XXX CONGRESSO NACIONAL DO CONPEDI FORTALEZA - CE

CONSTITUIÇÃO, TEORIA CONSTITUCIONAL E DEMOCRACIA II

FRANCISCO TARCÍSIO ROCHA GOMES JÚNIOR

LUIZ GUSTAVO GONÇALVES RIBEIRO

C755

Constituição, teoria constitucional e democracia II [Recurso eletrônico on-line] Organização CONPEDI

Coordenadores: Francisco Tarcísio Rocha Gomes Júnior; Luiz Gustavo Gonçalves Ribeiro. – Florianópolis: CONPEDI, 2023.

Inclui bibliografia
ISBN: 978-65-5648-843-1
Modo de acesso: www.conpedi.org.br em publicações
Tema: Saúde: Acesso à justiça, Solução de litígios e Desenvolvimento

1. Direito – Estudo e ensino (Pós-graduação) – Encontros Nacionais. 2. Constituição. 3. Teoria constitucional e democracia. XXX Congresso Nacional do CONPEDI Fortaleza - Ceará (3; 2023; Florianópolis, Brasil).

CDU: 34

Conselho Nacional de Pesquisa
e Pós-Graduação em Direito Florianópolis
Santa Catarina – Brasil
www.conpedi.org.br

XXX CONGRESSO NACIONAL DO CONPEDI FORTALEZA - CE

CONSTITUIÇÃO, TEORIA CONSTITUCIONAL E DEMOCRACIA II

Apresentação

O XXX Congresso Nacional do CONPEDI – Fortaleza-CE teve como tema central “Acesso à justiça, solução de litígios e desenvolvimento”. O evento foi marcado pelo encontro de pesquisadores, coordenadores de programas de pós-graduação stricto sensu, professores, estudantes de pós-graduação e de graduação de todo o Brasil.

Os artigos apresentados no GT “Constituição, Teoria Constitucional e Democracia II” tiveram como característica principal uma abordagem interdisciplinar, em que a ciência política serviu de instrumental teórico, juntamente com o instrumental teórico jurídico, para a compreensão da atuação da jurisdição constitucional brasileira em seus desafios contemporâneos.

O artigo “Ensino superior no contexto neoliberal: de direito constitucional a mercadoria” teve como objeto refletir sobre o ensino jurídico no contexto neoliberal, em que o papel do Estado tem diminuído na execução de políticas públicas estrategicamente relevantes como a educação. A análise trata da mercantilização e da privatização do ensino, redirecionando o sistema educacional para a atender as necessidades lucratividade do mercado.

O artigo “Direito à privacidade no Brasil e as dificuldades impostas pela deep web” se propõe estudar os desafios impostos à devida proteção do direito à privacidade na deep web, um ambiente não indexado da internet. Devido à ausência de supervisão, a inieficácia da Lei de proteção de Dados (LDPD) não tem tanta eficácia. O texto fundamenta as implicações jurídicas da falta de supervisão e as práticas de coletas de dados.

O artigo “Diálogos institucionais com o Superior Tribunal de Justiça: efeito backlash e leis in your face” utiliza o a doutrina dos diálogos institucionais como proposta metodológica para analisar as tensões entre uma democracia deliberativa e a jurisdição constitucional. Considerando a doutrina dos diálogos institucionais como uma solução viável a essa problemática, o texto contribui ainda apresentando a possibilidades de backlash e de leis in your face no Superior Tribunal de Justiça.

O artigo “Democracia participativa no Brasil e a (in)utilização dos mecanismos diretos pelos cidadãos” estuda a forma pela qual os mecanismos de participação são inutilizados no constitucionalismo brasileiro. Destacando o plebiscito, a iniciativa popular e o referendo, o

texto conclui que esses dispositivos acabam caindo no descaso e no desconhecimento da população, enfraquecendo o esforço constitucional de participação popular.

O artigo “Suprema função: passos e compassos do STF na consolidação dos direitos fundamentais” estuda o Supremo Tribunal Federal na sua função de garantido da princípios democráticos estabelecidos na constituição. O texto destaca que há uma evolução dessa função, mas que há pouca utilização do controle de convencionalidade e na atuação na vedação do retrocesso dos direitos já consolidados.

O artigo “O papel da doutrina dos precedentes para controle do ativismo judicial no STF em casos de judicialização da megapolítica” parte da questão da insegurança jurídica causada pela imprevisibilidade dos precedentes estabelecidos pelo Supremo Tribunal Federal. Os precedentes, então, são vistos como uma forma de garantir a segurança jurídica. Os exemplos trazidos são os relacionados aos mandados de segurança nº 37760 MC/DF e nº 38217/DF.

O artigo “Constituição como árvore viva e o desenvolvimento do direito antidiscriminatório: o caso da criminalização do discurso de ódio no Brasil”, de forma inovadora, propõe debater o constitucionalismo vivo de Wil Waluchow de forma crítica e contextualizada ao contexto brasileiro. Partindo de um olhar que aprofunda a participação popular em precedentes judiciais, ele sugere compreender a criminalização do antisseminitsmo e da homotransfobia como uma proposta de desenvolvimento do constitucionalismo brasileiro.

O artigo “A separação de poderes e a atuação expansiva do Poder Judiciário” estuda a questão da expansão do Poder Judiciário dentro dos clássicos da teoria política. O texto destaca que a doutrina norte-americana introduz um novo olhar para o problema, haja vista que confere um papel jurídico-político às cortes. Essa expansão, explicada por novas doutrinas, fundamentam essa expansão por meio da técnica, da racionalidade e da argumentação jurídicas.

O artigo “Acessibilidade ao meio físico como direito fundamental e pessoas com deficiência” questiona se o ordenamento jurídico brasileiro garante o acesso ao meio físico às pessoas com deficiência como direito fundamental. Partindo de um estudo relacionado à dignidade humana e à evolução histórica dos direitos fundamentais, o texto conclui que o acesso ao meio físico é um direito garantido no ordenamento brasileiro.

O artigo “A descolonização jurídica da América Latina a partir do plurinacionalismo” estuda o plurinacionalismo dentro do Constitucionalismo Latino-americano como uma prática que rompe com a tradição liberal ao construir um espaço jurídico baseado na cultura de povos

marginalizados na região. Tudo isso, logo, é defendido como uma experiência jurídica descolonial do poder e da justiça.

O artigo “A dignidade da pessoa humana e o Supremo Tribunal Federal: uma análise da decisão na ADPF 976” estuda a violação de direitos de pessoas em situação de rua a partir da dignidade humana e da teoria do estado de coisas inconstitucional. A proposta do texto é aferir o nível de correção e de transformação da realidade na ADPF nº 976. A conclusão é que o caso guarda sentido com uma nova compreensão de normatividade.

O artigo “Inaplicabilidade do acordo de não persecução penal nos crimes raciais: uma análise da jurisprudência do Supremo Tribunal Federal” estuda a decisão do Supremo Tribunal Federal que entendeu pela inaplicabilidade do acordo de não persecução penal em casos de incidência de crimes raciais. Defendendo a sua adequação constitucional, o texto sustenta sua tese por meio dos conceitos de dignidade humana e de cidadania racial.

O artigo “Presidência do STF e a construção da pauta do plenário: impactos na decisão de questões de megapolítica”, de forma inovadora, analisa o arranjo institucional do Supremo tribunal Federal e o poder que é conferido à instituição por meio dele. Nesse contexto, o poder decisão da pauta do plenário é inserida para explicar a judicialização da megapolítica. Tal poder, conferido ao presidente do STF, é estudado em seus mecanismos e em como sua utilização interfere na opinião pública brasileira.

O artigo “35 anos da constituição federal de 1988: do lobby do batom ao constitucionalismo feminista” estuda a participação das mulheres na Assembleia Nacional Constituinte de 1987 e, também, os reflexos dessa atuação atualmente. Reconhecendo a relevância dessa notícia histórica, o texto também conclui que é necessário continuar evoluindo, especialmente no que se refere aos direitos relacionados ao gênero e à superação da suposta neutralidade do sistema jurídico.

Finalizando o GT, o artigo “(Des)Cabimento das decisões monocráticas em ações diretas de inconstitucionalidade: análise da liminar que suspendeu trechos de decretos flexibilizadores de regras sobre armas de fogo” investiga a medida na qual o Supremo Tribunal Federal protegeu a liberdade ao abordar a regulação de armas de fogo por meio de decisões monocráticas. A conclusão foi que elas não contribuíram para a preservação do direito fundamental e relativizaram por meio de atuação moral e do desrespeito a textos legais.

Dessa forma, pelos temas abordados, é possível deduzir que os debates foram calorosos e que os textos dão subsídio para novos estudos a respeito dos temas abordados. A qualidade dos

argumentos trazidos demonstrou a concatenação do estudo da jurisprudência do STF com a doutrina política e jurídica a respeito da relação entre constituição, teoria constitucional e democracia.

Boa leitura a todos!

Francisco Tarcísio Rocha Gomes Júnior (Centro Universitário Christus). Email: tarcisiorg@gmail.com

Luiz Gustavo Gonçalves Ribeiro (Dom Helder – Escola Superior). Email: lgribeirobh@gmail.com

DIREITO À PRIVACIDADE NO BRASIL E AS DIFICULDADES IMPOSTAS PELA DEEP WEB

PRIVACY RIGHT ON THE DEEP WEB AND THE LGPD PRIVACY

Soraia Giovana Ladeia Forcelini
Jéssica Amanda Fachin

Resumo

Este estudo visa explorar os obstáculos impostos ao direito à privacidade na deep web, um ambiente não indexado da internet acessível por meio de ferramentas específicas. O foco reside na análise das questões envolvendo a proteção dos dados pessoais dos indivíduos dentro desse espaço, devido à ausência de supervisão e à ineficácia na aplicação da Lei Geral de Proteção de Dados (LGPD). Embora a LGPD estabeleça uma estrutura sólida para proteção de dados no Brasil, enfrenta desafios perante a natureza internacional e evasiva da deep web. A falta de jurisdição clara e a complexidade na identificação dos responsáveis por violações de privacidade dificultam a aplicação das penalidades legais. Em resumo, o estudo busca aprofundar a compreensão das implicações da redução do direito à privacidade na deep web, analisando a interação entre a falta de supervisão, as práticas de coleta de dados e os obstáculos na aplicação da LGPD, busca-se fornecer uma visão embasada nos desafios que surgem na proteção da privacidade nesse ambiente virtual complexo e multifacetado. O método empregado para o desenvolvimento da pesquisa é o dedutivo alinhado a técnicas de pesquisa bibliográfica

Palavras-chave: Deep web, Lgpd, Privacidade, Coleta de dados, Democracia

Abstract/Resumen/Résumé

This study aims to explore the obstacles imposed to the right to privacy on the deep web, a non-indexed internet environment accessible through specific tools. The focus lies on the analysis of issues involving the protection of individuals' personal data within this space, due to the lack of supervision and ineffective application of the General Data Protection Law (LGPD). Although the LGPD establishes a solid framework for data protection in Brazil, it faces challenges due to the international and evasive nature of the deep web. The lack of clear jurisdiction and the complexity in identifying those responsible for privacy violations make it difficult to apply legal penalties. In summary, the study seeks to deepen the understanding of the implications of reducing the right to privacy on the deep web, analyzing the interaction between the lack of supervision, data collection practices and obstacles in the application of the LGPD, seeking to provide an insight based on the challenges that arise in protecting privacy in this complex and multifaceted virtual environment. The method used to develop the research is deductive, aligned with bibliographic research techniques.

Keywords/Palabras-claves/Mots-clés: Deep web, Lgpd, Privacy, Data collection, Democracy

INTRODUÇÃO

A humanidade, embora de modo dispare, experiência a denominada Quarta Revolução Industrial, caracterizada por avanços tecnológicos que estão promovendo transformações profundas na sociedade. Essas mudanças se manifestam em diversos âmbitos, como o trabalho, a economia e as relações interpessoais.

Essas transformações sociais têm desafiado o campo jurídico a se adaptar a essa nova realidade digital, reexaminando e redefinindo os princípios constitucionais para abranger esse ambiente em constante evolução. Dentro desse contexto, é crucial que conceitos como privacidade, intimidade, honra e dignidade humana se estendam para abranger também o ciberespaço, embora sob novas circunstâncias e contextos.

Paralelamente, a legislação brasileira, além de uma perspectiva constitucional, tem tido a necessidade de inovação para lidar com os desafios da era digital. Isso tem ocorrido tanto pela introdução de novas definições de tipos penais quanto pela regulamentação de relações específicas no ambiente online, como a proteção de dados, por exemplo.

Dessa forma, a Quarta Revolução Industrial tem demandado uma resposta robusta do sistema jurídico, tanto para garantir que os direitos fundamentais das pessoas se estendam ao mundo digital quanto para criar instrumentos legais que sejam eficazes na regulação de questões emergentes no ciberespaço.

Dentro do contexto da *deep web*, onde a ausência da aplicação da LGPD é evidente, Fábio Konder Comparato, em sua obra "O Poder de Controle na Sociedade Anônima" (1976), traz à tona discussões que ganham relevância ao se examinar a privacidade. Nessa esfera, a privacidade dos atores envolvidos, como usuários, administradores e outros agentes, se destaca como uma preocupação primordial.

Sob a perspectiva da privacidade no contexto da *deep web*, considerando a ausência da aplicação da LGPD, surge uma série de reflexões sobre crimes virtuais que envolvem violações à privacidade. Condutas antes não contempladas pelo código penal podem ser tipificadas, resultando em ofensas à dignidade humana e à reputação das vítimas. Muitos desses crimes estão relacionados à invasão de sistemas com o intuito de cometer atos ilícitos, além de outras estratégias prejudiciais perpetradas pelos criminosos.

A notoriedade desses crimes se deve, em grande parte, ao fato de que frequentemente impactam aspectos extremamente valiosos para as pessoas, como a honra, a intimidade e a própria imagem.

O vazamento de informações sensíveis causa considerável dor, sofrimento e uma série de consequências adversas.

Na busca por perpetrar tais crimes, alguns indivíduos recorrem à *deep web*, embora isso não seja uma regra, uma vez que a surface web também oferece oportunidades. Nessas situações, criminosos buscam informações nos computadores das vítimas, visando o enriquecimento ilícito ou a difamação pública.

A utilização da internet, tanto na surface web quanto na *deep web*, por parte de criminosos, é inevitável. No entanto, a proteção dos princípios fundamentais estabelecidos na Constituição, bem como a salvaguarda da privacidade e da dignidade humana, são desafios significativos para as autoridades encarregadas de garantir esses direitos.

Dentro desse cenário, recai sobre o Poder Legislativo a responsabilidade de criar leis que não apenas preservem os direitos básicos dos cidadãos, mas também protejam a privacidade e a dignidade na era digital. Este trabalho se divide em duas partes.

Nesse sentido, no presente texto, primeiramente, serão explorados os direitos fundamentais, como intimidade, privacidade, honra e dignidade humana, a fim de delimitar sua extensão e abordar os desafios em meio à atual era digital. Na segunda parte, serão analisadas legislações infraconstitucionais que buscam oferecer maior proteção a esses direitos, adaptando-se à nova realidade digital e social no Brasil.

A abordagem metodológica adotada é a teórico-dogmática, que se fundamenta na utilização de princípios doutrinários e pesquisas científicas. Diversas fontes, desde questões constitucionais até correntes filosóficas, serão exploradas para enriquecer essa análise crítica e sistemática, proporcionando uma compreensão abrangente e embasada do tema abordado.

1 DIREITO FUNDAMENTAL À PRIVACIDADE NA CONSTITUIÇÃO BRASILEIRA

No estudo das tecnologias, Castells enfatiza que ela é uma força motriz por trás das transformações sociais, econômicas e culturais (Castells, 2020, p. 87). Ainda, argumenta que a tecnologia não é apenas uma ferramenta neutra, mas está enraizada em contextos sociais, políticos e econômicos mais amplos, influenciando e sendo influenciada por eles. Suas ideias sobre a "sociedade em rede" ressaltam como a tecnologia da informação e comunicação tem dado forma às estruturas sociais e às interações humanas na era contemporânea.

Desse modo, a definição de tecnologia de Castells vai além da mera descrição de dispositivos técnicos e incorpora o papel vital que a tecnologia desempenha na construção e transformação da sociedade em todas as suas dimensões (Castells, 2020, p. 90).

O ciberespaço tem imposto novos desafios para o Direito e o resgate de alguns valores para adaptação a esse novo cenário. Nesse sentido, Pierre Lévy define ciberespaço como:

> novo meio de comunicação que surge da interconexão mundial dos computadores. O termo especifica não apenas a infraestrutura material de comunicação digital, mas também o universo oceânico de informações que ela abriga, assim como os seres humanos que navegam e alimentam esse universo.” (Lévy, 1999, p. 17).

Logo, para Lévy, o ciberespaço é um ambiente em que a inteligência coletiva pode florescer, permitindo que pessoas de diferentes partes do mundo se conectem e compartilhem conhecimentos. Ele também destaca a importância das comunidades virtuais, da criação colaborativa e do acesso à informação nesse novo espaço digital (Lévy, 1999, p.29).

Na definição de ciberespaço de Pierre Lévy, o autor enfatiza a dimensão social e cultural da internet, destacando-a como um espaço onde as interações humanas ocorrem de maneira única, transformando a maneira como as pessoas se comunicam, colaboram e constroem conhecimento (Lévy, 1999, p. 36).

Dentro dessa perspectiva, é relevante destacar que a privacidade, configura um direito de primeira dimensão, claramente delineado na Constituição Brasileira de 1988 e também nas legislações infraconstitucionais. Esse direito, que evoluiu ao longo dos séculos e está presente nos textos constitucionais desde o século XVIII, e necessita de uma reinterpretação à luz da complexa realidade apresentada pela era digital.

A violação desses direitos, os quais o artigo 5º da Constituição assegura de maneira inequívoca, ocorre quando a garantia de que a privacidade de cada indivíduo, é desrespeitada, não se submetendo a qualquer tipo de ação com essa intenção.

Ademais, como será demonstrado mais adiante, dentro do contexto do Direito Brasileiro, é possível identificar implicações de natureza penal voltadas para a proteção desses mesmos valores mencionados anteriormente.

Nesse contexto, certos comportamentos podem se caracterizar como transgressões criminais, resultando em responsabilidade legal e submissão às punições delineadas pelas leis em vigor. A legislação atual estabelece critérios e diretrizes que servem como parâmetros para avaliar a seriedade dessas violações e determinar as consequências adequadas, garantindo, assim, a efetiva salvaguarda desses princípios vitais.

Essas avaliações preconizadas pela Constituição possuem um caráter fundamentalmente protetor, visando resguardar a dignidade da pessoa humana e seus direitos, independentemente de serem de natureza puramente econômica.

No entanto, antes de explorar esses direitos essenciais delineados na Constituição, é imperativo ressaltar a importância da dignidade da pessoa humana. Essa premissa está expressa

no artigo primeiro da Constituição Federal, em seu terceiro inciso, e é considerada o princípio que irradia legitimidade para todo o sistema jurídico.

Segundo Celso Ribeiro Bastos (Bastos, 2004, p. 63), consiste o direito à privacidade na faculdade que tem cada indivíduo de obstar a intromissão de estranhos na sua vida privada e familiar, assim como de impedir-lhes acesso a informações sobre a privacidade de cada um e também impedir que sejam divulgadas informações sobre esta área da manifestação existencial do ser humano.

Celso Lafer discute questões fundamentais relacionadas à privacidade e à sua violação, à luz dos direitos humanos, contando com reflexões sobre o significado da privacidade no contexto dos direitos humanos e como essa dimensão crucial da dignidade humana pode ser afetada por diversas formas de violação (Lafer, 1988, p. 67).

Lafer aborda a quebra da privacidade em diversas esferas, incluindo as governamentais, empresariais e tecnológicas (Lafer, 1988, p. 69). De maneira inovadora, ele argumenta que práticas como a excessiva coleta de informações pessoais, a vigilância em larga escala e a perda de controle sobre dados individuais podem minar a autonomia e a liberdade pessoal, que são valores essenciais dos direitos humanos.

Além disso, Lafer explora o impacto da evolução da tecnologia da informação e da comunicação nas concepções tradicionais de privacidade, considerando elementos como as redes sociais, a internet e as capacidades crescentes de monitoramento.

Por fim, ele propõe que se estabeleçam mecanismos legais e institucionais para salvaguardar a privacidade e evitar sua violação (Lafer, 1988, p. 112). Ele enfatiza a importância da educação e conscientização, capacitando os indivíduos a compreender melhor seus direitos de privacidade e adotar medidas para protegê-los.

Muitas vezes encontra-se os termos intimidade e privacidade interligados, o que não é correto, pois são distintos entre si, uma vez que a intimidade, como já mencionado, trata-se dos fatos da vida humana em seus aspectos pessoais, onde cabe somente a este ser humano a decisão de divulgar ou não, já a privacidade tem relação com outras pessoas, como relação familiar e entre amigos (Júnior, São Paulo. 1993, p. 25).

Paulo José da Costa Junior (Junior, 2007, p. 27-28), analisando a questão das diferenças expostas acima, preleciona:

> Ainda, se são dois os momentos de um único direito, não vemos razão para denominar diversamente ambas as esferas privadas. Chamemo-las, pois, indiferentemente, de direito à intimidade. Se se trata de preservá-la, ou de mantê-la, pouco importa. É sempre direito à intimidade. Intimidade e não

> recato (riservatezza), que mais parece uma “disposição de ânimo que um modo de viver exterior”.

Portanto a intimidade é direito pessoal que não pode (sem que o titular deste direito deseje) ser exposto à publicidade, sob pena de implicações criminais para aquele que trazê-la à público de modo indevido.

Diante desta definição, verifica-se que o doutrinador, tem a percepção de distinção entre a privacidade e intimidade, mas considera estas pertencentes a um mesmo direito, ainda que ocorram em momentos distintos.

O direito à privacidade foi reconhecido pela Constituição Federal de 1988, mas antes disso já existiam regulamentos isolados, como o Código Civil de 1916, que tratava da relação da vizinhança e ao sigilo da correspondência.

Além disso, o Código Penal também protegia a intimidade ao abordar temas como invasão de domicílio, violação de correspondência e divulgação de segredos. Isso demonstra que as normas foram evoluindo ao longo do tempo para abordar mais amplamente esse direito.

Para Bastos e Martins (1989) em sua obra comentários à Constituição do Brasil, a privacidade é protegida na Constituição, possivelmente referindo-se ao artigo 5º, inciso X, onde estabelece que "são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas".

A partir desse ponto, a discussão envolve a proteção da privacidade em diferentes contextos, como relações pessoais, comunicação, tecnologia, entre outros, podendo explorar os avanços tecnológicos, como a internet e as redes sociais, impactaram a privacidade das pessoas e levantaram novas questões legais e éticas. Abordando temas como a coleta de dados pessoais, vigilância governamental, direito ao esquecimento, entre outros, bem como, a relação entre a violação de privacidade e outros direitos fundamentais, como liberdade de expressão, acesso à informação e segurança.

Bastos e Martins (1989) também analisam os limites da privacidade quando entra em conflito com outros interesses públicos ou individuais, explorando as medidas legais e institucionais disponíveis para proteger a privacidade e remediar sua violação, considerando a jurisprudência nacional e internacional, bem como os tratados de direitos humanos dos quais o Brasil é signatário.

O direito à privacidade tem o cunho de relacionamento entre pessoas, como relação familiar, comercial, entre outras que os envolvidos não desejam que o conhecimento venha a público.

Maria Helena Diniz (Diniz, 2005, p. 135) salienta que intimidade e privacidade são distintas e não podem ser confundidas, ao escrever que “(...) a privacidade não se confunde com

a intimidade, mas esta pode incluir-se naquela". Assim a autora, tem a consideração que questões relacionadas à privacidade são aspectos externos da vivência do ser humano e a intimidade seriam os internos de cada pessoa.

O direito à privacidade também veio ganhando espaço no ordenamento jurídico brasileiro, como pode-se verificar o artigo 147-A do Código Penal.

Encontra-se respaldo para o direito a privacidade em tratados internacionais, como se pode verificar na Declaração Universal dos Direitos Humanos (ONU, 1948), que, em seu artigo 12, dispõe: "Ninguém será sujeito a interferências na sua vida privada, na sua família, no seu lar ou na sua correspondência, nem a ataques à sua honra e reputação. Toda pessoa tem direito à proteção da lei contra tais interferências ou ataques".

Portanto a privacidade da pessoa, não se restringe a um entendimento nacional, mas sim a uma preocupação mundial, ainda que de forma diferente da abordada no Brasil, trazendo neste caso o conceito para a normatização brasileira, não havendo qualquer minoração inclusive no âmbito da internet.

2 . PROTEÇÃO INFRACONSTITUIONAL À PRIVACIDADE E AS DIFICULDADES IMPOSTAS PELA *DEEP WEB*

Observando os direitos constitucionalmente protegidos, relacionados à intimidade, privacidade e imagem da pessoa, resultaram na compreensão desta modalidade criminosa e como forma de combate, houve a edição de inúmeras normas com a finalidade de proteção.

Nesse sentido, as principais leis que deram impulso um normativo mais aprimorado sobre o tema, começaram já em 2012 e caminharam até os dias de hoje adotando maiores sistemáticas de proteção a cada nova norma.

Nesse sentido a lei vigente brasileira em relação ao cibermundo dipõe de normas infraconstitucionais que auxiliam o judiciário a resolução problemas relacionados à ocorrência de violações de privacidade como a lei Azeredo, Lei Carolina Dieckmann, marco civil da internet, que alteraram em alguns casas o código penal, em seus artigos 154-a e b,

> Art. 154-A. Invadir dispositivo informático de uso alheio, conectado ou não à rede de computadores, com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do usuário do dispositivo ou de instalar vulnerabilidades para obter vantagem ilícita: (Redação dada pela Lei nº 14.155, de 2021)
> § 2º Aumenta-se a pena de 1/3 (um terço) a 2/3 (dois terços) se da invasão resulta prejuízo econômico. (Redação dada pela Lei nº 14.155, de 2021)
> § 3o Se da invasão resultar a obtenção de conteúdo de comunicações eletrônicas privadas, segredos comerciais ou industriais, informações

> sigilosas, assim definidas em lei, ou o controle remoto não autorizado do dispositivo invadido: (Incluído pela Lei nº 12.737, de 2012) Vigência Art. 154-B. Nos crimes definidos no art. 154-A, somente se procede mediante representação, salvo se o crime é cometido contra a administração pública direta ou indireta de qualquer dos Poderes da União, Estados, Distrito Federal ou Municípios ou contra empresas concessionárias de serviços públicos."

Já o artigo 154-B dispõe que se trata de uma ação condicionada à representação, excetuando-se aqueles cometidos contra a administração pública direta ou indireta.

Assim, tem-se que a lei em questão, embora tenha trazido alguns avanços, demonstra claramente que o legislativo nesse meio, necessita de inúmeras implantações até atingirem um patamar aceitável em relação aos crimes ocorridos e a sua efetiva punição.

5.3. MARCO CIVIL DA INTERNET

Veio à luz para ditar as diretrizes de normatização do uso da rede mundial de computadores no Brasil.

É conhecido como o Marco Civil da Internet, pois trata dos princípios, garantias, direitos e deveres dos usuários e até mesmo do Poder Público.

O Marco Civil da Internet se tornou um instrumento norteador de decisões judiciárias em casos relacionados aos crimes virtuais, pois, anteriormente, não havia nenhuma norma específica que os magistrados pudessem tomar como base.

Para entender a Lei 12.965 de 2014, precisamos primeiramente saber qual o seu objetivo, pois esta lei trata de diretrizes da atuação da União, direitos e deveres dos usuários e seus princípios e garantias, conforme exposto no seu artigo 1º: "Art. 1º Esta Lei estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil e determina as diretrizes para atuação da União, dos Estados, do Distrito Federal e dos Municípios em relação à matéria". (BRASIL, 2014).

Mas os princípios descritos nesta lei não podem colidir com os Constitucionais, pois a Carta Magna resguarda todos os direitos individuais, fundamentais dos indivíduos. Resta esclarecer que os princípios tratados pelo Marco Civil da Internet não são rol taxativos e sim exemplificativos, pois o Brasil é signatário de vários tratados internacionais, que podem resguardar outros princípios que não estão expressos na lei.

2.1. LEI GERAL DE PROTEÇÃO DE DADOS

Outra norma que deu importantíssima contribuição ao combate a praticas lesivas a imagem, a privacidade e a honra, foi a edição da Lei Geral de Proteção de Dados, onde dispõe de artigos específicos tratados pela Constituição Brasileira.

A proteção de dados sob o enfoque constitucional, tem melhor explicitação através do artigo 2º da lei, respaldando aqueles já tratados anteriormente:

> Art. 2º A disciplina da proteção de dados pessoais tem como fundamentos:
> I - o respeito à privacidade;
> IV - a inviolabilidade da intimidade, da honra e da imagem;

Nesse novo normativo, o tratamento de dados tem papel fundamental para o combate a desinformação e a consequente invasão a intimidade da pessoa, posto que é passível de indenização a prática ilícita de qualquer forma, ainda que a empresa não tenha participado ativamente.

O fato é que a negligência da empresa, segundo o texto legal, também fica responsável pela sua falta de comprometimento com os dados de seus clientes e usuários, o que gera uma preocupação com a violação de direitos constitucionalmente previstos.

Efetivamente, no cenário contemporâneo, as empresas que se envolvem na coleta e manipulação de dados dos usuários estão cada vez mais inclinadas a adotar uma postura criteriosa no que diz respeito à divulgação de qualquer forma de informação pertinente aos seus clientes.

Esse comportamento deriva da crescente conscientização sobre a importância da proteção da privacidade e dos direitos individuais.

Ao adotar tal abordagem, tais empresas almejam mitigar potenciais interferências que possam afetar a relação com seus clientes, bem como salvaguardar a honra e a imagem dos mesmos diante de possíveis ameaças ou violações.

Tal postura se respalda tanto em princípios éticos e morais quanto em regulamentações legais e práticas de conformidade, que reconhecem a relevância da preservação da dignidade e da reputação dos indivíduos em um contexto digital cada vez mais interconectado.

Portanto, ao adotar medidas cautelosas no tratamento de informações sensíveis, as empresas buscam não apenas atender às exigências do mercado, mas também demonstrar um compromisso genuíno com a proteção integral dos direitos e valores dos seus clientes.

A *deep web* é assim chamada devido ao fato de que é uma zona desvinculada de controle por parte de empresas e governos, aos quais propiciam outra forma de vinculação de violação dos direitos constitucionalmente trazidos pelas normas vigentes até então. De fato, o ambiente em questão não oferece grandes seguranças que são tão veementemente buscadas pela lei Geral de Proteção de dados.

Nesse ambiente, a proteção de dados é algo que não se busca, do qual os navegantes têm plena ciência desse fato.

Já a *surface* não oferece tantos problemas tornando-se mais fácil a localização do agente que cometer ato ilícito, da qual se auxilia em muito a proteção e o sigilo das informações exigidos pela lei.

Contudo, no âmbito do empenho para preservar não somente a imagem, honra e intimidade individuais, mas também em prol do bem-estar coletivo, emerge um conjunto abrangente de procedimentos técnicos conduzidos por profissionais especializados.

O escopo desse esforço consiste em responsabilizar de maneira adequada e eficaz aqueles indivíduos ou entidades que venham a infringir quaisquer dos direitos fundamentais, cujas transgressões possam resultar em prejuízos tangíveis ou intangíveis para os indivíduos afetados ou para a sociedade em geral.

Esta abordagem recai sobre um conjunto interdisciplinar de ações, envolvendo profissionais do direito, da tecnologia da informação, da segurança cibernética e da comunicação, entre outros. Esses especialistas se dedicam a desenvolver e implementar estratégias que abordem tanto a prevenção quanto a punição, considerando os desafios intrínsecos ao ambiente digital em constante evolução.

A preparação técnica mencionada engloba desde a análise e a interpretação das leis e regulamentos pertinentes até o desenvolvimento de soluções tecnológicas avançadas, como sistemas de detecção de violações, análise forense digital e métodos de rastreamento de atividades suspeitas. Adicionalmente, o sistema legal também é mobilizado para promover a responsabilização por meio de ações civis ou criminais, a depender da natureza da violação e dos danos resultantes.

Em última análise, a preparação técnica e a atuação coordenada desses agentes especializados representam uma resposta robusta e abrangente à proteção dos direitos individuais e coletivos. Ao promover a justiça e a responsabilização diante de violações, essa abordagem contribui para a manutenção de um ambiente digital mais seguro e respeitoso, no qual os direitos e a dignidade das pessoas são resguardados com diligência e comprometimento.

Apesar desses esforços esbarrarem em impossibilidades técnicas, quando os infratores trazem seus atos para o mundo real, é possível aplicar punições das mais diversas, o que infelizmente não é possível se os criminosos permanecerem no ambiente virtual apenas.

A *surface* não possui esses os mesmos empecilhos técnicos impostos pela *deep web,* o que torna os serviços das autoridades competentes para a investigação de crimes no ambiente virtual mais eficazes.

Nesse sentido, é possível, hoje, apresentar diversas Fake News além de vinculações de notícias que invariavelmente atacam a honra e a intimidade de pessoas ligadas ou não ao governo, algo que somente ocorria em épocas eleitorais.

Hoje, basta que uma pessoa tenha certa credibilidade para presenciar sua vida privada exposta em diversas mídias e redes sociais, sem qualquer controle se estas forem oriundas desse meio.

Logo, tanto a *surface* quanto a *deep web* possuem suas dificuldades para assegurar a garantia dos direitos constitucionais dos cidadãos brasileiros.

Para Comparato o poder de controle e sua influência na privacidade dos envolvidos nas empresas anônimas ressoam de maneira relevante na discussão sobre a privacidade dentro da *deep web*, onde a falta de regulamentação como a LGPD amplifica os desafios relacionados à proteção dos dados pessoais e à guarda dos direitos individuais.

Portanto, a normatização de conteúdo da navegação na internet, é possivelmente o foco de leis com o cunho de proteção dos direitos mais básicos do cidadão brasileiro, tais como a honra, imagem e intimidade.

Além desse fato, a busca pela privacidade na internet é um tema muito relevante, e a implementação da LGPD (Lei Geral de Proteção de Dados) no Brasil reflete a crescente preocupação em proteger as informações pessoais dos usuários online.

No entanto, é importante destacar que a privacidade e o anonimato na *deep web* representam uma faceta diferente desse desafio.

A *deep web* é um espaço online que não é indexado pelos motores de busca convencionais, e muitas vezes requer softwares específicos, como o *tor*, para acessá-la. É verdade que na *deep web*, as atividades dos usuários podem ser mais anônimas em comparação com a superfície da web convencional.

Isso ocorre porque o anonimato é uma característica fundamental do *tor* e de outros sistemas que permitem navegar de forma anônima.

No entanto, essa busca por anonimato também traz desafios e questões éticas. A *deep web* é conhecida por abrigar não apenas atividades legítimas e benignas, mas também atividades ilegais, como tráfico de drogas, armas e conteúdo ilegal.

O anonimato na *deep web*, muitas vezes, é utilizado por pessoas que buscam se esconder para cometer crimes, e isso cria um dilema entre a proteção da privacidade e a necessidade de fazer cumprir a lei.

A LGPD e leis semelhantes em outros lugares visam encontrar um equilíbrio entre a proteção da privacidade dos indivíduos e a necessidade de garantir que as atividades ilegais não ocorram impunemente.

Portanto, embora o anonimato na *deep web* possa oferecer uma forma de privacidade, ele também levanta preocupações sérias sobre a regulamentação e a aplicação das leis.

Em resumo, a busca pela privacidade na internet é uma preocupação legítima e importante, e a LGPD é um passo na direção certa para proteger os dados pessoais dos usuários.

No entanto, a *deep web*, com seu anonimato, traz desafios adicionais e questões éticas relacionadas à regulamentação e à aplicação da lei. O equilíbrio entre a proteção da privacidade e a prevenção de atividades ilegais é um desafio complexo e em constante evolução no mundo cibernético.

2.2 O QUE É A "*DEEP WEB"*

Tão antigo quanto a própria internet, a *"deep web"* é um conceito que se estruturou com objetivo de divulgar a informação não só a comum, mas também todo e qualquer dado de forma livre sem filtros, sem intervenção do governo, sem intervenções políticas de qualquer forma, o objetivo da *"deep web"* em sua essência é pura e mera divulgação de informações, porém de forma equivocada as pessoas que nela navegam tem a tendência a cometer diversos atos ilícitos, atos esses, que serão estudados neste trabalho.

Ainda sem adentrar no próprio mérito do estudo, a *"deep web"* é um meio ambiente rico em pesquisas, informações e diversos outros serviços que, embora não entre em destaque na atualidade, é incontroverso a sua utilidade para os usuários, apesar do grande destaque internacional que se dá a *"dark web"*, esta, não serve somente para o cometimento de crimes e atos ilícitos mas também como um ótimo instrumento de aprendizado e de desalienação do mundo como um todo.

A "*deep*" é um ambiente ao qual a liberdade do ser humano é exercida de forma mais ampla, sem as restrições impostas pelos meios de comunicação e pelos governos, de forma que a quantidade de adeptos que ingressam nesse submundo aumenta de forma exponencial.

Nesse contexto, é necessário o entendimento da forma de navegação, que já explicitado anteriormente, porém, para a internet normal ("*surface*"), agora demonstraremos como se dá a utilização na *"deep web"*.

Comparato explora a estrutura de poder e controle nas empresas anônimas, o que pode ser relacionado à dinâmica da *deep web*, onde a identidade e as ações dos atores muitas vezes permanecem ocultas.

As decisões tomadas, bem como as informações compartilhadas, podem impactar diretamente a privacidade e os direitos das partes envolvidas. Isso ressoa no ciberespaço, onde a ausência de supervisão e regulamentação pode permitir práticas que afetem negativamente a privacidade dos indivíduos.

Ao discutir questões éticas e legais, Comparato destaca a importância da divulgação de informações, transparência e deveres fiduciários nas empresas anônimas. No âmbito da deep web, esses princípios também podem ser aplicados, enfatizando a necessidade de considerar a privacidade como um valor essencial na tomada de decisões e nas atividades que ocorrem nesse espaço virtual.

A grande diferença entre a "*deep*" e a "*surface*", se da na forma de mascarar o número que o computador recebe quando ingressa no mundo virtual, tornando assim, extremamente difícil o rastreio desses equipamentos, o que facilita para os usuários mal intencionados para o cometimento de atos ilícitos.

2.3 Servidor Hibernado

Como explicado anteriormente, na internet comum, cada computador assume um número único quando ingressa no ambiente virtual, e diferentemente da internet comum, a *"deep web"* passa por uma série de criptografias que impossibilitam o rastreio do computador em si.

No mundo da internet, a comunicação entre os computadores não se dá de forma direta, mas sim através de diversos outros equipamentos.

Nesse sentido, o conceito de servidor, é um computador que contém as informações que necessitamos, e na internet comum, quando buscamos essa informação o sistema de DNS (Sistema de Domínio de Nomes) nos envia diretamente para o computador que possui essa informação.

Basicamente o DNS, é um sistema de gerenciamento de nomes, onde contém registros com o nome do "*site* " e o número do IP à ele relacionado e quando o computador faz a busca, este é imediatamente direcionado para aquele número de equipamento especificado.

Na *"deep web"*, a requisição passa por diversos computadores, até possamos acessar a informação que necessitamos, de modo que não se sabe ao certo quem esta acessando aquele computador.

Assim temos que o servidor encaminha todas as informações através da rede, e todos os computadores tem uma espécie de cópia do conteúdo acessado, em cada requisição, de forma, tudo que é acessado na internet tem cópias e mais cópias, no mundo virtual.

No entanto, na *"deep web"*, a criptografia permite que apenas os computadores requisitante e requisitado, possam decodificar a informação, de modo que, qualquer computador que intercepte as requisições, não conseguirá decifrar os dados.

Logo, temos que o servidor no ambiente virtual, trabalha de forma hibernada, ou seja, todas as informações que ele dispõe, não ficam arquivadas em memória virtual, mas sim, no disco rígido do próprio computador, ou seja, toda a informação que ele possui, encontra-se exclusivamente nele, não havendo cópias, o que impossibilita aos investigadores a interceptação de qualquer informação útil à localização do computador ou usuário.

Neste sentido, a dificuldade de localização do servidor hibernado é extrema, o que, por sua vez, torna a procura de qualquer pista em relação aos crimes cometidos nesse ambiente, uma impossibilidade de proporções gigantescas.

Portanto, não havendo possibilidade de localização do computador que possibilita o cometimento de crimes, estes restam totalmente impunes, uma vez que o criminoso não pode ser localizado, para responder pelos seus atos ilícitos.

2.4 NAVEGAÇÃO NA "DEEP WEB"

A internet trabalha através de um sistema onde todas as informações são registradas por meio de servidores e inúmeras outras ferramentas ao qual destina-se ao controle do fluxo de dados que transitam pelo meio virtual.

Diferentemente da internet comum, temos que o submundo da internet trabalha de forma contrária ao da chamada "*surface*", nesse aspecto, a chamada "*dark web*" tem um tratamento diferenciado por aqueles que a utilizam uma vez que a transmissão de informações não segue nenhum controle governamental, institucional ou de qualquer outra natureza.

Enquanto que na internet normal, todos os meios para registro das informações e, automaticamente, supervisão dessas, é utilizado, na *deep web* as informações transitam com certa liberdade, aliás, com toda a ela, visto que não há restrição do material postado o mesmo pesquisando nesse ambiente.

A verdade é que não havendo o poder estatal para infringir regramento no ambiente virtual da *"deep web"*, os usuários desse ambiente, podem transitar livremente sem qualquer restrição, facilitando e muito a ocorrência de crimes diversos, das mais variadas formas e gravidade.

A navegação nesse meio virtual é um tanto complicada e de vagarosa visto que a linha de investimento não conta com a colaboração de grandes corporações, estados, e organizações

não governamentais, que pudessem alavancar um investimento alto para auxiliar os servidores desse meio.

A navegação neste ambiente, envolve um conhecimento mais profundo sobre informática, fato que diferente do que a maioria das pessoas possam acreditar, cerca de 90% daqueles que utilizam a internet normal, não tem a menor noção de como é e de como funciona, e da informação ou melhor o valor dessa pode ter para os mau intencionados.

É certo que, a menor das informações, ou até mesmo aquela mais sutil e discreta, pode ser utilizada de forma criminosa por aqueles que se destinam a aplicação de golpes e crimes no cyber mundo.

5.7 COMO FUNCIONA

A "*deep web*" opera como um sistema em que um computador solicita uma informação através da rede global de computadores. Essa solicitação é processada em outro ponto, gerando um resultado que é então devolvido ao computador solicitante. Nesse processo, entra em cena a criptografia, que pode ser comparada aos hieróglifos do antigo Egito, em que cada símbolo representava uma palavra, número ou objeto. No contexto da informática, a criptografia envolve a codificação da informação em sequências de números ou letras chamadas de caracteres alfanuméricos. O computador receptor conhece o código correspondente, decodifica a informação, processa-a e, após obter o resultado, recodifica-o para devolvê-lo ao computador de origem. Esse método assegura que os usuários possam receber informações da internet.

No entanto, na "*deep web*", onde a regulamentação é quase inexistente, o rastreamento de informações é difícil. Usuários versados em informática, que compreendem as complexidades da criptografia, aproveitam essa vantagem para cometer atos mais engenhosos. A criptografia pode ser explorada por indivíduos mal-intencionados que interceptam os pacotes de dados e, após uma análise minuciosa, iniciam um processo de descodificação.

Para combater essa ameaça, as estratégias de criptografia evoluíram. Pacotes de dados foram ampliados para acomodar mais substituições, tornando a decodificação uma tarefa extremamente complicada, se não impossível.

No cenário da "*deep web*", os "hackers" precisam adotar métodos mais criativos para contornar a criptografia mais avançada usada por empresas. Eles frequentemente enviam e-mails falsos prometendo prêmios valiosos ou promoções tentadoras para atrair vítimas. Ao clicar em links nesses e-mails, os usuários podem ser redirecionados para sites que implantam vírus, como cavalos de Tróia, "trojans", "malware" e "spyware".

Ao serem infectados, as informações pessoais das vítimas podem ser roubadas, levando a consequências como desfalques financeiros, alterações de dados nas redes sociais e mudanças de senhas, entre outras possibilidades.

Embora os crimes na internet convencional geralmente possam ser rastreados e punidos, na "*deep web*", a falta de supervisão permite que os criminosos operem com maior impunidade. Como resultado, o ambiente da "*deep web*" torna-se propício para golpes, vírus e fraudes, com a ausência de restrições facilitando ações prejudiciais.

Em resumo, a criptografia na "*deep web*" é um desafio complexo, onde as informações podem ser interceptadas sem supervisão ou controle. O ambiente virtual sem regulamentação torna-se um terreno fértil para atividades ilícitas, exigindo que os usuários estejam bem informados para identificar e mitigar ameaças, evitando assim a propagação de golpes e fraudes.

5.8 COMO SÃO PRATICADOS OS CRIMES NA "DEEP WEB"

A ausência da LGPD (Lei Geral de Proteção de Dados) no contexto da internet, especialmente na "deep web", aumenta a seriedade dos crimes cometidos nesse ambiente em comparação com os da internet convencional. Enquanto a internet regular é usada para golpes que afetam a reputação e, ocasionalmente, o patrimônio de algumas pessoas, a "deep web" possui um caráter mais grave, afetando um público maior e revelando realidades muito mais explícitas do que as experiências individuais.

A impunidade na "deep web" leva as pessoas a cometer ações mais ousadas do que na internet convencional. O rastreamento na internet, mesmo em crimes na "surface", é complexo e muitas vezes envolve a cooperação involuntária do usuário, que muitas vezes não compreende as implicações de suas comunicações sendo rastreadas.

As difamações frequentes nas redes sociais, onde as pessoas erroneamente pensam estar protegidas legalmente devido à natureza virtual, podem resultar em ações legais se prejudicarem a honra, levando a condenações ou consequências legais. Além disso, crimes que afetam o patrimônio também ocorrem nas redes sociais, muitas vezes praticados por pessoas já detidas, cujos ganhos ajudam a cumprir suas penas, destacando a precariedade do sistema carcerário que permite o acesso a dispositivos móveis e a continuidade de golpes.

A "deep web" oferece oportunidades para crimes sofisticados, como o envio de e-mails de "spam" que podem capturar o IP do remetente e revelar sua localização física, embora a maioria das pessoas não perceba esse risco. Há diversas outras formas de fraude, incluindo a tradução de informações incorretas em sites para fins criminosos, sem saber que esses sites armazenam informações do usuário para possíveis ações legais futuras.

No entanto, na "deep web", onde não há supervisão nem restrições, o rastreamento dessas atividades é praticamente inexistente. Usuários experientes nesse ambiente aproveitam a criptografia e a falta de regulamentação para evitar serem rastreados, contrastando com os usuários inexperientes que erroneamente acreditam estar protegidos contra golpes. A natureza criptografada da "deep web" torna quase impossível rastrear essas atividades.

Assim, para profissionais que buscam prevenir esses golpes, a única pista muitas vezes é a informação rastreada no ambiente virtual, que pode ser usada em investigações que afetam o mundo físico, como questões de honra e danos financeiros. Além disso, os crimes virtuais eventualmente deixam rastros no mundo real, permitindo que investigadores efetivamente capturem os infratores, tornando o trabalho no ambiente virtual mais produtivo.

CONCLUSÃO

A expansão da internet indiscutivelmente contribuiu para disseminar conhecimento entre diversas culturas e nações, acelerando o compartilhamento de informações de forma sem precedentes. Entretanto, essa ampliação de informações trouxe consigo a facilidade na violação da privacidade das pessoas, muitas vezes com o inadvertido auxílio de indivíduos que navegam pela rede global de computadores.

A imagem dos usuários da internet tem se tornado alvo de ataques por parte de criminosos, especialmente quando se trata de figuras públicas, como os influenciadores digitais. O objetivo é semear desconfiança entre seus seguidores, com potencial para arruinar reputações e violar a liberdade de opinião e a consequente privacidade. A disseminação não autorizada de imagens íntimas é uma ocorrência comum, deixando as vítimas vulneráveis a julgamentos públicos que muitas vezes prejudicam qualquer possibilidade de defesa, uma vez que o veredicto público age como juiz implacável.

Um fato ou imagem divulgado na internet pode gerar interpretações equivocadas e controversas, demonstrando o impacto poderoso que o ambiente virtual tem sobre a percepção e opiniões das pessoas.

A era digital se tornou um terreno fértil para violações de inúmeros direitos em especial a privacidade. Nesse contexto, é crucial reconhecer o papel central da Constituição Federal em proteger os cidadãos contra violações que possam ocorrer nesse meio digital.

Importante salientar que os crimes cometidos nesse ambiente carecem de legislação específica para garantir a devida punição aos infratores. O ordenamento jurídico brasileiro ainda carece de regulamentações adequadas, não apenas em relação a danos morais, mas também para

corretamente tipificar crimes envolvendo patrimônio e até mesmo aqueles que prejudicam a privacidade das pessoas.

No Direito Brasileiro, observa-se a emergência de novos crimes oriundos do ambiente digital, bem como a necessidade de proteções e punições mais rigorosas quando tais crimes são cometidos nos espaços virtuais. A falta de uma estrutura legislativa abrangente e eficaz para combater essas violações é um desafio que precisa ser abordado, especialmente dada a ausência da aplicação da LGPD nesse cenário caótico da *deep web*.

A dificuldade de permear os ambientes "obscuros" da internet é um desafio significativo enfrentado por governos, empresas, sociedade civil e até mesmo pelos próprios usuários. Esses ambientes obscuros são geralmente associados a fóruns da *deep web*, redes anônimas, sites clandestinos e espaços digitais onde a identidade e a atividade dos usuários são protegidas por anonimato e criptografia.

A tecnologia de anonimato e criptografia permite que os usuários naveguem na internet de forma completamente anônima, ocultando sua identidade e localização. Isso dificulta a identificação de pessoas envolvidas em atividades ilegais ou maliciosas.

A natureza global da internet torna difícil a aplicação da lei e a regulamentação em escala internacional. Os criminosos cibernéticos podem operar em um país enquanto estão fisicamente em outro, tornando complicada a coordenação entre jurisdições.

Em alguns países com censura estrita da internet, os usuários podem usar esses ambientes obscuros para acessar informações e se comunicar sem serem detectados pelo governo.

À medida que a tecnologia avança, os ambientes obscuros também evoluem. Novas técnicas e ferramentas surgem constantemente, tornando mais desafiador o rastreamento e o controle desses espaços.

Não são apenas criminosos que usam esses ambientes. Muitos usuários legítimos valorizam a privacidade online e buscam proteger seus dados pessoais e comunicações. Portanto, tentar regulamentar esses espaços pode levantar questões de privacidade.

Os ambientes obscuros não são apenas locais para atividades ilegais. Eles também podem abrigar grupos de defensores dos direitos humanos, jornalistas investigativos e ativistas políticos que buscam proteção contra regimes opressores.

A investigação e a aplicação da lei em ambientes obscuros exigem conhecimento especializado em segurança cibernética e técnicas de rastreamento, o que pode ser escasso em algumas agências e organizações.

Em resposta a esses desafios, muitos governos e organizações estão trabalhando para desenvolver estratégias de combate a atividades ilegais na internet, fortalecer a cooperação internacional e investir em tecnologias de segurança cibernética. No entanto, é um campo em constante evolução e um equilíbrio delicado entre a proteção da privacidade dos usuários legítimos e a necessidade de combater atividades criminosas e prejudiciais online.

É importante notar que a abordagem ideal para lidar com esses ambientes obscuros ainda está sendo debatida e pode variar dependendo das prioridades de segurança, privacidade e liberdade de expressão de diferentes sociedades e governos.

REFERÊNCIAIS BIBLIOGRÁFICAS

BASTOS, Celso, MARTINS, Ives Gandra. Comentários à Constituição do Brasil. São Paulo : Saraiva, 1989. v.2.

BASTOS, Celso Ribeiro. Comentários à Constituição do Brasil. v.II. p. 63, São Paulo: Saraiva, 2004.

BRASIL. **Código Penal.** Disponível em: <http://www.planalto.gov.br/ccivil_0 3/decreto-lei/Del2848compilado.htm>. Acesso em 29 de ago. de 2023.

BRASIL. **Constituição Federal**. Disponível em: <http://www.planalto.gov.br/ccivi l_03/constituicao/constituicao.htm>. Acesso em 29 de ago. de 2023.

BRASIL. **Lei 12.735/**2012. Disponível em: <http://www.planalto.gov.br/cciv il_03/_ato2011-2014/2012/lei/l12735.htm>. Acesso em 29 de ago. de 2023.

BRASIL. **Lei 12.737/2012**. Disponível em: <http://www.planalto.gov.br/cci vil_03/_ato2011-2014/2012/lei/l12737.htm>. Acesso em 29 de ago. de 2023.

BRASIL. **Lei de Introdução do Código Penal**. Disponível em: <http://www.planalto.gov.br/ccivil_03/decreto-lei/del3914.htm>. Acesso em 29 de ago. de 2023.

BRASIL. **Lei Geral de Proteção de Dados.** Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm>. Acesso em 29 de ago. de 2023.

BRASIL. **Lei 12.965/2014**. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>. Acesso em 29 de ago. de 2023.

CASTELLS, Manuel. A Revolução da Tecnologia da Informação. in: CASTELLS, Manuel**. Sociedade em Rede.** Trad. Roneide Vecancio Majer. 22ª ed. São Paulo: Paz e Terra, 2020, p. 87-133.

COMPARATO, Fábio. O poder de controle na sociedade anônima. São Paulo : Revista dos Tribunais, 1976.

COSTA JR, P.J. **O direito de estar só – tutela penal da intimidade** – 4ª ed. rev. e atual. São Paulo: Editora Revista dos Tribunais, 2007.

DINIZ, M.H. **Teoria Geral do Direito Civil, 1º volume**, Editora Saraiva, 22ª ed. 2005. São Paulo.

GETSCHKO, D. **Marco Civil da Internet**. São Paulo: Atlas, 2014. 1ª ed.

JÚNIOR, TÉRCIO SAMPAIO FERRAZ, Sigilo De Dados: O Direito à Privacidade e Os Limites À Função Fiscalizadora do Estado. **Revista da Faculdade de Direito**, Universidade de São Paulo. São Paulo. 1993.

LAFER, Celso. A reconstrução dos direitos humanos. São Paulo : Companhia das Letras, 1988.

LÉVY, Pierre. **Cibercultura**. 1ª ed. Trad. Carlos Irineu da Costa. São Paulo: Editora 34, 1999.

NAÇÕES UNIDAS. **Declaração Universal dos Direitos Humanos.** Disponível em: <https://declaracao1948.com.br/declaracao-universal/declaracao-direitos-humanos/?gclid=EAIaIQobChMI-cSh2uz28gIVlYKRCh3OvAGyEAAYASAAEgJjOvD_BwE>. Acesso em 29 de ago. de 2023.

RAYMOND, E.S. **The New hacker's dictionary**. MIT Press. .ISBN 0-262-68092-0 5ª ed, 1991.