SERVIÇO PÚBLICO FEDERAL

UNIVERSIDADE FEDERAL DE UBERLÂNDIA

Faculdade de Direito Professor Jacy de Assis - FADIR

Gabriella Rodrigues dos Santos

ABORDAGEM DE ILICITOS CIBERNÉTICOS NAS REDES SOCIAIS, A RESPONSABILIDADE DAS PLATAFORMAS E AS IMPLICAÇÕES DA LGPD

Uberlândia-MG

2024

Gabriella Rodrigues dos Santos

ABORDAGEM DOS ILICITOS CIBERNÉTICOS NAS REDES SOCIAIS, A RESPONSABILIDADE DAS PLATAFORMAS E AS IMPLICAÇÕES DA LGPD

Artigo apresentado como Trabalho de Conclusão de Curso à Universidade Federal de Uberlândia-UFU, como requisito para obtenção parcial do título de bacharel em Direito.

Orientador: Prof.Dr Ricardo Padovini Pleti Ferreira

Aprovado em: _/_/_

Uberlândia-MG

2024

ABORDAGEM DOS ILICITOS CIBERNÉTICOS NAS REDES SOCIAIS, A RESPONSABILIDADE DAS PLATAFORMAS E AS IMPLICAÇÕES DA LGPD

APPROACH TO CYBERILÍCITOSS ON SOCIAL NETWORKS, PLATFORM RESPONSIBILITY, AND THE IMPLICATIONS OF THE LGPD

Gabriella Rodrigues dos Santos

Resumo: O presente artigo visa analisar os conceitos de Ilícitos cibernéticos cometidos nas plataformas de redes sociais, explorando suas características principais e a responsabilidade das plataformas envolvidas. Para isso, discute-se a legislação atual, incluindo o papel da Lei Geral de Proteção de Dados (LGPD) em situações que envolvem dados protegidos, além de apresentar casos concretos e comparações com o cenário global.

Palavras-chave: Ilícitos cibernéticos, Responsabilidade das Plataformas, Globalização, Proteção de Dados, Legislação Digital, Lei Geral de Proteção de Dados.

Abstract: This article aims to analyze the concepts of cyberIlícitoss committed on social media platforms, exploring their main characteristics and the responsibility of the involved platforms. It discusses current legislation, including the role of the General Data Protection Law (LGPD) in situations involving protected data, as well as presenting case studies and comparisons with the global landscape.

Key Words: CyberIlícitoss, Platform Responsibility, Globalization, Data Protection, Digital Legislation, General Data Protection Law (LGPD)

1.INTRODUÇÃO

A ascensão das redes sociais nas últimas décadas transformou profundamente a maneira como as pessoas se comunicam, interagem e consomem informações. Plataformas como Facebook, Twitter, Instagram e TikTok se tornaram ferramentas essenciais para a expressão individual, mobilização social e compartilhamento de conteúdo. Entretanto, essa nova dinâmica social também trouxe à tona uma série de problemas, incluindo a disseminação de informações falsas, cyberbullying, e outros Ilícitoss cibernéticos que afetam a integridade e a segurança dos usuários.

O documentário "O Dilema das Redes Sociais" ilustra os desafios éticos e sociais associados ao uso dessas plataformas, revelando como elas exploram as vulnerabilidades humanas e manipulam comportamentos em busca de lucro. Essa exploração levanta questões cruciais sobre a responsabilidade das plataformas em prevenir e responder a Ilícitoss cibernéticos que ocorrem dentro de seus ambientes. Assim, é imperativo discutir não apenas a natureza desses Ilícitoss, mas também as implicações legais e éticas que surgem no contexto do Marco Civil da Internet e da Lei Geral de Proteção de Dados (LGPD).

Neste trabalho, analisaremos a abordagem dos Ilícitoss cibernéticos nas redes sociais, enfatizando a responsabilidade das plataformas e as obrigações que têm para proteger os usuários. A partir das lições apresentadas no documentário e da evolução das regulamentações, buscamos compreender como a legislação atual pode responder de maneira eficaz aos desafios impostos pela era digital, garantindo a segurança e a privacidade dos dados dos usuários.

2. DEFINIÇÃO DOS ILÍCITOSS CIBERNÉTICOS E AS REDES SOCIAIS

Ilícitoss cibernéticos são ações ilegais que utilizam a tecnologia da informação e a internet como ferramentas para a prática de delitos. Esses Ilícitoss podem ocorrer

de diversas formas, como invasão de sistemas, fraudes eletrônicas, roubo de identidade, disseminação de malware e espionagem virtual. Com o aumento da dependência da internet e dos dispositivos conectados, esses delitos têm se tornado cada vez mais frequentes e sofisticados, representando um desafio significativo para a segurança digital. A característica principal dos Ilícitoss cibernéticos é o uso de redes digitais para atingir vítimas, sejam elas pessoas físicas, empresas, governos ou outras organizações.

Um dos aspectos mais críticos dos Ilícitoss cibernéticos é a violação de dados, que envolve o roubo, manipulação ou uso indevido de informações pessoais e corporativas. Os Ilícitoss relacionados a dados têm crescido rapidamente, especialmente em plataformas digitais, onde os usuários compartilham e armazenam uma grande quantidade de informações sensíveis. Redes sociais, aplicativos de mensagens e serviços de e-commerce são alvos frequentes de criminosos que buscam acessar dados pessoais, financeiros e confidenciais, muitas vezes para a prática de fraudes de identidade, invasão de contas ou venda de informações no mercado negro.

Embora os Ilícitoss cibernéticos sejam cometidos por indivíduos, as plataformas digitais têm um papel crucial na prevenção e no combate a essas ações. A responsabilização dessas plataformas por Ilícitoss relacionados a dados é um tema de crescente relevância. A falha em proteger essas informações pode resultar em sanções legais e em responsabilização judicial, um aspecto que será explorado em maior detalhe ao longo deste trabalho.

2.1 CRESCIMENTO DOS ILICITOS ONLINE E SUAS CONSEQUÊNCIAS SOCIAIS

O Brasil ocupa o segundo lugar entre os países mais afetados por Ilícitoss cibernéticos na América Latina, de acordo com uma pesquisa da empresa de segurança Fortinet. Os dados revelam que, somente em 2022, foram registradas aproximadamente 103,1 bilhões de tentativas de ataques.

Esses dados se tornam ainda mais preocupantes quando consideramos que a maior parte desses Ilícitoss cibernéticos está relacionada ao roubo de dados e à fraude de identidade. Isso evidencia o risco crescente para a privacidade e segurança das informações pessoais dos usuários, além do impacto financeiro e social causado por esses ataques.

Na ausência de uma legislação específica para Ilícitoss eletrônicos, os tribunais brasileiros têm enfrentado e punido internautas, crackers e hackers que utilizam a internet para cometer delitos. A maioria dos magistrados, advogados e consultores jurídicos considera que cerca de 95% dos Ilícitoss praticados eletronicamente já estão previstos no Código Penal brasileiro, por serem infrações comuns realizadas por meio da internet. Os 5% restantes, que ainda carecem de um enquadramento jurídico adequado, envolvem transgressões que ocorrem exclusivamente no ambiente virtual, como a disseminação de vírus, cavalos de tróia e worms (vermes).

3. A RESPONSABILIDADE CIVIL DAS PLATAFORMAS

No Brasil, as plataformas digitais que hospedam conteúdos gerados por usuários (como redes sociais, sites de compartilhamento de vídeos e fóruns) têm responsabilidades legais relacionadas a esses conteúdos, mas o regime de responsabilidades é regulado principalmente pelo **Marco Civil da Internet** (Lei n.º 12.965/2014).

As plataformas **não são automaticamente responsáveis** pelo conteúdo postado por seus usuários. Elas só podem ser responsabilizadas civilmente por danos causados por terceiros (usuários) se, após **ordem judicial**, não removerem o conteúdo considerado ilícito.

- **Ordem judicial**: A plataforma só tem obrigação de remover conteúdos gerados por usuários que sejam considerados ofensivos, caluniosos, ou que violem os

[1]direitos de outrem após uma decisão judicial que determine a remoção do conteúdo. Se não removerem após essa ordem, podem ser responsabilizadas por danos.

Porém, o assunto é diferente quando se trata de direitos autorais, para questões relacionadas à violação de **direitos autorais**, as plataformas podem ser obrigadas a remover conteúdos infratores sem a necessidade de ordem judicial, desde que notificadas diretamente pelo titular dos direitos, conforme previsto na **Lei de Direitos Autorais.**

O caso Botelho vs. Google é um exemplo significativo de questões de direitos autorais e a responsabilidade das plataformas digitais no Brasil.

O caso envolve o artista Eros Botelho, que é um cantor e compositor brasileiro, e a Google Brasil, proprietária do YouTube, uma plataforma de compartilhamento de vídeos onde a música é frequentemente utilizada e monetizada.

Eros Botelho moveu uma ação contra o Google após perceber que suas músicas estavam sendo reproduzidas no YouTube sem a devida autorização ou compensação financeira. Botelho alegou que as obras estavam sendo utilizadas em vídeos de terceiros, que, por sua vez, geravam receita publicitária, sem que ele fosse creditado ou remunerado adequadamente por isso.

O caso foi levado à Justiça, e a 4ª Turma do Superior Tribunal de Justiça (STJ) decidiu que o Google, na qualidade de intermediário, deveria ter responsabilidade em relação ao conteúdo que disponibiliza na plataforma. O tribunal destacou que, embora o YouTube não seja o criador do conteúdo, ele deve agir para garantir que as obras protegidas por direitos autorais sejam respeitadas e que os direitos dos autores sejam assegurados.

Como resultado da decisão, o Google foi instado a adotar medidas mais rigorosas para garantir que as músicas e outros conteúdos protegidos por direitos

[1] BRASIL. Superior Tribunal de Justiça. Recurso Especial nº 1.707.859/RJ. Relator: Ministro Luis Felipe Salomão. Julgado em: 30 set. 2019. Disponível em: <https://www.stj.jus.br/portal/portal_stj/publicacao/portal_stj_19/portal_stj_19_noticias/portal_stj_19_publicacao_4031/portal_stj_19_acompanhamento/portal_stj_19_detalhe/2019/10/01/16099/1.707.859-RJ>. Acesso em: 27 out. 2024.

autorais fossem utilizados de forma adequada, promovendo a necessidade de sistemas de identificação e remoção de conteúdo que infrinja direitos autorais. Além disso, o caso reforçou a importância da plataforma em colaborar com os titulares de direitos para evitar a violação de suas obras.

Esse caso é emblemático por abordar a responsabilidade das plataformas digitais na proteção dos direitos autorais, destacando que, mesmo que não sejam os criadores do conteúdo, elas têm um papel fundamental na supervisão e regulação do que é compartilhado em suas plataformas. A decisão também reforça a necessidade de um diálogo contínuo entre criadores de conteúdo e plataformas, promovendo um ambiente mais justo e transparente para todos os envolvidos na cadeia de produção artística.

. EXEMPLIFICAÇÃO DE CASOS PRÁTICOS (TELEGRAM E X)

A análise de casos de Ilícitoss cibernéticos no Brasil é crucial para compreender suas repercussões no ambiente digital atual. Com o aumento da utilização das plataformas online, esses delitos têm impactado tanto indivíduos quanto instituições, gerando preocupações relacionadas à segurança pública e à proteção de dados. Neste tópico, serão apresentados e discutidos dois casos emblemáticos de Ilícitoss cibernéticos, evidenciando a gravidade dessas ameaças e a necessidade de uma regulação adequada.

CASO TELEGRAM NO BRASIL

O bloqueio do Telegram no Brasil em 2022 foi um episódio significativo que envolveu questões de regulamentação, desinformação e a responsabilidade das plataformas digitais. O caso se desenrolou em março de 2022, quando o Tribunal de Justiça de São Paulo (TJ-SP) decidiu suspender o funcionamento do aplicativo devido à sua falta de cooperação em investigações sobre a disseminação de informações falsas e conteúdo ilegal.

Em 2022, as autoridades brasileiras expressaram insatisfação com a postura do Telegram em relação a investigações e solicitações feitas pela Justiça. O Tribunal Superior Eleitoral (TSE), encarregado de supervisionar as eleições no Brasil, solicitou

a colaboração do Telegram por vários meses para ajudar a combater a disseminação de fake news em canais políticos.

Além disso, o Ministério Público Federal, que investiga Ilícitoss na internet, buscou discutir estratégias para enfrentar delitos como pornografia infantil e comércio de armas na plataforma. No entanto, diversas cartas judiciais foram ignoradas, e uma comunicação enviada para a sede da empresa em Dubai chegou a ser devolvida ao TSE.

Em março de 2022, o ministro Alexandre de Moraes, a pedido da Polícia Federal, decidiu suspender a operação do Telegram no Brasil, argumentando que a empresa não estava cumprindo ordens judiciais. Em seu despacho, Moraes destacou que "o aplicativo Telegram é amplamente reconhecido por sua falta de cooperação com autoridades judiciais e policiais de vários países, usando essa postura como uma vantagem competitiva em relação a outros aplicativos de comunicação, o que o transforma em um ambiente propício para a disseminação de conteúdos ilegais, incluindo atividades criminosas".

A determinação teve impacto imediato. O bilionário Pavel Durov, fundador do Telegram, se desculpou com Moraes, levando o ministro a revogar rapidamente a ordem de bloqueio.

CASO X NO BRASIL

O ministro do Supremo Tribunal Federal (STF), Alexandre de Moraes, determinou, na sexta-feira (30), a suspensão imediata das atividades do X (antigo Twitter) em todo o Brasil. Essa decisão ocorreu após uma intimação apresentada pelo ministro, que estabeleceu um prazo de 24 horas para que Elon Musk, proprietário da rede social, designe um representante legal no país.

O principal motivo para o banimento do aplicativo X no Brasil estava relacionado à segurança dos dados dos usuários. A plataforma foi acusada de não cumprir a Lei Geral de Proteção de Dados (LGPD), que exige que as empresas tratem as informações pessoais de forma segura e transparente. Entre as acusações, destacou-se a coleta inadequada de dados, pois o aplicativo teria obtido informações dos usuários sem o devido consentimento.

Além disso, as informações dos usuários brasileiros eram armazenadas em servidores localizados fora do Brasil, o que aumentava o risco de vazamentos e uso indevido desses dados. A falta de clareza da plataforma em relação ao processamento e à utilização das informações dos usuários também foi uma preocupação significativa. Diante dessas falhas, o governo brasileiro decidiu retirar o app das lojas de aplicativos, como Google Play e App Store, o que impediu novos downloads e atualizações.

Renata Mieli, coordenadora do Comitê Gestor da Internet (CGI) no Brasil, ressalta a necessidade de regular as plataformas digitais. Ela argumenta que essa regulação é fundamental para assegurar que o debate público ocorra dentro dos parâmetros da legislação brasileira, proporcionando segurança jurídica tanto para os usuários quanto para as plataformas. Além disso, essa regulação ajudaria a orientar as decisões do Judiciário brasileiro.

A plataforma estava bloqueada no país desde 31 de agosto de 2024, por determinação de Moraes, após não cumprir um prazo de 24 horas para indicar um representante no Brasil e atender a ordens judiciais. O ministro autorizou o restabelecimento do serviço na terça-feira seguinte, após a empresa confirmar ao STF que havia cumprido as determinações judiciais e a Procuradoria-Geral da República se manifestar a favor do desbloqueio.

A liberação ocorreu depois que o X comprovou ter indicado um representante legal no Brasil, bloqueado perfis de nove investigados no STF e pago R$ 28,6 milhões em multas pela demora em atender a essas ordens de exclusão das contas.

Em conclusão, a análise do comportamento das plataformas em relação à legislação brasileira evidência que, para a continuidade de suas operações no país, foi necessário que essas empresas se sujeitassem às normas e exigências locais. A conformidade com a legislação, especialmente a Lei Geral de Proteção de Dados, ressalta a importância da responsabilidade e da transparência nas práticas dessas plataformas, refletindo a relação intrínseca entre regulação e operação no Brasil.

3. LEGISLAÇÃO ATUAL E O MODO DE DENUNCIAR

Os Ilícitoss cibernéticos possuem particularidades que os distinguem dos Ilícitoss convencionais e que desafiam a legislação vigente. Primeiramente, destacam-

se pela atuação em ambiente virtual, com caráter transnacional, onde a ausência de fronteiras físicas permite que o agente realize ações ilícitas a partir de uma jurisdição, impactando vítimas em diversas outras, o que demanda cooperação internacional para sua investigação e repressão.

Outra característica fundamental é o anonimato, uma vez que a infraestrutura da internet possibilita ao infrator ocultar sua identidade, empregando métodos de mascaramento da origem das atividades criminosas, o que dificulta a identificação do autor. Além disso, os Ilícitoss cibernéticos frequentemente demandam elevado grau de sofisticação técnica, envolvendo conhecimentos específicos em tecnologia e segurança da informação, como ocorre em ataques de engenharia social e de negação de serviço (DDoS).

O potencial lesivo e o alcance dos Ilícitoss virtuais são também características marcantes, pois estes delitos podem gerar danos em larga escala, atingindo múltiplas vítimas simultaneamente, seja por meio de fraudes financeiras, roubo de dados, espionagem ou disseminação de desinformação. Essa potencialidade lesiva é reforçada pela rapidez com que podem ser executados e pela celeridade das consequências, como vazamentos de dados e fraudes instantâneas.

A dificuldade de rastreamento e investigação desses Ilícitoss também se destaca, pois o agente pode ocultar ações e deletar informações rapidamente, e o uso de criptografia e redes privadas (VPNs) complexifica o rastreamento pelas autoridades competentes. Essas características exigem, portanto, um tratamento jurídico específico, que considere a necessidade de métodos de investigação e punição diferenciados, adequados à natureza única do ambiente digital e à dinâmica desses Ilícitoss.

As principais leis que tipificam Ilícitoss cibernéticos e as penas correspondentes, além de observar que existem dispositivos no Código Penal aplicáveis a delitos digitais:

- **Lei nº 12.737/2012** (conhecida como Lei Carolina Dieckmann) – Define Ilícitoss informáticos, como invasão de dispositivos e violação de dados de usuários, estabelecendo sanções específicas para essas práticas.

- **Lei nº 12.965/2014** (Marco Civil da Internet) – Regula o uso da internet no Brasil e estabelece direitos e responsabilidades para usuários e provedores, garantindo a privacidade e a liberdade de expressão.
- **Lei nº 13.709/2018** (Lei Geral de Proteção de Dados) – Protege dados pessoais, especificando normas para a coleta, armazenamento e compartilhamento de informações, com o objetivo de garantir a privacidade e promover a transparência em operações que envolvem dados.

No Brasil, as denúncias de Ilícitoss cibernéticos são formalizadas junto às autoridades competentes, permitindo às vítimas recorrer ao sistema judiciário para assegurar seus direitos. Além disso, é possível acionar diretamente as plataformas onde ocorreram os delitos, embora cada rede social tenha seu próprio modo de lidar com esses casos. Esse procedimento reflete a forma atual de abordar legalmente esses Ilícitoss, combinando o papel das autoridades com a atuação das plataformas para proteger os direitos das vítimas e responsabilizar os envolvidos.

4. EXEMPLOS DE LEGISLAÇÃO ESTRANGEIRA

A responsabilidade das plataformas online sobre conteúdos postados por seus usuários é um tema complexo e de grande relevância, especialmente no contexto atual em que as redes sociais e outras plataformas digitais desempenham um papel central na disseminação de informações. A discussão envolve aspectos jurídicos, éticos e sociais, e é marcada por diversas legislações e jurisprudências ao redor do mundo.

- Estados Unidos: A Seção 230 do Communications Decency Act é uma das mais notórias, pois protege as plataformas de serem responsabilizadas por conteúdos postados por terceiros. Isso incentiva a inovação e a liberdade de expressão, mas também levanta questões sobre a desinformação e o discurso de ódio.

Nos Estados Unidos, a abordagem em relação aos Ilícitoss cibernéticos e à proteção de dados é complexa e fragmentada, refletindo a estrutura federalista do país. Ao

[2]contrário de muitos países que possuem uma legislação abrangente sobre proteção de dados, como a LGPD no Brasil ou o GDPR na União Europeia, os EUA contam com uma variedade de leis que variam conforme o setor. Existem normas específicas que tratam de aspectos da proteção de dados, como a Health Insurance Portability and Accountability Act (HIPAA), que se aplica a dados de saúde, e a Children's Online Privacy Protection Act (COPPA), que protege dados de crianças. Contudo, não há uma legislação federal única que aborde todos os dados pessoais.

Além disso, muitos estados, como a Califórnia, têm adotado suas próprias leis de proteção de dados. A California Consumer Privacy Act (CCPA), por exemplo, estabelece direitos para os consumidores em relação aos seus dados pessoais, similar ao GDPR europeu. Esse mosaico legislativo resulta em uma abordagem descentralizada, onde as empresas são incentivadas a implementar medidas robustas de segurança para proteger os dados dos usuários. Falhas de segurança que levam a vazamentos de dados podem resultar em ações judiciais e sanções, mas as penalidades não são tão severas quanto em algumas jurisdições internacionais.

No que tange aos Ilícitoss cibernéticos, eles são tratados sob várias leis federais, sendo o Computer Fraud and Abuse Act (CFAA) uma das principais normas, criminalizando o acesso não autorizado a computadores e sistemas. O combate aos Ilícitoss cibernéticos é uma prioridade crescente, e as agências federais, como o FBI, possuem unidades especializadas para investigar essas infrações. Em razão do aumento de incidentes cibernéticos, iniciativas de colaboração entre o setor público e privado têm sido promovidas para melhorar a segurança cibernética.

---

[2] **Health Insurance Portability and Accountability Act (HIPAA)**: U.S. Department of Health & Human Services. **Health Insurance Portability and Accountability Act of 1996**. Disponível em: https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html. Acesso em: 27 out. 2024.

 Children's Online Privacy Protection Act (COPPA): U.S. Federal Trade Commission. **Children's Online Privacy Protection Act of 1998**. Disponível em: https://www.ftc.gov/business-guidance/privacy-security/children%27s-online-privacy-protection-rule. Acesso em: 27 out. 2024.

 California Consumer Privacy Act (CCPA): State of California. **California Consumer Privacy Act (CCPA)**. Disponível em: https://oag.ca.gov/privacy/ccpa. Acesso em: 27 out. 2024.

 Computer Fraud and Abuse Act (CFAA): U.S. Department of Justice. **Computer Fraud and Abuse Act**. Disponível em: https://www.law.cornell.edu/uscode/text/18/1030. Acesso em: 27 out. 2024.

Entretanto, a abordagem fragmentada dos EUA pode resultar em lacunas na proteção de dados e na responsabilização por Ilícitoss cibernéticos. A discussão sobre a necessidade de uma legislação federal unificada continua a evoluir, com uma crescente demanda por normas que ofereçam uma abordagem mais coesa à proteção da privacidade e dos dados pessoais. Essa realidade reflete um desafio significativo tanto para as empresas quanto para os consumidores, que enfrentam incertezas em relação à privacidade e à segurança de seus dados na era digital.

- **União Europeia:** A Diretiva de Comércio Eletrônico estabelece que os provedores não são responsáveis por conteúdos de usuários, mas com a entrada em vigor do Regulamento Geral sobre a Proteção de Dados (GDPR), a responsabilidade das plataformas em relação à privacidade e proteção de dados pessoais ganhou maior destaque.

Esse sistema reconhece a necessidade de incentivar o setor privado a cumprir funções de interesse público, sendo assim, a estrutura de responsabilização prevista na Diretiva do Comércio Eletrônico é mantida, ou seja, ela se aplica apenas nos casos em que há conhecimento efetivo de conteúdo ou atividades ilegais e a falta de ação para removê-los. Ao mesmo tempo, o regulamento introduz uma supervisão mais rigorosa, sujeitando as atividades privadas das empresas às normas do bloco europeu, tanto em termos substanciais quanto processuais.

Brasil: No Brasil, a responsabilidade de uma plataforma digital (provedor de conteúdo) só se efetiva por meio de uma ordem judicial para a remoção de um conteúdo. Se um usuário se sentir prejudicado de alguma maneira, ele pode notificar a rede social solicitando a retirada do conteúdo, mas a decisão sobre a remoção fica a critério da plataforma. Por outro lado, se o usuário recorrer à justiça e obter uma ordem judicial, o provedor é obrigado a retirar o conteúdo, sob pena de ser responsabilizado civilmente por ele.

Esse é o entendimento estabelecido pelo ordenamento jurídico brasileiro, conforme a Lei 12.965/2014 (Marco Civil da Internet) e a jurisprudência do STJ.

> *Art. 19. Com o intuito de assegurar a liberdade de expressão e impedir a censura, o provedor de aplicações de internet somente poderá ser responsabilizado civilmente por danos decorrentes de conteúdo gerado por terceiros se, após ordem judicial específica, não tomar as providências para, no âmbito e nos limites técnicos do seu serviço e dentro do prazo assinalado, tornar indisponível o conteúdo apontado como infringente, ressalvadas as disposições legais em contrário.*
>
> *§ 1º A ordem judicial de que trata o caput deverá conter, sob pena de nulidade, identificação clara e específica do conteúdo apontado como infringente, que permita a localização inequívoca do material.*
>
> *§ 2º A aplicação do disposto neste artigo para infrações a direitos de autor ou a direitos conexos depende de previsão legal específica, que deverá respeitar a liberdade de expressão e demais garantias previstas no art. 5º da Constituição Federal.*
>
> *§ 3º As causas que versem sobre ressarcimento por danos decorrentes de conteúdos disponibilizados na internet relacionados à honra, à reputação ou a direitos de personalidade, bem como sobre a indisponibilização desses conteúdos por provedores de aplicações de internet, poderão ser apresentadas perante os juizados especiais.*

Ainda, no Congresso Nacional, o Projeto de Lei 2630, popularmente chamado de "PL das Fake News", tem como objetivo estabelecer a Lei Brasileira de Liberdade, Responsabilidade e Transparência na Internet. Essa legislação pretende regular o uso das plataformas digitais no Brasil, implementando ações para combater a disseminação de informações falsas nas redes sociais e responsabilizando as empresas de tecnologia por sua inação diante da desinformação. O projeto já recebeu aprovação no Senado e agora aguarda análise pelo plenário da Câmara dos Deputados.

5. PENSAMENTOS DIVERGENTES E CRÍTICAS

Entendimento de que as plataformas não são responsáveis - As plataformas, por sua vez, argumentam que a fiscalização e a verificação prévia do conteúdo gerado por seus usuários são inviáveis. Elas afirmam que responsabilizá-las por danos causados a terceiros violaria o direito à liberdade de expressão e poderia levar a uma censura prévia indiscriminada. Além disso, sustentam que a imposição de uma responsabilidade mais severa afetaria sua viabilidade operacional, técnica e financeira, limitando também a livre manifestação dos usuários na internet.

O dilema central que permeia a discussão sobre a responsabilidade das plataformas online é a tensão entre liberdade de expressão e privacidade. De um lado, a liberdade de expressão é um direito fundamental que garante a todos a possibilidade de se manifestar, compartilhar ideias e participar de debates públicos. Por outro lado, a privacidade e a proteção dos direitos individuais são igualmente essenciais, especialmente em um ambiente digital onde informações pessoais podem ser facilmente divulgadas ou mal utilizadas.

Nesse cenário, surge a questão da responsabilidade civil ou criminal daqueles que participam da criação e disseminação de conteúdo. Os usuários precisam estar cientes de que, ao se expressar online, podem estar, inadvertidamente, infringindo direitos de terceiros, como o direito à honra, à imagem e à privacidade. A linha que separa a liberdade de expressão de um ato ilícito pode ser tênue e, muitas vezes, subjetiva, o que torna essencial que cada indivíduo conheça seus direitos e os limites que a lei impõe.

Além disso, a falta de compreensão sobre essas questões pode levar a consequências significativas, como a responsabilização por danos morais ou materiais. Por isso, é crucial que os usuários da internet se informem sobre as leis vigentes e as diretrizes das plataformas que utilizam. O entendimento dos seus direitos e das suas responsabilidades não apenas ajuda a prevenir conflitos, mas também promove um ambiente digital mais seguro e respeitoso.

O desafio, portanto, é encontrar um equilíbrio entre o exercício da liberdade de expressão e a proteção dos direitos individuais, sempre em conformidade com as normas legais. Essa busca é fundamental para garantir que a internet permaneça um espaço de diálogo e troca de ideias, sem que isso resulte em violações de direitos ou em consequências legais indesejadas.

6. PENSAMENTOS DIVERGENTES

Diante desse novo cenário de regulação, surge a necessidade de o Estado se adaptar. A discussão não pode mais se restringir à regulação estatal, uma vez que existe um espaço transnacional onde diversas normas competem e onde agentes privados estabelecem a "regra vigente" (BALKIN, 2014, p. 2325). Esses agentes frequentemente ignoram jurisdições locais em favor de regulamentações mais influentes, seja por meio da adequação de suas estratégias de mercado ou pelas vantagens oferecidas pelos regimes de responsabilidade desses Estados, entre outros fatores. Essa dinâmica resulta em uma inversão do fluxo normativo, em que as empresas determinam como a liberdade de expressão será regulada online, fazendo com que usuários ao redor do mundo se submetam a uma regra única e geral, muitas vezes influenciada por pressões de governos estrangeiros.

Como o controle do conteúdo que circula na Internet está, em grande parte, nas mãos de entidades privadas, como as plataformas digitais, esses agentes assumem um papel central na regulação de seus próprios ambientes virtuais. Os Estados parecem ser insuficientes para monitorar e prevenir violações a direitos na Internet, como a liberdade de expressão, por meio de suas legislações nacionais. Seja devido a pressões estatais, incentivos de mercado ou demandas de organizações da sociedade civil, as plataformas incorporam legislações estatais em seus termos de uso, exercendo uma autorregulação que não distingue entre usuários, independentemente de sua localização.

[3]**A Favor da Responsabilidade**: Alguns juristas argumentam que as plataformas devem ser responsabilizadas por conteúdos prejudiciais, uma vez que lucram com a atividade de seus usuários. Essa visão defende que a responsabilidade deve ser proporcional à capacidade de controle das plataformas sobre o que é publicado. (achar alguém)

Em 30 de março de 2019, Mark Zuckerberg, CEO e fundador do Facebook, publicou um artigo no Washington Post reconhecendo a necessidade de regulamentação para sua plataforma. Essa não foi a primeira vez que abordou o tema. Em um depoimento a um comitê do Congresso dos Estados Unidos em 2018, ele respondeu a perguntas de parlamentares, admitindo pela primeira vez que "nossa posição não é de que a regulação seja negativa. A verdadeira questão é: qual é a estrutura adequada? Os detalhes são importantes" (VALENTE, 2018).

Para Renata Mieli, anteriormente citada, “A discussão da regulação das plataformas de rede social é tão central para a democracia e para o mundo contemporâneo, porque são empresas que lidam com uma atividade que é de interesse social, de interesse público, que é justamente a discussão sobre os temas da sociedade, não apenas os políticos e eleitorais, mas os temas da saúde pública, os temas da cultura, os temas do esporte, o entretenimento, tudo isso compõe a esfera pública de debates que acontece hoje de forma muito predominante no interior dessas empresas. Portanto, essas empresas precisam estar em aderência às legislações do país, porque elas lidam com um insumo que é essencial para garantia do Estado Democrático de Direito”

- Contra a Responsabilidade: Outros defendem que a responsabilização excessiva pode levar à censura e à limitação da liberdade de expressão. O temor é

---

[3] Renata Mielli: “Marco Civil da Internet não é uma legislação que foi feita para regular plataformas”Disponível em: https://www.youtube.com/watch?v=FwT-W7aRupY
ZUCKERBERG, Mark. Internet needs new rules. *Los Angeles Times*, 30 mar. 2019. Disponível em: https://www.latimes.com/opinion/op-ed/la-oe-mark-zuckerberg-internet-needs-new-rules-20190330-story.html. Acesso em: 17 out. 2024.

[4]que as plataformas adotem medidas excessivas para evitar responsabilidades, resultando em uma autocensura que prejudica a diversidade de vozes.

Segundo Bucci (2020), jornalista e professor da Universidade de São Paulo, a liberdade de expressão nas redes é essencial para a manutenção de um espaço público democrático. Em seu artigo Direito de livre expressão e direito social à informação na era digital, ele argumenta que, embora não seja contrário à regulamentação das plataformas, considera que a responsabilidade excessiva dessas empresas pode levar a práticas de censura, prejudicando o livre acesso à informação. Bucci alerta que um controle demasiado poderia impactar negativamente a diversidade de opiniões e o exercício da cidadania, ameaçando a "natureza pública" da internet e das redes sociais.

O debate sobre a responsabilidade das plataformas online é dinâmico e continua evoluindo. Com o crescimento da inteligência artificial e a automação na moderação de conteúdos, surgem novas questões sobre a eficácia dessas ferramentas e a possibilidade de erros que podem levar à remoção indevida de conteúdo.

Além disso, a pressão por regulação mais rigorosa tem aumentado, especialmente após escândalos relacionados à desinformação e discursos de ódio nas redes sociais. A busca por um equilíbrio entre liberdade de expressão e proteção dos usuários é um desafio que requer a colaboração entre legisladores, plataformas e sociedade civil.

A responsabilidade das plataformas online é uma questão multifacetada que envolve a análise de legislações, decisões judiciais e a opinião pública. A evolução

---

[4] BUCCI, EUGÊNIO. Independência dos veículos frente ao governo e vigência de regras públicas são essenciais à garantia da liberdade de expressão e do direito à informação.

BUCCI, Eugênio. Direito de livre expressão e direito social à informação na era digital. Revista Brasileira de Política Internacional, Brasília, v. 63, n. 2, p. 1-18, 2020.

das tecnologias e das práticas sociais exigirá uma constante revisão das normas e um diálogo aberto entre todas as partes interessadas. A construção de um ambiente digital seguro e justo é um objetivo que deve ser perseguido coletivamente, respeitando a pluralidade de opiniões e a proteção de direitos fundamentais.

7. A LGPD E SUA APLICAÇÃO

A Lei Geral de Proteção de Dados (LGPD), instituída pela Lei nº 13.709/2018, é a principal legislação brasileira voltada para a proteção dos dados pessoais. Ela estabelece regras sobre a coleta, armazenamento, uso e compartilhamento de dados pessoais por organizações, públicas ou privadas, com o objetivo de proteger a privacidade dos cidadãos e garantir maior transparência. A LGPD também define direitos dos titulares de dados, como o acesso e correção de suas informações, e impõe responsabilidades às empresas para implementar medidas de segurança, além de penalidades para quem não seguir as normas.

Os titulares de dados possuem uma série de direitos garantidos pela Lei Geral de Proteção de Dados (LGPD), que visam assegurar o controle sobre suas informações pessoais. Entre esses direitos, destacam-se o acesso aos dados coletados, a correção de informações incorretas ou desatualizadas, a eliminação ou anonimização de dados quando o tratamento for desnecessário, e a portabilidade dos dados para outras empresas ou serviços. Além disso, o titular pode solicitar informações sobre o compartilhamento de seus dados com terceiros, bem como revogar o consentimento previamente concedido. Outro direito importante é a possibilidade de solicitar a revisão de decisões automatizadas que possam impactá-lo de maneira significativa.

As plataformas digitais, por sua vez, possuem diversas obrigações relacionadas ao tratamento de dados pessoais. Entre as principais responsabilidades, destaca-se a necessidade de garantir a segurança dos dados, implementando medidas técnicas e administrativas adequadas para evitar vazamentos ou acessos indevidos. Quando há um incidente de segurança que compromete os dados, a plataforma deve comunicar o fato à Autoridade Nacional de Proteção de Dados

(CNPD) e aos titulares afetados. As plataformas também precisam oferecer mecanismos claros para que os usuários possam exercer seus direitos, além de fornecer transparência sobre como os dados estão sendo utilizados.

No que tange aos Ilícitoss que ocorrem dentro dessas plataformas, elas devem disponibilizar mecanismos eficazes para que os usuários possam realizar denúncias. Um dos formatos mais comuns são os botões de denúncia integrados, presentes em redes sociais e outros serviços online, que permitem que os usuários relatem comportamentos inadequados ou ilícitos diretamente na plataforma. Além disso, muitas plataformas oferecem formulários específicos para que os usuários detalhem o ocorrido e anexem evidências, quando necessário, como por exemplo o Instagram, que irá analisar o conteúdo da denúncia fornecida. Outras opções incluem o contato direto com o suporte ao cliente ou a utilização de sistemas automatizados de moderação, que usam inteligência artificial para detectar atividades suspeitas. Em casos de Ilícitoss mais graves, as plataformas são obrigadas a cooperar com as autoridades, fornecendo informações relevantes, sempre em conformidade com as normas de proteção de dados e privacidade.

Essas medidas demonstram o compromisso das plataformas em manter um ambiente digital seguro e em conformidade com a legislação de proteção de dados, equilibrando o respeito aos direitos dos titulares com a necessidade de prevenir e combater Ilícitoss cibernéticos.

7.1 A RELAÇÃO ENTRE A LGPD, A RESPONSABILIDADE DAS PLATAFORMAS DIGITAIS E OS ILÍCITOSS CIBERNÉTICOS

A LGPD, ao estabelecer normas rigorosas para a coleta e o tratamento de dados pessoais, evidencia a importância da proteção da privacidade dos usuários. Em um cenário digital onde as plataformas frequentemente solicitam dados sensíveis, como informações de contato, localização e dados financeiros, a responsabilidade delas em assegurar a segurança dessas informações é fundamental.

As plataformas digitais, ao coletar e processar dados pessoais, assumem a responsabilidade de proteger essas informações contra vazamentos e abusos, além de garantir que suas práticas estejam em conformidade com as diretrizes da LGPD. A

[5]não observância dessas normas pode resultar em penalidades previstas pela LGPD e claro, em um impacto negativo sobre a confiança dos usuários.

A recente legislação da LGPD contribui para o combate aos Ilícitoss cibernéticos ao impor exigências de maturidade em segurança da informação, o que torna as empresas menos suscetíveis a ataques cibernéticos e vazamentos de dados pessoais.

A Lei Geral de Proteção de Dados (LGPD) destaca-se por estabelecer um quadro rigoroso para a proteção de dados pessoais, o que faz com que os Ilícitoss cibernéticos voltados para dados se tornem uma preocupação significativa para as empresas. Com a implementação da LGPD, as organizações estão mais atentas aos riscos associados ao vazamento e à manipulação inadequada de informações pessoais, temendo punições que podem resultar de não conformidade com a lei.

A LGPD atua como um intermediário ao exigir que as empresas adotem medidas de segurança eficazes para proteger os dados que coletam e processam. Isso inclui a necessidade de realizar avaliações de riscos, implementar protocolos de segurança da informação e treinar colaboradores sobre boas práticas de manejo de dados. Assim, a legislação não apenas impõe responsabilidades às empresas, mas também promove uma cultura de segurança, estimulando-as a proteger proativamente os dados e, consequentemente, a reduzir a incidência de Ilícitoss cibernéticos.

CASO FACEBOOK

Um exemplo notório de vazamento de dados ocorreu com o Facebook em 2019, quando a empresa anunciou que 540 milhões de registros de usuários estavam expostos em servidores públicos da Amazon. Esses dados incluem informações como comentários, curtidas e reações de usuários, que foram armazenados em bancos de dados acessíveis sem a devida proteção. O caso levantou sérias preocupações sobre a segurança dos dados pessoais na plataforma, evidenciando a vulnerabilidade de redes sociais diante de práticas inadequadas de armazenamento de informações.

---

[5] *THE GUARDIAN. Facebook data leak: 540 million records exposed on Amazon servers. 4 abr. 2019. Disponível em: https://www.theguardian.com/technology/2019/apr/04/facebook-data-leak-540-million-records-exposed-aws. Acesso em: 27 out 2024.*

Esse incidente ilustra a problemática de como vazamentos de dados podem ocorrer nas redes sociais, especialmente quando as empresas não implementam medidas rigorosas de segurança da informação. A falta de controles adequados pode levar à exposição de informações sensíveis, colocando em risco a privacidade dos usuários e a integridade de suas contas. Além disso, tais vazamentos não apenas prejudicam a confiança dos usuários nas plataformas, mas também podem resultar em consequências legais para as empresas, que enfrentam sanções sob a LGPD caso não garantam a proteção adequada dos dados pessoais.

8. PERSPECTIVAS FUTURAS

No Brasil, a revisão do modelo atual está ocorrendo por meio de duas abordagens principais. De um lado, o Supremo Tribunal Federal está analisando a constitucionalidade do artigo 19 no RE 1.037.396/SP, no âmbito da repercussão geral (Tema 987). De outro lado, o Projeto de Lei 2.630/2020, conhecido como PL das Fake News, propõe a revogação do artigo 19 e a imposição de novas responsabilidades para as empresas.

No final de 2023, a discussão também começou a incluir uma terceira abordagem: a reforma do Código Civil. No relatório publicado pela Subcomissão de Direito Digital, sugere-se que a responsabilização das plataformas possa ocorrer de duas formas: pela reparação de danos causados por conteúdos que tenham sido distribuídos através de publicidade na plataforma, e pelo descumprimento sistemático das obrigações legais, o que poderia levar à revogação do dispositivo do Marco Civil da Internet por incompatibilidade com o novo contexto.

E por outro lado temos a proposta da Autorregulação Privada e Supervisão Pública, na qual é importante destacar como uma segunda possibilidade. Inspirada pelo Regulamento dos Serviços Digitais da União Europeia, a proposta da comissão estabelece diversas obrigações para os provedores de plataformas. Isso inclui a adoção de medidas que garantam a conformidade de seus sistemas com os direitos da personalidade e a liberdade de expressão; a prevenção e mitigação de danos por meio da gestão de riscos sistêmicos; a implementação de mecanismos eficazes de

reclamação que permitam aos usuários informar a plataforma sobre conteúdos ilegais; e a criação de termos de uso que sejam acessíveis e transparentes.

A proposta da comissão, portanto, rompe com a ideia convencional de que o Poder Judiciário é a única instância social confiável para a resolução de conflitos. Ela reconhece que existem diversas situações jurídicas em que danos irreparáveis podem ocorrer se a proteção dos direitos só for buscada por meio de processos judiciais.

Análise de propostas alternativas para a regulamentação

CONCLUSÃO

A análise dos Ilícitoss cibernéticos no Brasil evidencia um crescimento preocupante, demandando atenção redobrada das autoridades jurídicas e legislativas. O país enfrenta desafios significativos na regulamentação desse fenômeno, necessitando de uma abordagem que considere as legislações existentes, como a Lei Carolina Dieckmann, o Marco Civil da Internet e a Lei Geral de Proteção de Dados (LGPD), que visam mitigar tais infrações. É imprescindível reconhecer que, para operar no Brasil, as plataformas digitais devem se submeter à legislação nacional, um fator que se revela essencial na busca por um ambiente digital mais seguro.

Ademais, a discussão acerca da responsabilidade compartilhada entre usuários, plataformas e o governo se torna cada vez mais relevante. A regulamentação não apenas traria clareza em relação às obrigações das empresas, mas também serviria como um guia para futuras decisões judiciais, proporcionando um ambiente de segurança jurídica. Embora a questão da moderação de conteúdo esteja em pauta, é fundamental que se estabeleçam diretrizes claras para que as plataformas saibam quais requisitos legais devem atender.

Por fim, a necessidade de um marco regulatório específico para plataformas digitais no Brasil se torna evidente, contribuindo para a construção de um espaço digital que respeite os direitos dos usuários e promova a integridade do ambiente

online. A busca por um equilíbrio entre proteção de dados e liberdade de expressão é um aspecto crucial nesse processo, que deverá ser abordado com cautela e rigor, considerando a complexidade do cenário contemporâneo.

REFERÊNCIAS

ALBUQUERQUE, Roberto Paulino. **Notas sobre a teoria da Responsabilidade Civil sem danos**. Revista dos Tribunais, v.6, p.89-103, Jan/Mar. 2016.

BBC NEWS BRASIL. Por que o app X foi bloqueado no Brasil e depois liberado novamente. 8 out. 2024. Disponível em: https://www.bbc.com/portuguese/articles/cvgr0p67p65o. Acesso em: 27 out. 2024.

BRASIL DE FATO. Do Twitter ao fim do X: entenda os capítulos que levaram à decisão de derrubar a rede social no Brasil. 30 ago. 2024. Disponível em: https://www.brasildefato.com.br/2024/08/30/do-twitter-ao-fim-do-x-entenda-os-capitulos-que-levaram-a-decisao-de-derrubar-a-rede-social-no-brasil. Acesso em: 17 out. 2024.

BRASIL. Projeto de Lei n° 2630, de 2020. Altera a Lei n° 12.965, de 23 de abril de 2014, para instituir a Lei Brasileira de Liberdade, Responsabilidade e Transparência na Internet. 2020. Disponível em https://legis.senado.leg.br/sdleg-getter/documento?dm=8110634&disposition=inline . Acesso em: 28 out.2024.

BRASIL DE FATO. Como fica o debate público com o banimento do X no Brasil. 31 ago. 2024. Disponível em: https://www.brasildefato.com.br/2024/08/31/como-fica-o-debate-publico-com-o-banimento-do-x-no-brasil. Acesso em: 17 out. 2024.

BUCCI, Eugênio. Direito de livre expressão e direito social à informação na era digital. *Revista Brasileira de Política Internacional*, Brasília, v. 63, n. 2, p. 1-18, 2020. Disponível em: https://www.eca.usp.br/acervo/producao-academica/001725398.pdf . Acesso em: 27 out 2024..

GLOBO. X volta ao ar no Brasil. 8 out. 2024. Disponível em: https://g1.globo.com/tecnologia/noticia/2024/10/08/x-volta-ao-ar-brasil.ghtml. Acesso em: 27 out. 2024.

MIELI, Renata. A importância da regulação das plataformas digitais. *YouTube*, 17 out. 2023. Disponível em: https://www.youtube.com/watch?v=FwT-W7aRupY. Acesso em: 17 out. 2024.

CONJUR. Responsabilidade civil dos provedores de plataformas digitais no novo Código Civil. 24 mar. 2024. Disponível em: https://www.conjur.com.br/2024-mar-24/responsabilidade-civil-dos-provedores-de-plataformas-digitais-no-novo-cc/. Acesso em: 17 out. 2024.

U.S. DEPARTMENT OF HEALTH & HUMAN SERVICES. **Health Insurance Portability and Accountability Act of 1996**. Disponível em: https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html. Acesso em: 27 out. 2024.

U.S. FEDERAL TRADE COMMISSION. **Children's Online Privacy Protection Act of 1998**. Disponível em: https://www.ftc.gov/business-guidance/privacy-security/children%27s-online-privacy-protection-rule. Acesso em: 27 out. 2024.

STATE OF CALIFORNIA. **California Consumer Privacy Act (CCPA)**. Disponível em: https://oag.ca.gov/privacy/ccpa. Acesso em: 27 out. 2024.

U.S. DEPARTMENT OF JUSTICE. **Computer Fraud and Abuse Act**. Disponível em: https://www.law.cornell.edu/uscode/text/18/1030. Acesso em: 27 out. 2024.

ZUCKERBERG, M. The Internet needs new rules. Let's start in these four areas. Washington Post. Publicada em 30 de março de 2019.