

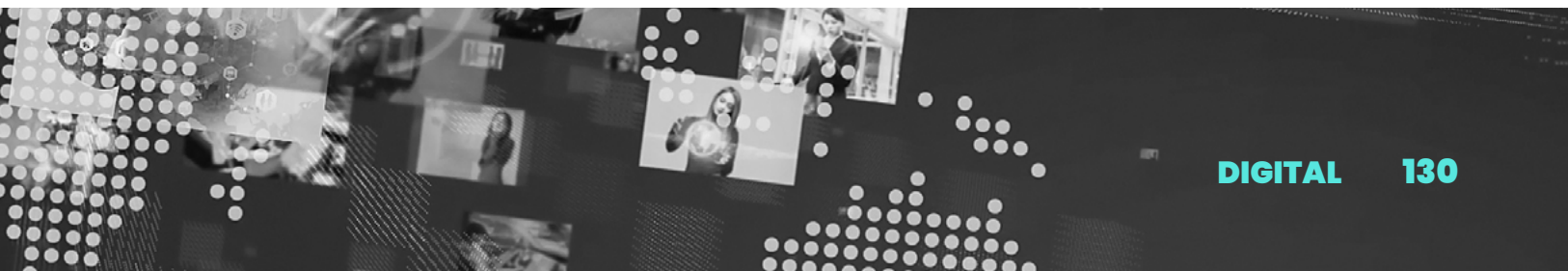
Para cumprir esse papel essencial, os reguladores precisarão exercer quatro poderes básicos:


1. Acesso: Acesso abrangente e sem restrições aos dados e metadados (timestamps, algoritmos de conteúdo ativo, originando e disseminando usuários etc.) específicos à informação falsa que está sendo auditada.
2. Auditoria: O estabelecimento de autoridades de auditoria permitindo o estabelecimento de um “limiar de dano” (uma medida quantitativa e qualitativa de exposição de um grupo de usuários ou demografia a conteúdo nocivo que constitui uma violação da lei).
3. Mandatos de implementação: A criação de medidas que as empresas devem implementar – sejam elas de concepção, entrega ou mudanças nos termos de uso – a fim de mitigar os danos reais e potenciais.
4. Intervenção: Intervenções significativas que desincentivam as plataformas de continuar a permitir a propagação de informações errôneas e outros conteúdos prejudiciais.

O primeiro poder é direto – assim como durante uma Avaliação de Impacto na Privacidade (PIA), todos os dados relevantes em torno do conteúdo em questão precisarão ser disponibilizados para auditoria. As auditorias de plataformas de mídia digital são necessárias para ajudar a lidar com a perigosa propagação de desinformação e informação errada. O segundo e o terceiro poderes estão relacionados com a natureza e os objetivos dessas auditorias: De que devem ser compostas e a que devem conduzir? Após o exercício dos três primeiros poderes, o poder final será necessário para garantir a conformidade e a responsabilização das empresas pelas falhas contínuas.

## **ACESSO E AUDITORIA**

A primeira área proposta de foco regulatório requer acesso não apenas ao conteúdo, mas também aos conjuntos de algoritmos, processos decisórios e estruturas pelas quais o conteúdo da plataforma é promovido, rebaixado, censurado, removido e compartilhado (assim como quais partes interessadas internas e externas têm acesso para visualizar, modificar ou manipular esses dados). Ao equipar os reguladores com as informações necessárias para entender como a informação falsa tem se espalhado por uma determinada rede, eles estarão mais bem munidos para enfrentar os episódios atuais e futuros.





A próxima faceta de um regime de auditoria abrangente para plataformas de mídia digital é a investigação dos métodos usados para difundir conteúdos problemáticos (e os concomitantes resultados prejudiciais e deletérios engendrados por sua propagação). Os impactos da disseminação também devem ser examinados – identificando as consequências negativas e os públicos-alvo mais vulneráveis, determinando se a propagação direcionada é intencional ou o subproduto do foco “acidental”, avaliando quais são os círculos mais propensos a contribuir para a disseminação de informações errôneas específicas, e examinar se existem “nós” identificáveis que tendem a agir como “multiplicadores de força” para a disseminação de informações falsas. Relacionado a este fim, a Aliança Global para Mídia Responsável (GARM) é uma iniciativa da indústria para coordenar esforços entre plataformas, agências de mídia e marqueteiros para desenvolver entendimentos comuns de conteúdo “prejudicial e sensível”, criar transparência para os participantes da indústria sobre onde o conteúdo sensível pode estar presente e discutir opções para aplicar políticas de monetização consistentes com a estrutura da GARM<sup>2</sup>. No entanto, embora a criação da GARM seja um começo positivo, confiar na autorregulamentação pelas partes interessadas no negócio não será suficiente para amenizar adequadamente o problema. Dada a centralidade da otimização da atenção para o modelo de negócios principal do setor, deve haver um papel para que os reguladores intervenham e influenciem os incentivos para remover o conteúdo problemático.

Os reguladores também precisarão ter acesso a todas as informações necessárias para identificar a composição, natureza e amplitude das redes de difusão de informações falsas, bem como informações sobre a sua própria difusão. Da mesma forma, os efeitos do mundo real da informação falsa atingindo seu alvo demográfico, influenciando seu público e substituindo a informação especializada, tudo isso precisa ser estudado e avaliado para que os reguladores compreendam a extensão total dos danos causados por qualquer algoritmo particular ounexo de informação falsa.

## IMPLEMENTAÇÃO E INTERVENÇÃO

Quando violações, o não cumprimento ou a não observância de mandatos destinados a conter informações falsas forem documentados, os reguladores precisarão impor multas impactantes e outros desincentivos, bem como ter o poder de intimar plataformas de mídia digital a fim de obter o nível necessário de acesso e permissões para conduzir uma investigação e auditoria completas. Em todo o mundo, já existem precedentes relevantes para esses tipos de poderes dentro dos setores de privacidade, financeiro/bancário, de segurança alimentar e farmacêutico, e precisariam simplesmente ser transferidos para o domínio de dados e informações (ver box ao final do artigo) . Nos Estados Unidos, o leque de atividades da Food and Drug Administration contra violações da segurança alimentar inclui a emissão de notificações para a empresa infratora de delitos, solicitando injunções judiciais contra uma ação e até mesmo abrindo processos criminais por determinadas violações sob a Seção 301 da Lei de Cosméticos (que diz respeito principalmente à adulteração de marcas e produtos).<sup>3</sup>

Da mesma forma, a Comissão de Títulos e Câmbio pode impor punições civis e administrativas contra os infratores, incluindo ordens judiciais que obriguem os indivíduos a se envolverem em certas ações, restituição de dinheiro recebido por atividade de conduta ilegal e penalidades civis.<sup>4</sup> Nesta mesma linha, a Agência de Proteção Ambiental, recentemente, flexibilizou sua força reguladora para processar a Volkswagen por violação das normas de emissão de poluentes, resultando em multas de vários bilhões de dólares.<sup>5</sup>

Os reguladores também devem assegurar que a divulgação de conteúdos relevantes e a alfabetização digital sejam incorporadas ao funcionamento das plataformas de mídia digital. O cumprimento das medidas propostas exigiria que essas fornecessem as informações e treinamento necessários para que os usuários tomassem decisões esclarecidas sobre a propagação da informação. Da mesma forma, assim é possível que os usuários possam ser responsabilizados pela participação voluntária na distribuição de informação falsa.

***Em essência, as plataformas de mídia digital seriam obrigadas a ajudar a informar e educar os usuários e visitantes sobre o conteúdo que poderia ser enganoso antes de se espalhar, ajudando tanto a educar os cidadãos sobre técnicas úteis para identificar a informação falsa quanto a limitar o ciclo de vida da publicação problemática.***

Vários países, incluindo o Reino Unido, Finlândia e Holanda, já ordenaram campanhas de alfabetização sobre a mídia com o objetivo de conter a informação falsa e orientar os cidadãos sobre como verificar as fontes e estar vigilantes antes de compartilhar ou repassar um conteúdo potencialmente enganoso. Embora tais medidas sejam um bem-vindo passo adiante, deve-se tomar cuidado para evitar censurar os esforços jornalísticos e a liberdade de expressão – apesar de a maioria das informações falsas (ao contrário da opinião pessoal) ser facilmente identificada como tal, mesmo na revisão mais superficial.


***No Brasil, o artigo 12 do Marco Civil da Internet estabelece uma estrutura legal abrangente para crescentes intervenções por violações de proteção à privacidade. No entanto, embora seja pioneira no campo da privacidade e proteção ao consumidor, esta lei de 2014 permanece em grande parte omissa quanto aos direitos dos usuários da Internet de serem livres de propaganda e quanto às responsabilidades das plataformas de mídia digital em impedir sua disseminação.***

## DANOS A SEREM TRATADOS

***A misinformation – ou informação falsa sem intenção de prejudicar – é o principal dano a ser tratado pela estrutura de intervenção proposta. Neste contexto, o termo abrange tanto a informação errada, a tradicional misinformation (informações manifestamente falsas que são compartilhadas, independentemente da intenção) quanto a desinformação e a desinformação maliciosa (disinformation e mal-information, informações que são intencionalmente, voluntariamente e maliciosamente criadas e compartilhadas em um esforço para avançar ou suprimir certos pontos de vista ou posições subjetivas). A disseminação da informação falsa também pode ser vista como uma forma de propaganda, especialmente quando visa depreciar ou promover uma determinada posição, apesar de existirem informações objetivas/factuais em sentido contrário. Notavelmente, os danos potenciais à sociedade atribuíveis à informação falsa podem ser divididos em dois campos: danos causados quando as plataformas estão funcionando conforme planejado (isto é, por projeto) e danos causados quando as plataformas estão sendo utilizadas de maneira inapropriada.***

### DANOS CAUSADOS POR PLATAFORMAS QUE FUNCIONAM CONFORME O ESPERADO POR PROJETO

Os danos decorrentes de plataformas que funcionam conforme o esperado são os problemas que a sociedade experimenta não por causa de conteúdo ilegal ou exploração enganosa de tais plataformas, mas sim devido à disseminação viral de informações falsas através de uma plataforma quando esse produto está sendo utilizado como pretendido. Ou seja, danos causados pelas plataformas que estão sendo utilizadas para disseminar mídia e propaganda legal – mas factualmente imprecisa.



**Esses danos, muitas vezes, surgem do que é conhecido como o problema da “otimização da atenção”: onde um sistema de distribuição de informações é projetado com o objetivo principal de maximizar a exposição, as opiniões, as leituras ou os cliques a fim de gerar a máxima receita (por exemplo, dos anunciantes). Com muita frequência, nestes casos, os usuários são superexpostos a conteúdo que maximiza a taxa de cliques, que muitas vezes é profundamente diferente – e muitas vezes diametralmente oposto – do conteúdo que informa, protege e de outra forma impacta positivamente indivíduos e comunidades. É bem documentado que a heurística de otimização da atenção muitas vezes leva à rápida disseminação do sensacionalismo, ultraje, falsidade, conspiração e até mesmo do discurso do ódio.**

**Além disso, os mecanismos de proteção contra esses danos são particularmente complicados de serem aperfeiçoados, dada sua interseção com a liberdade de expressão e outros direitos protegidos. Em essência, demonstram uma tensão fundamental entre objetivos conflitantes de liberdade individual e danos à sociedade.**

## **DANOS DE PLATAFORMAS QUE ESTÃO SENDO UTILIZADAS INAPROPRIADAMENTE**

Os danos resultantes do uso inadequado das plataformas são causados pela sua manipulação ou exploração por agentes malignos. Esta forma de dano muitas vezes se sobrepõe e/ou alavanca os danos das plataformas que trabalham adequadamente. Por exemplo, a criação de redes de contas falsas e/ou híbridas reais/falsas com o propósito de ampliar artificialmente o conteúdo explora a lógica dos algoritmos de otimização da atenção. Normalmente, são utilizados “hacks” projetados para fazer com que os algoritmos de curadoria das plataformas de mídia digital priorizem a mídia para beneficiar um conjunto de usuários ou pontos de vista em relação a outro. Os maus agentes procuram conduzir uma conversa para fins comerciais ou políticos em detrimento do grupo-alvo.

***A exploração dos danos pode incluir: Comportamento Inautêntico Coordenado perpetrado por atores estatais ou não estatais, influenciadores pay-for-play que promovem produtos ou ideias sem revelar pagamento, publicidade discriminatória ou enganosa, click-bait para ganhos comerciais e a organização de atividades ilegais e/ou grupos de ódio.***

## **FOCOS DE INTERVENÇÃO**

***Existem dois objetos principais de intervenção para alterar a propagação de mídia nociva e informação falsa: agências reguladoras e órgãos legislativos.***

Em muitas jurisdições, os órgãos reguladores já estão autorizados a instituir a estrutura de intervenção proposta abaixo. Em alguns países e estados, entretanto, novas leis precisariam ser criadas para instituir uma supervisão significativa das plataformas de mídia digital.

Os locais regulatórios em potencial incluem agências de supervisão transnacionais, como as autoridades da Comissão Europeia (estabelecidas pela Digital Services Act's E-Commerce Directive), bem como entidades de nível nacional, como a Federal Trade Commission e a Federal Communications Commission dos Estados Unidos. No nível estadual ou regional, as comissões de serviços públicos e outras agências semelhantes têm capacidades de supervisão dos serviços de telecomunicações e serviços online que se integrem na estrutura atual. Em países específicos, as leis nacionais de proteção ao consumidor em relação às condições de trabalho, fabricação e segurança de produtos, controles de poluição e supervisão da autoridade tributária fornecem esquemas úteis de como o comportamento corporativo pode ser efetivamente investigado - e desincentivos significativos criados - para conter a disseminação de desinformação.

Em uma escala mais global, a legislação transnacional poderia tomar emprestado do domínio dos direitos autorais e da propriedade intelectual elementos que poderiam ser utilizados para defender que plataformas de mídia digital prestem contas além das fronteiras nacionais. Da mesma forma, nos setores financeiro/bancário e de investimento, vários tratados internacionais trabalham para garantir que o mau comportamento corporativo possa ser reprimido através das fronteiras internacionais.

## ESTRUTURA DE INTERVENÇÃO PROPOSTA

***As empresas que administram plataformas de mídia digital precisam de uma estrutura de supervisão transparente, com um conjunto claro de expectativas e um sistema de responsabilização padronizado. Para garantir que as empresas não sejam pegas desprevenidas por novos mandatos regulatórios, a criação de uma estrutura de escalonamento multiníveis concederá às empresas múltiplas oportunidades de cumprimento da lei antes que as medidas mais sérias sejam instituídas. Assim, operando de boa-fé, as empresas serão capazes de resolver rapidamente as questões para eliminar o risco de responsabilização financeira e legal bem antes que se torne necessária uma intervenção mais relevante.***

***A estrutura de intervenção de cinco níveis proposta abaixo oferece um caminho claro para o futuro, equilibrando as práticas e prioridades empresariais com a responsabilidade corporativa para com a sociedade em geral. Cada um dos cinco níveis contém tanto uma oportunidade de melhorar as questões de propagação de informação falsa e vieses, como uma série ascendente de medidas sobre as empresas, caso fracassem na resolução de problemas recorrentes. Os exemplos apresentados, retirados de plataformas de mídia digital e outras indústrias, oferecem precedentes relevantes para as intervenções que estão sendo propostas.***

## DIVULGAÇÃO E TRANSPARÊNCIA

Em geral, as empresas já têm indivíduos em cargos com obrigações legais que as tornam pessoalmente responsáveis pela conduta de sua empresa, caso se verifique que a organização tenha infringido a lei. Um diretor financeiro, por exemplo, pode ser responsabilizado pessoalmente se supervisionar uma violação de certas leis contábeis e de relatórios fiscais. No mesmo espírito, um indivíduo ou equipe de indivíduos deve ter a responsabilidade legal primária de administrar o tratamento de informações falsas, desinformações e seus perigos e danos



associados. Exigir que um indivíduo (ou grupo de indivíduos) exerça ativamente a diligência em assuntos de informação falsa permitirá que as plataformas de mídia digital desinem e capacitem as partes interessadas, estabeleçam protocolos de tomada de decisão e garantam a conformidade com essa estrutura regulatória proposta. Tal pessoa, ou equipe de pessoas, seria responsável por assinar o desempenho, impacto e resultados dos vários algoritmos usados pela plataforma de mídia para publicar, exibir, compartilhar e difundir conteúdo.

O professor de Direito de Harvard, Jonathan Zittrain, e o professor de Direito de Yale, Jack Balkin, propõem que esses requisitos de divulgação e transparência poderiam se enquadrar em uma categoria mais ampla de “fiduciários de informação”. As empresas concordariam com um conjunto de práticas de informação justa e prometeriam vender esses dados somente a outros atores que obedecessem a regras semelhantes.<sup>6</sup>

## **AUDITORIAS ALGORÍTMICAS**

***Uma autoridade reguladora governamental independente deve estar totalmente habilitada com a autoridade para perseguir a priorização e censura algorítmica. Assim como as agências governamentais de tributação em todo o mundo estão autorizadas a rever toda e qualquer transação durante uma auditoria financeira, essa nova entidade reguladora deve ter acesso a toda e qualquer informação que permita uma auditoria completa dos sistemas utilizados pelas plataformas de mídia digital para analisar e distribuir mídia e dados. Com relação às considerações e preocupações dos auditores algorítmicos, James Guszcza et al. argumentam que tais auditorias precisariam adotar uma perspectiva holística que se baseasse em múltiplas metodologias complementares das ciências sociais.***<sup>7</sup>

Além disso, um plano de melhoria da auditoria algorítmica deve ser desenvolvido pelo auditor para assegurar tanto a divulgação completa dos resultados dos fatos, como também que as empresas tenham total clareza quanto ao que precisa ser feito para cumprir a lei atual. Os resultados e os entregáveis deste plano também serão da competência da(s) posição(ões) interna(s) descrita(s) acima, no Nível I de intervenção.

***O indivíduo ou indivíduos nesta posição precisarão assinar os resultados da auditoria, bem como as mudanças necessárias para que a empresa esteja em conformidade com as exigências legais.***

## **MULTAS SIGNIFICATIVAS E IMPACTANTES PELO NÃO CUMPRIMENTO INTENCIONAL**

O General Data Protection Regulation da União Europeia, sob o artigo 83, tem um sistema de multas de dois níveis que prevê multas de 2% ou 4% (especificamente relacionadas a violações de privacidade) da receita global da empresa. Da mesma forma, quando se trata de divulgação e contenção de informações falsas, os valores das multas podem variar, dependendo do tipo de infração, da vontade das partes interessadas e dos impactos ou potenciais impactos da não conformidade.

***A fim de desenvolver um incentivo multicanal à conformidade, as penalidades financeiras também devem ser combinadas com restrições às operações comerciais.***

Investigações sobre a forma como as plataformas lidam com a disseminação de informações errôneas em suas redes serão seguidas por medidas para mitigar os danos atribuíveis a falhas no cumprimento. As empresas que lucram com a disseminação de informações falsas terão que tomar medidas concretas e imediatas para demonstrar seu compromisso de interromper a disseminação. A Lei de Aplicação da Rede Alemã poderia fornecer um modelo potencial para tais multas. De acordo com essa legislação, as empresas de tecnologia poderiam enfrentar multas de até 50 milhões de euros, por incidência, caso não removam o discurso do ódio das suas plataformas.<sup>8</sup>

## **DIMINUIÇÃO DA PROTEÇÃO DE RESPONSABILIDADE (DIMINUIÇÃO DA “NEUTRALIDADE” DA DOCTRINA DA TERCEIRA PARTE)**

As plataformas neutras que fornecem conteúdo gerado pelo usuário sem qualquer ponderação ou curadoria são fundamentalmente diferentes dos serviços e aplicações que priorizam e adaptam ativamente a mídia para seus usuários. Da mesma forma, as proteções de responsabilização destinam-se a garantir que plataformas neutras não sejam responsabilizadas pelo conteúdo em que não tiveram participação na criação ou disseminação. Isto, entretanto, é bem diferente do papel desempenhado por uma plataforma de mídia digital que, tendo falhado sistematicamente, em melhorar uma conhecida propagação de informação falsa ou violação da informação, e seguindo a implementação de um plano de melhoria e/ou multas, não se qualifica mais como uma plataforma neutra – mas sim como o curador ativo de mídia problemática. Assim, uma menor proteção de responsabilidade deveria se aplicar à plataforma de mídia digital como um intermediário – o que não infringiria nenhum direito relevante de liberdade de expressão concedido aos transmissores de ideias e informações.

Exemplos de proteções de responsabilização que podem ser retiradas das plataformas de mídia digital que continuam a propagar informações nocivas/militares incluem as concedidas através da Seção 230 da Lei de Decência das Comunicações de 1996 e/ou Seção 512 da Lei de Direitos Autorais do Milênio Digital nos Estados Unidos, ou a Diretiva de Comércio Eletrônico de 2000 na União Europeia. Alguns comentaristas propuseram que a Seção 230 deveria ser usada como alavanca para induzir que as plataformas fossem mais transparentes – forçando-as a ganhar imunidade ao revelar como seus algoritmos ordenam as notícias e quanta informação falsa está sendo divulgada.<sup>9</sup> Nesta linha, Danielle Citron e Benjamin Wittes sugerem que a reforma da Seção 230 pode envolver a adição de linguagem sobre “medidas razoáveis para prevenir ou abordar usos ilegais” de serviços como um pré-requisito para proteções de responsabilidade.<sup>10</sup>

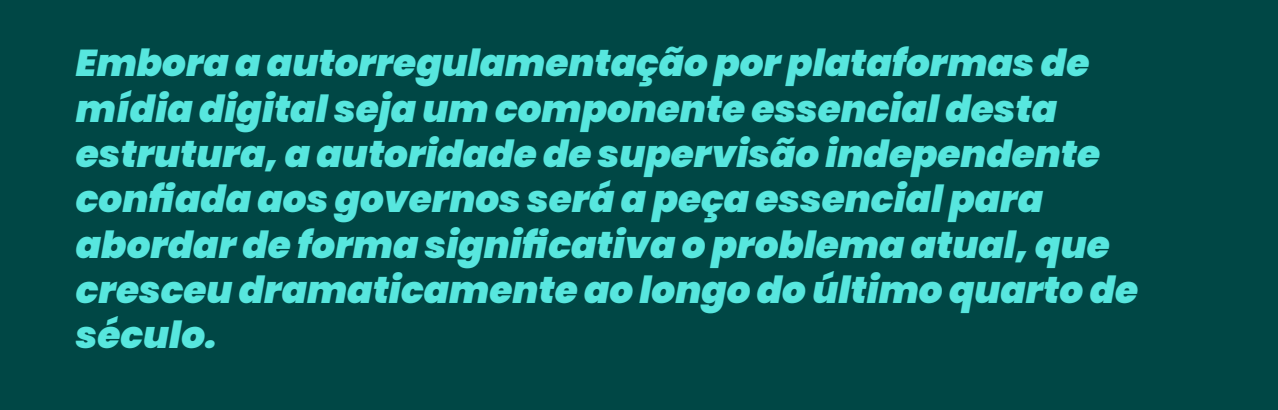
## **AÇÃO PENAL**

Por mais que existam estruturas de processo penal dentro dos domínios financeiro e de produção/extração de recursos nacionais, são necessárias vias claramente delineadas para o processo penal no setor de divulgação de dados/informações para garantir que as corporações e os indivíduos envolvidos em atividades sistemáticas de violação da lei sejam responsabilizados.

Para plataformas de mídia digital reincidentes/intransigentes que continuam a propagar informação falsa e conteúdo nocivo/abusivo, apesar das vias anteriores de intervenção, a última camada desta estrutura de intervenção envolve um processo criminal em duas etapas:

1. Ação penal corporativa visando a empresa/organização infratora; e,
2. Ação penal contra o(s) indivíduo(s) designado(s) para supervisionar a conformidade da plataforma de mídia digital com a lei.

Embora a intenção e a esperança desta estrutura regulatória proposta seja que cada nível proporcione um desestímulo adequado e crescente para fomentar a cessação imediata da mídia prejudicial e/ou a informação falsa, os reguladores não devem se coibir de instituir regras claras e/ou prazos que desencadeiem novas intervenções.



***Embora a autorregulamentação por plataformas de mídia digital seja um componente essencial desta estrutura, a autoridade de supervisão independente confiada aos governos será a peça essencial para abordar de forma significativa o problema atual, que cresceu dramaticamente ao longo do último quarto de século.***

## BOX

### EXEMPLOS DOS CINCO NÍVEIS DA ESTRUTURA DE INTERVENÇÃO

Cada um dos cinco níveis da estrutura de intervenção proposta contém tanto uma oportunidade de melhorar as questões de propagação de informação falsa e vieses, como uma série crescente de repercussões para um fracasso contínuo na resolução de problemas recorrentes. Os exemplos a seguir, retirados de plataformas de mídia digital e outras indústrias, fornecem precedentes relevantes para as intervenções que estão sendo propostas:

- I. Divulgação e Transparência – A carta da Aliança Global para Mídia Responsável estabelece os primeiros passos para a divulgação e transparência, criando um mecanismo aprovado pela indústria para regras de divulgação padrão e exigindo a necessidade de uma autoridade de auditoria independente: <https://wfanet.org/garm>
- II. Auditorias algorítmicas – Exemplos de agências governamentais que obrigam as organizações a divulgar informações são inúmeras, sendo a Receita Federal dos Estados Unidos apenas uma das muitas instituições com poder de auditoria para obrigar a divulgação de todo e qualquer documento relevante para uma auditoria financeira: <https://www.irs.gov/businesses/small-businesses-self-employed/irs-audits>
- III. Multas Significativas e impactantes pelo não cumprimento intencional – Em 2020, a Amazon enfrentou multas antitruste propostas de 10% de sua receita mundial, ou cerca de US\$ 30 bilhões, por possíveis violações das regras antitruste da União Europeia: [https://ec.europa.eu/commission/presscorner/detail/en/ip\\_20\\_2077](https://ec.europa.eu/commission/presscorner/detail/en/ip_20_2077)
- IV. Diminuição da Proteção de Responsabilização – No outono de 2020, a Federal Communication Commission dos Estados Unidos abriu um processo para investigar a reformulação da Seção 230 da Lei de Decência das Comunicações para aumentar a responsabilidade por plataformas de mídia que censuram informações: [https://www.fcc.gov/ecfs/search/filings?proceedings\\_name=RM-11862](https://www.fcc.gov/ecfs/search/filings?proceedings_name=RM-11862). Embora esse esforço particular pareça estar em desacordo com os padrões internacionais de apoio à liberdade de expressão, a noção de que as empresas de mídia não têm direito à responsabilidade ilimitada está consagrada em inúmeros instantes da lei de difamação ao redor do mundo .
- V. Processo Penal – A Volkswagen (IAV GmbH) foi acusada de conspiração para fraudar os Estados Unidos, e vários funcionários receberam penas de prisão por suas atividades criminosas: <https://www.justice.gov/usao-edmi/us-v-volkswagen-16-cr-20394>



## Sascha Meinrath

Sascha Meinrath is the Palmer Chair in Telecommunications at Penn State and director of X-Lab, an innovative think tank focusing on the intersection of vanguard technologies and public policy. Professor Meinrath is a renowned technology policy expert and is internationally recognized for his work over the past two decades as a community internet pioneer, social entrepreneur, and angel investor.

Prior to founding X-Lab, Meinrath was vice president of the New America Foundation, where he founded the Open Technology Institute in 2008 and built it into one of the largest public interest tech policy organizations in Washington, D.C. He also founded the Commotion Wireless Project, which works around the globe to strengthen communities by providing tools to build their own local communications infrastructures, and co-founded Measurement Lab, a global online platform for researchers to deploy Internet measurement tools that empower the public and key decision-makers with useful information about broadband connectivity.

Professor Meinrath was elected as an Ashoka Fellow for Social Entrepreneurship in 2012, and has been named to the Time Magazine "Tech 40" as one of the most influential figures in technology, to the "Top 100" in Newsweek's Digital Power Index, and is a recipient of the Public Knowledge IP3 Award for excellence in public interest advocacy. He is widely published in both academic and media outlets, including Critical Studies in Media Communications, International Journal of Communications, Journal of Communications Law and Policy, Journal of Internet Law, Journal for Community Informatics, IEEE Internet Computing Magazine, IEEE Spectrum, Foreign Policy, The Hill, Time Magazine, Politico, Slate, The Guardian and many others.

Mr. Meinrath has been a vocal public intellectual and a leading voice calling for accountability over the governmental spying programs, and is at the forefront of D.C. policy debates over how Congress and the White House should rein in the cybersecurity-industrial complex. He serves as a board member for the American Indian Policy Institute, Brave New Software Foundation; Defending Rights and Dissent Foundation; Acorn Active Media Foundation; and Fourth Amendment Advisory Committee. He is also a member of the advisory councils for the Calyx Institute, FreedomBox Foundation, Loomio, and Whistleblower Aid.

Meinrath's research focuses on broadband connectivity, distributed communications, Digital Feudalism, Digital Craftsmanship, telecommunications and spectrum policy, cybersecurity and privacy, and the impacts of disruptive technology, and is a testament to his lifelong commitment to promoting social and economic justice -- values he embraced while attending a rough inner-city school in New Haven, Connecticut.



## Steven Mansour

Steven Mansour provides training and support to scientists, non-profits and community groups throughout Latin America since 2004. He has given Linux & Open Source Software workshops in Cuba, and works closely with the Fundación Canguro in Colombia, developing knowledge transfer strategies for doctors and researchers working with premature & low birth weight (LBW) infants. He was Director of Technology & Partnerships at the World Association of Young Scientists, a UNESCO project to support young scientists and early-career researchers. Steven worked closely with the McGill University Health Center, the Centre Hospitalier Universitaire Sainte-Justine and the Alberta Children's Hospital to develop social research and e-learning tools for professors and students in Mother-Child research. His work on Internet privacy and security has been featured in international media.



## Humza Jilani

Humza Jilani studies digital public policy and national security at the University of Oxford, where he reads for a Master of Philosophy in International Relations as a Marshall Scholar. His research explores the role of historical media networks, both online and offline, in fomenting political violence. Born and raised in Houston, Humza has researched terrorists' use of emerging technologies for Tech Against Terrorism, worked in business development in Karachi, Pakistan at rural development startup UpTrade and as an economic analyst at the Foreign, Commonwealth and Development Office in London, U.K., and spent a summer reporting on technology and defense for Foreign Policy magazine. Jilani graduated magna cum laude with highest honors in Social Studies from Harvard University.

## NOTAS E REFERÊNCIAS

- 1** See, e.g., the European Commission's Consultation on the Digital Services Act: <https://ec.europa.eu/digital-single-market/en/news/consultation-digital-services-act-package>.
- 2** "GARM: Brand Safety Floor + Suitability Framework." Global Alliance for Responsible Media. <https://wfanet.org/1/library/download/urn:uuid:7d484745-41cd-4cce-a1b9-a1b4e30928ea/garm+brand+safety+floor+suitability+framework+23+sept.pdf>.
- 3** "FD&C Act Chapter III: Prohibited Acts and Penalties." U.S. Food & Drug Administration. <https://www.fda.gov/regulatory-information/federal-food-drug-and-cosmetic-act-fdc-act/fdc-act-chapter-iii-prohibited-acts-and-penalties>. Also see, "Types of FDA Enforcement Actions." U.S. Food & Drug Administration. <https://www.fda.gov/animal-veterinary/resources-you/types-fda-enforcement-actions>.
- 4** "About the Division of Enforcement." U.S. Securities and Exchange Commission. <https://www.sec.gov/enforce/Article/enforce-about.html>.
- 5** "Learn About Volkswagen Violations." United States Environmental and Protection Agency. <https://www.epa.gov/vw/learn-about-volkswagen-violations>.
- 6** Zittrain, Jonathan and Jack M. Balkin. "A Grand Bargain to Make Tech Companies Trustworthy." *The Atlantic*, October 3, 2016. <https://www.theatlantic.com/technology/archive/2016/10/information-fiduciary/502346/>; Balkin, Jack M. "Information Fiduciaries and the First Amendment." *U.C. Davis Law Review* 49, no. 4 (2016): 1183-1283.
- 7** Guszczka, James, Iyad Rahwan, Will Bible, Manuel Cebrian, & Vic Katyal. "Why We Need to Audit Algorithms." *Harvard Business Review*, November 28, 2018. <https://hbr.org/2018/11/why-we-need-to-audit-algorithms>.
- 8** Toor, Amar. "Germany Passes Controversial Law to Fine Facebook over Hate Speech." *The Verge*, June 30, 2017. <https://www.theverge.com/2017/6/30/15898386/germany-facebook-hate-speech-law-passed>.
- 9** Stigler Committee on Digital Platforms, Final Report, September 2019. <https://www.chicagobooth.edu/-/media/research/stigler/pdfs/digital-platforms---committee-report---stigler-center.pdf>.
- 10** Citron, Danielle, and Benjamin Wittes. "The Internet Will Not Break: Denying Bad Samaritans § 230 Immunity." *Fordham Law Review* 86, no. 2 (2017): 401-23.